

installation
guide

HP StorageWorks Command View XP

Product Version: 1.8A

First Edition (March 2004)

Part Number: B9357-96084

This guide provides an installation checklist and step-by-step instructions on how to install Command View XP, Path Connectivity, and the snap-in modules as well as set up XP disk arrays and integrate Command View XP with other platforms.



© Copyright 1999-2004 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.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft®, MS-DOS®, MS Windows®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

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 for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Command View XP Installation Guide
First Edition (March 2004)
Part Number: B9357-96084

About this Guide	7
Overview	8
Intended Audience	8
Prerequisites	8
Related Documentation	8
Conventions	9
Document Conventions	9
Text Symbols	9
Getting Help	11
HP Technical Support	11
HP Storage Website	11
HP Authorized Reseller	11
1 Installation	13
Installation Overview	13
Verifying the System Requirements	14
Verify Management Station Requirements	14
Verify Web Client Requirements	14
Verify Disk Array Firmware Requirements	16
Verify Host Agent Disk Space Requirements for Path Connectivity	16
Verify Host Bus Adapter Support for Path Connectivity	17
Verify Command Line Interface (CLI) Requirements	25
Installing Command View	26
Implement the Recommended Network Configuration	26
Set Up Ports to Bypass a Network Firewall	27
Using Multiple LAN Cards	27
Verify the Host System Name	28
Install SSL for Secure Communication (Optional)	29
Install the SNMP Service	29
Verify the SNMP Configuration	30

Install Remote Control (XP256 Only)	30
Install Command View	33
Modify or Repair Command View	36
Uninstall Command View	37
Verify Command View Services	37
Verify Command View Execution	38
Set Up SMI-S XP	38
Set Up Event Notification and History Reporting	45
Setting Up Command View	46
Migrate Data, Settings, and Preferences from a Different Management Station	46
Disable the Web Proxy Service	47
Verify the Internet Explorer Browser Requirements and Configuration	48
Verify the Netscape or Mozilla Browser Requirements and Configuration	49
Change the Session Timeout Value	50
Add Disk Arrays to Command View	51
Install License Keys	52
Set Up Auto LUN (XP48/XP512 Only)	52
Install the Command View Command Line Interface (CLI)	53
Setting Up Path Connectivity	54
Add Switches through Path Connectivity	54
Install Path Connectivity Host Agents	55
Add or Remove Host Agent Installation Files	61
Verify Data Collection from Disk Arrays, Hosts and Switches	62
Install the Path Connectivity Command Line Interface (CLI)	62
Integrating Snap-In Modules into Command View	63
HP StorageWorks Performance Advisor XP	63
HP StorageWorks Application Policy Manager	63
Integrating Command View with Other Platforms	64
Integrating with HP OpenView Storage Area Manager	64
Integrating with Miscellaneous Management Applications	65
2 Troubleshooting	67
Unable to Start Command View	67
General Command View Connection Errors	69
Host Agent Deployment Errors	71

A Installation Checklist75

Index79

Figures

1 Example of a network with added security from a firewall 26

2 Verifying the public community name and its attributes 31

3 Configuring the SNMP service 32

4 Internet Options dialog box (Internet Explorer). 49

Tables

1 Document Conventions 9

2 Web client requirements 15

3 Host disk space requirements. 16

4 HP-UX, Solaris, and AIX host directory requirements 17

5 Supported HBAs 18

6 Command View installation process 33

7 Command View services 37

8 Providers.list properties 40

9 cim.properties parameters 40

10 Command View compatibility with Performance Advisor and Application
Policy Manager 63

11 Command View host agent compatibility with Storage Area Manager host agents 64



about this guide

This installation guide provides information to help you:

- Install Command View XP, Path Connectivity, and the snap-in modules.
- Set up the XP disk arrays.
- Integrate Command View XP with other platforms.

“About this Guide” topics include:

- [Overview](#), page 8
- [Conventions](#), page 9
- [Getting Help](#), page 11

Overview

This section covers the following topics:

- [Intended Audience](#)
- [Prerequisites](#)
- [Related Documentation](#)

Intended Audience

This book is intended for use by customers and HP authorized service providers who are experienced with the following:

- Disk array hardware and software.
- Storage systems.

Prerequisites

Before you complete the procedures in this installation guide, make sure you consider the items below.

- Read through the installation guide.
- Meet all the minimum installation requirements.
- Refer to the *readme.txt* file on the CD for any last minute announcements.

Related Documentation

In addition to this guide, HP provides corresponding information:

- *HP StorageWorks Command View XP Path Connectivity User Guide*
- *HP StorageWorks Command View XP Path Connectivity Command Line Interface (CLI) Reference Guide*
- *HP StorageWorks Command View XP for XP Disk Arrays User Guide*
- *HP StorageWorks Command View XP Command Line Interface (CLI) Reference Guide*
- Command View XP and Path Connectivity online help

Conventions

Conventions consist of the following:

- [Document Conventions](#)
- [Text Symbols](#)

Document Conventions

The document conventions included in [Table 1](#) apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key and field names, menu items, buttons, and dialog box titles	Bold
File names, application names, and text emphasis	<i>Italics</i>
User input, command and directory names, and system responses (output and messages)	Monospace font COMMAND NAMES are uppercase monospace font unless they are case sensitive
Variables	<monospace, italic font>
Website addresses	Blue, underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.



Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: <http://www.hp.com>.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP website: <http://www.hp.com/support/>. From this website, select the country of origin.

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

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: <http://www.hp.com>.

Installation



HP StorageWorks Command View XP is a disk array management platform for the XP family of disk arrays. This guide describes how to install Command View.

In addition to disk array management functions, Command View includes Path Connectivity functionality. Path Connectivity diagnoses and reports the status of connections between disk arrays and hosts that consume disk array storage space.

Both Command View and Path Connectivity have graphical user interfaces and command line interfaces.

Additional software (known as snap-in modules) can be purchased to expand Command View functions. They include HP StorageWorks Performance Advisor XP and HP StorageWorks Application Policy Manager.

Information about the integration of Command View with other management platforms such as HP OpenView is included in this user guide.

This chapter contains detailed descriptions of the installation procedures listed in [Installation Checklist](#) on page 75.

Installation Overview

Installing Command View involves the following tasks:

1. Verifying that you have met or exceeded the requirements for the management station, any clients, disk array firmware, host agent disk space, HBAs, and CLI.
2. Installing Command View on the management station.
3. Setting up Command View.
4. Setting up Path Connectivity.
5. If needed, integrating snap-in modules into Command View.
6. If needed, integrating Command View with other platforms.

Verifying the System Requirements

Refer to the *readme.txt* file on the Command View CD for the most current requirements and any last minute announcements.

Verify Management Station Requirements

The management station is the Windows-based host on which Command View is installed. Make sure the workstation that will serve as the Command View management station meets the minimum requirements.

- Processor: Minimum 800 MHz Pentium III PC. 2 GHz or greater recommended.
- Operating system: Windows Server 2003 (32-bit), Windows 2000 (Service Pack 4), or Windows NT 4.0 (Service Pack 6a) workstation or server.
- RAM: Minimum 1 GB RAM.
- Free disk space:
 - 2.5 GB free disk space (FAT or NTFS). *For security reasons, HP strongly recommends using NTFS.*
 - 30 MB free disk space per managed disk array.
 - If you plan to integrate other applications such as HP StorageWorks Performance Advisor XP, additional disk space will be required. Refer to the application's documentation for disk space requirements.
- VGA monitor with 256 colors or better.
- At least one LAN Card: If you have multiple LAN cards installed in the Command View management station, see [Using Multiple LAN Cards](#) on page 27 for important configuration information.
- Static IP address. Do not use a dynamic IP address.
- Web browser: Microsoft Internet Explorer 5.5 (SP2) or 6.0.
- Sun Java 2 Runtime Environment (JRE) 1.4.2. To download the JRE, go to: <http://java.sun.com/products/archive/j2se/1.4.2/index.html>.

Verify Web Client Requirements

The Web client is any computer used to access Command View through a Web browser. Make sure any computer used as a Web client uses the supported operating system, Web browser, and Java software.

Table 2: Web client requirements

Operating System	Supported Web Browsers	Supported JRE Plug-in ¹
Windows Server 2003 (32-bit)	Internet Explorer 6.0	JRE 1.4.2
Windows XP	Internet Explorer 6.0 (SP1)	JRE 1.4.2
Windows 2000 Windows NT 4.0	Internet Explorer 5.5 (SP2) or 6.0	JRE 1.4.2
HP-UX 11.00	Netscape Navigator 7.0	JRE/RTE 1.4.1.03 (see footnote) Runtime Plug-in (JPI) 1.4
HP-UX 11.11	Netscape Navigator 7.0 Mozilla 1.2.1.01	JRE/RTE 1.4.1.03 (see footnote) Runtime Plug-in (JPI) 1.4
HP-UX 11.23 (64-bit)	Mozilla 1.2.1.01	JRE/RTE 1.4.1.03 (see footnote) Runtime Plug-in (JPI) 1.4

1. If you plan to use Configuration File Loader or LDEV Guard, you need to install Java Web Start 1.2. For Windows, installing JRE 1.4.2 also installs Java Web Start 1.2. For HP-UX, the JRE/RTE 1.4.1.03 download also includes Java Web Start, but you need to install Java Web Start separately. For more information, see [Install Java Web Start](#) on page 50.

To download the supported JRE for Windows, go to:

<http://java.sun.com/products/archive/j2se/1.4.2/index.html>.

To download the supported JRE/RTE and JPI that have been certified for HP-UX, go to: <http://www.hp.com/products1/unix/java/>.

Note: If you install an earlier version of the JRE after installing the supported version, do not set the client browser to use the older JRE. Choosing the older JRE as the default JRE may cause Command View not to work correctly.

In addition to these requirements, also review the browser configuration requirements. For Internet Explorer, see [Verify the Internet Explorer Browser Requirements and Configuration](#) on page 48. For Netscape Navigator or Mozilla, see [Verify the Netscape or Mozilla Browser Requirements and Configuration](#) on page 49.

Verify Disk Array Firmware Requirements

Command View requires that the managed disk arrays have certain minimum firmware levels. For more information, please contact your HP support team representative.

Verify Host Agent Disk Space Requirements for Path Connectivity

If you plan to use Path Connectivity, verify that the host agent operating system and disk space requirements are met.

Path Connectivity host agents run on various hosts in your SAN that consume disk space. They are responsible for collecting data-to-LDEV mapping and host HBA information. The following table shows which operating systems are supported and the host disk space requirements for that operating system.

Table 3: Host disk space requirements

Operating System	Disk Space
Windows NT 4.0 (Service Pack 6a) Windows 2000 (Service Pack 4) Windows Server 2003 (32-bit and 64-bit)	50 MB
HP-UX 11.00 HP-UX 11.11 HP-UX 11.23 (32 and 64-bit)	146 MB
Solaris 8 Solaris 9	70 MB
AIX 4.3.3 AIX 5.1	72.5 MB
Red Hat Linux 7.1, 2.4.2 kernel (32-bit) Red Hat Linux Advanced Server 2.1, 2.4.9 kernel (32-bit) UnitedLinux 1.0, kernel 2.4.19 (32-bit) SuSE Linux Enterprise Server 8 (SLES8), 2.4.19 kernel (32-bit)	192 MB

Some hosts have additional directory space requirements. The following table shows which hosts and the minimum requirements.

Table 4: HP-UX, Solaris, and AIX host directory requirements

Directory	Disk Space Requirements (in MB)			
	HP-UX	Solaris	AIX	Linux
/opt	55	40	40	31
/etc	.5	.5	.5	.5
/var	88	26	95	42
/usr	N/A	N/A	106	N/A

On UNIX systems, the `tmp` directory is used during the Path Connectivity host agent deployment process. If your `tmp` directory does **not** have sufficient space for the installation, use your Volume Management System (e.g. Online JFS or Veritas) to extend the available disk space in the `tmp` directory. Failure to ensure that the `tmp` directory can accommodate the space requirements above may result in an installation failure.

Verify Host Bus Adapter Support for Path Connectivity

Path Connectivity supports the HP StorageWorks XP family of disk arrays and the HP B-series and M-series product lines of Fibre Channel switches. If you plan to use Path Connectivity, verify that you the HBA(s) you are using are supported.

The following table lists HBAs that HP has verified to work properly with Path Connectivity. Fibre Channel connectivity to XP disk arrays using these HBAs is subject to disk array firmware compatibility. Please consult your HP support representative for further questions.

For Path Connectivity to collect all necessary information about the HBA, you should install the HBA SNIA library provided by the HBA driver vendor.

Table 5: Supported HBAs

OS	HBA Model	HBA Driver	HBA Vendor
HP-UX 11.00	A3404A (1 GB), A3591B (1 GB), A3636A (1 GB), A3740A (1 GB)	PHKL_23939	HP
	A5158A (1 GB), A6684A (1 GB), A6685A (1 GB), A6795A (2 GB)	B.11.00.10	HP
HP-UX 11.11	A6826A (2 GB)	B.11.11.01	HP
	A6826A (2 GB), A9782A/A9784 (2 GB)	B.11.11.02	
	A3404A (1 GB), A3591B (1 GB), A3636A (1 GB), A3740A (1 GB)	B.11.11.03	HP
	A5158A (1 GB), A6684A (1 GB), A6685A (1 GB), A6795A (2 GB)	B.11.11.09	HP
HP-UX 11.23	A6795A (2 GB), A6826A (2 GB)	B.11.23.01	HP

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
Windows NT 4.0	HHBA5101C, HHBA5121A/B (1 GB), HHBA5221A/B	3.5.15.18	Agilent
	LP7000E (1 GB), LP8000 (1 GB), LP9000 (1 GB), LP9002 (2 GB), LP9002DC (2 GB), LP952 (2 GB), LP9802/LP9802DC (2 GB), LP982 (2 GB)	Models on left are supported by the following drivers: 4-4.82a4 (SNIA 1.8), 4-5.00a10-1 (SNIA 1.12.2.0), 4-2.13a4 (SNIA 1.8), 4-2.20a12-2 (SNIA 1.12.2.0)	Emulex
	D8602B (1 GB)	2.0.25.44	HP
	DS-KGPSA-CB (33 MHz)	4-4.82.a9 (SNIA 1.6), 4-4.82.a14 (SNIA 1.6) 4-4.82.a16 (SNIA 1.6)	HP
	FCA2101 (66 MHz), FCA2355	Models on left are supported by the following drivers: 4-4.82a9 (SNIA 1.6), 4-4.82a14 (SNIA 1.6), 4-4.82.a16 (SNIA 1.6)	HP
	FCA2408, FCA2404/FCA2404DC	4-4.82a16 (SNIA 1.6)	HP
	Persian 120186-B21 (66 MHz)	4.30.0.69 D	HP
	FCE-3210 (1 GB), FCE-6410 (1 GB), FCE2-6410 (1 GB), FCE2-6412 (1 GB)	3.1	JNI
	FCE-6460 (2 GB), FCE2-6560 (2 GB), FCX-6562 (2 GB), FCX2-6562 (2 GB)	5.1 (SNIA 2.0)	JNI
	Z3400 (1 GB)	1.0.12.14	JNI
	QLA2200F, QLA2202F, QLA2204F, QLA2300F (2 GB), QLA2302F (2 GB), QLA2310F (2 GB/66 MHz), QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz)	Models on left are supported by the following drivers: 8.1.5.12 (SNIA 1.27.06), 8.1.5.15 (SNIA 1.27.13)	QLogic

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
Windows 2000	HHBA5101C, HHBA5121A/B (1 GB), HHBA5221A/B	3.5.15.18	Agilent
	LP7000E (1 GB), LP8000 (1 GB), LP9000 (1 GB), LP9002 (2 GB), LP9002DC (2 GB), LP952 (2 GB), LP9802/LP9802DC (2 GB), LP982 (2 GB)	Models on left are supported by the following drivers: 5-4.82a4 (SNIA 1.8), 5-5.00a10-1 (SNIA 1.12.2.0), 5-2.13a4 (SNIA 1.8), 5-2.20a12-2 (SNIA 1.12.2.0)	Emulex
	D8602B (1 GB)	2.0.25.44	HP
	DS-KGPSA-CB (33 MHz), FCA2101 (66 MHz), FCA2355	Models on left are supported by the following drivers: 5-4.82a9 (SNIA 1.6), 5-4.82a14 (SNIA 1.6), 5-4.82a16 (SNIA 1.6)	HP
	FCA2408, FCA2404/FCA2404DC	5-4.82a16 (SNIA 1.6)	HP
	FC2214/FCA2214DC, FC Mezzanine Card for BL20P	Models on left are supported by the following drivers: 5-8.2.0.72 (SNIA 1.27.15.0), 5-8.2.0.73 (SNIA 1.27.15.0)	HP
	Persian 120186-B21 (66 MHz)	5.14.4.69 B	HP
	FCE-3210 (1 GB), FCE-6410 (1 GB), FCE2-6410 (1 GB), FCE2-6412 (1 GB)	3.1	JNI
	FCE-6460 (2 GB), FCE2-6560 (2 GB), FCX-6562 (2 GB), FCX2-6562 (2 GB)	5.1 (SNIA 2.0)	JNI
	Z3400 (1 GB)	1.0.12.14	JNI
	QLA2200F, QLA2202F, QLA2204F, QLA2300F, QLA2302F	8.1.5.12 (SNIA 1.27.06)	QLogic
	QLA2200F, QLA2202F, QLA2204F	8.1.5.15 (SNIA 1.27.13)	QLogic
	QLA2310F (2 GB/66 MHz), QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz)	Models on left are supported by the following drivers: 8.2.0.10 (SNIA 1.27.12), 8.2.2.10 (SNIA 1.27.15)	QLogic

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
Windows Server 2003 (32-bit and 64-bit)	LP9002 (2 GB), LP9002DC (2 GB), LP952 (2 GB), LP9802/LP9802DC (2 GB), LP982 (2 GB)	Models on left are supported by the following drivers: 5-5.00a10-1 (SNIA 1.12.2.0) (32-bit), 5-2.20a12-2 (SNIA 1.12.2.0) (32-bit)	Emulex
	LP9802 (2 GB), LP9802DC(2 GB), LP982 (2 GB)	6-5.00a11-1 (SNIA 1.5.20) (64-bit)	Emulex
	DS-KGPSA-CB (33 MHz) FCA2101 (66 MHz), FCA2355	Models on left are supported by the following drivers: 5-4.82a14 (SNIA 1.6) (32 bit), 5-4.82a16 (SNIA 1.6) (32 bit)	HP
	FCA2408, FCA2404/FCA2404DC	Models on left are supported by the following drivers: 5-4.82a16 (SNIA 1.6) (32-bit), 6-5.00a.11 (64-bit)	HP
	FC2214/FCA2214DC, FC Mezzanine Card for BL20P	Models on left are supported by the following drivers: 5-8.2.0.72 (SNIA 1.27.150) (32-bit), 5-8.2.0.73 (SNIA 1.27.15.0) (32-bit)	HP
	QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz)	Models on left are supported by the following drivers: 8.2.0.10 (SNIA 1.27.12) 32-bit), 8.2.2.10 (SNIA 1.27.15) (32-bit)	QLogic

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
Red Hat Linux 7.1 (2.4.2 kernel)	167433-B21 (64 Bit), FC2214/FCA2214DC, FC Mezzanine Card for BL20P	6.04.00	HP
	LP7000E(1GB), LP8000 (1 GB), LP9000 (1 GB), LP9002 (2 GB), LP9002DC (2 GB), LP952 (2 GB), LP9802 (2 GB), LP9802DC(2 GB) LP982 (2 GB)	Models on left are supported by the following drivers: 4.20p (SNIA 1.3) 4.21g	Emulex
	QLA2200F, QLA2202F, QLA2204F, QLA2300F, QLA2302F, QLA2310F, QLA2340, QLA2342	5.38.9	QLogic
	QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz), QLA2200F, QLA2202F, QLA2204F, QLA2300F, QLA2302F, QLA2310F	4.03 (SNIA 2.01), 4.06 (SNIA 2.02), 4.08 (SNIA 2.02), 5.38.9	QLogic
Red Hat Linux Advanced Server 2.1 (2.4.9 kernel)	LP9002 (2 GB), LP9002DC (2 GB), LP952 (2 GB), LP9802 (2 GB), LP9802DC(2 GB) LP982 (2 GB)	Models on left are supported by the following drivers: 4.20p (SNIA 1.3), 4.21g	Emulex
	FC2214/FCA2214DC, FC Mezzanine Card for BL20P	6.04.00	HP
	QLA2310F, QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz)	6.01.00	QLogic
	QLA2310F, QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz)	6.04.00	QLogic

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
SuSE Linux Enterprise Server 8 (SLE8) (2.4.19 kernel)	LP9002 (2 GB), LP9002DC (2 GB), LP952 (2 GB), LP9802 (2 GB), LP9802DC (2 GB), LP982 (2 GB)	Models on left are supported by the following drivers: 4.20p (SNIA 1.3), 4.21g	Emulex
	FC2214/FCA2214DC, FC Mezzanine Card for BL20P	6.04.00	HP
	QLA2310F, QLA2340 (2 GB/133 MHz), QLA2342 (2 GB/133 MHz)	6.04.00	QLogic

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
Solaris 8 or 9	LP7000E (1 GB), LP8000 (1 GB), LP8000S (1 GB), LP9002S (2 GB), LP9802 (2 GB), LP9802DC(2 GB)	Models on left are supported by the following drivers: 5.00i (SNIA 1.3), 5.01e-1 (SNIA 1.6a)	Emulex
	FCA2257s	Model on left is supported by the following drivers: 3.26, 4.11 SNIA v2.0	HP
	FCA2257c, FCA2257p (64 bit) 254457-B21 (64 Bit)	Models on left are supported by the following drivers: 3.26T, 4.11	HP
	FCE-3210(1 GB), FCE-6410 (1 GB), FCE2-6410 (1GB), FCE2-6412 (1GB)	Models on left are supported by the following drivers: 4.1.3 (SNIA 2.0), 4.1.5 (SNIA 2.0)	JNI
	FCE-6460 (2 GB), FCE2-6560 (2 GB), FCX-6562 (2 GB), FCX2-6562 (2 GB), FCC-6460 (2 GB), FCC2-6560 (2 GB)	Models on left are supported by the following drivers: 5.1.1 (SNIA 2.0), 5.2.1 (SNIA 2.0), 5.3.0.1 (SNIA 2.0)	JNI
	QLA2200F, QLA2202F, QLA2204F, QLA2300F, QLA2302F, QLA2310F, QLA2340, QLA2342	4.03 (SNIA 2.01)	QLogic
	QLA2200F, QLA2202F, QLA2204F, QLA2310F, QLA2340, QLA2342	4.08 (SNIA 2.02)	QLogic
	QLA2300F, QLA2302F	4.06 (SNIA 2.02)	QLogic
	X6730A (1 GB), X6799A (1 GB), X6767A (2 GB)	11.8.0	Sun

Table 5: Supported HBAs (Continued)

OS	HBA Model	HBA Driver	HBA Vendor
AIX 4.3.3	197819-B21	1.5.20.2, 1.5.23.2, 1.5.24.1	HP
	7026-6H1-6228 (1 GB)	4.3.3.75	IBM
AIX 5.1	7026-6H1-6228 (1 GB)	5.1.0.15, 5.1.0.35	IBM
	7026-6H1-6239 (2 GB)	5.2.0.10	IBM

Verify Command Line Interface (CLI) Requirements

If you are installing the Command View Command Line Interface (CLI) and/or Path Connectivity Command Line Interface (CLI), verify the minimum requirements are met:

- The CLI client version of Command View must be the same version as the version installed on the Command View management station.
- Be sure that JRE 1.4.2 (Windows) or JRE/RTE 1.4.1.03 (HP-UX) is installed on the client platform (the system from which you run the CLI). Other operating systems or JRE versions are not supported.
- The CLI client platform must have network connectivity to the Command View management station.
- To run the CLI from a telnet session using a command prompt window, use a command prompt window that supports the X Windows function, such as Reflection X, or use the command line login method, such as `e2ecli -p user/user`.

Installing Command View

Implement the Recommended Network Configuration

Before installing Command View, complete the following recommendations. Failure to follow these recommendations may result in unauthorized access to the SVP.

1. The SVP should never be connected to the Internet.
2. HP recommends an SVP network separate from the corporate intranet. To implement this:
 - Install a firewall using a router or firewall software on a separate workstation with two LAN cards, one LAN card for a separate network to the SVP and the other for connecting to the intranet (see [Figure 1](#)).
 - If you are using firewall software, also consider installing antivirus software on the same machine.
 - The firewall needs to allow only the ports mentioned in [Set Up Ports to Bypass a Network Firewall](#) on page 27.

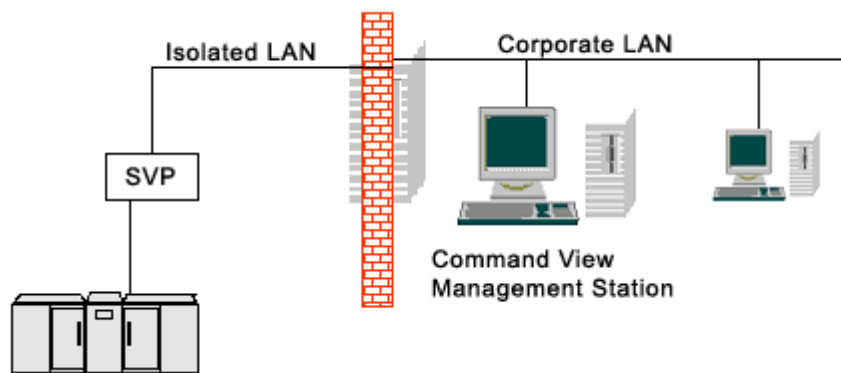


Figure 1: Example of a network with added security from a firewall

3. If an additional firewall separating the management station and GUI clients is required, make sure that the GUI clients can communicate with the management station and SVP for certain content. Some access is required for each XP128/XP1024 GUI client. Follow the instructions discussed in [Set Up](#)

[Ports to Bypass a Network Firewall](#) to set up port access, except do not allow access to port 161 for SNMP. Also, provide access to port 443 for https, if using SSL.

Set Up Ports to Bypass a Network Firewall

When placing XP disk arrays behind a firewall, open certain ports to enable access by the Command View management station and clients.

The Command View management station needs access through the firewall to the disk array. The Command View management station communicates with the XP48/XP512 (SVP) using SNMP and with the XP128/XP1024 (SVP) using TCP/RMI.

For the XP128/XP1024, Command View GUI clients establish communication directly to the array for some of the content. Access through the firewall is needed for each XP128/XP1024 GUI client.

To support Command View access through the firewall, you must allow access to the following ports.

For an XP128/XP1024:

- Port 80 for http, for all Command View GUI clients and the Command View management station if also used as GUI client.
- Ports 1099, 51099, and 51100 for TCP/RMI, for all Command View GUI clients and Command View management station.
- Port 162 for SNMP Trap, outgoing only from the disk array/SVP.

For an XP48/XP512:

- Port 161 for SNMP.
- Port 162 for SNMP Trap, outgoing only from disk array/SVP.

Using Multiple LAN Cards

If you have multiple LAN cards installed in the Command View management station, you must:

- Configure the first LAN card to communicate with the hosts and Command View API clients on the SAN.
- Modify the `SERVER_HOST` parameter in the `APIServer.cfg` file to point to the first LAN card.

To set the LAN card as the first network card, modify the bindings order of the network adapters to bind that network card first. To modify the connection bindings order, you must be logged on as a member of the Administrators group.

To modify the connection bindings order on Windows NT:

1. Open the Network properties dialog box by going to the Control Panel in Windows and choosing **Network**.
2. Click the **Bindings** tab.
3. From the **Show Bindings for** drop-down list, click **All adapters**.
4. Click the connection you want to move, and then click **Move Up** or **Move Down** to change the order.
5. Click **OK** to save your changes.

To modify the connection bindings order on Windows 2000 or Windows Server 2003:

1. Open the Network and Dial-up Connections window by right-clicking the **My Network Places** icon on the desktop and then choosing **Properties**.
2. From the **Advanced** menu, click **Advanced Settings**.
3. Click the connection you want to move, and then click the up or down arrow button to change the order.
4. Click **OK** to save your changes.

Verify the Host System Name

The host system name should not contain spaces or non-alphanumeric characters.

To confirm or modify the system name:

1. From the Control Panel in Windows, click **System**.
2. Depending on your version of Windows, click the **Network Identification** tab or the **Computer Name** tab to display the system name.
3. To modify the system name, click **Properties** (Windows NT or Windows 2000) or **Change** (Windows Server 2003).
4. Enter a new system name and click **OK** to save your changes.

Install SSL for Secure Communication (Optional)

Command View uses the Apache Web Server, which supports secure communication using SSL. However, some manual configuration is required. The default Command View installation is non-SSL.

Refer to the *Apache Web Server SSL Configuration for Command View Applications* white paper (*hpss_apache_whitepaper.pdf*) for SSL configuration instructions. The file is located in two places:

- The root directory of the Command View installation CD.
- In Command View, under the **Support > Reference Documents** menu item.

Install the SNMP Service

If you are integrating Command View with another application that will receive events from Command View, be sure that the SNMP service is installed on the Command View management server.

To install the SNMP service on Windows NT 4.0:

1. From the Control Panel in Windows, click **Network > Services**.
2. Click **Add**.
3. Click **SNMP Service**.
4. Click **OK**.

If Windows NT Setup requests the I386 folder, enter the location, usually `C:\I386`. In some cases you must insert the Windows NT product CD and enter its location: `<drive>:\i386`.

5. Click **Continue**.
6. Reboot the PC.
7. Verify the SNMP service as described in the next section.

To install the SNMP service on Windows 2000 or Windows Server 2003:

1. From the Control Panel in Windows, click **Add/Remove Programs > Add/Remove Windows Components**.
2. Highlight the “Management and Monitoring Tools” entry **without** selecting the check box.
3. Click **Details** in the lower right corner of the window.
4. Select the **Simple Network Management Protocol** check box.

5. Click **OK**. You may be required to insert Windows product CD.
6. Click **Next**.
7. Click **Finish**.
8. Verify the SNMP service as described in the next section.

Verify the SNMP Configuration

To verify the configuration:

1. From the Control Panel in Windows, click **Network > Services** (Windows NT) or **Administrative Tools > Services > SNMP Services** (Windows 2000 or Windows Server 2003).
2. Verify that “SNMP Services” and “SNMP Trap” are displayed in the Network Services list and running.

Install Remote Control (XP256 Only)

If you are not managing an XP256, skip this section.

Command View must communicate with Remote Control to manage the XP256. Use the installation instructions provided with Remote Control to install it. Be sure to install the Remote Control software version associated with the installed firmware. For more information, please contact your HP support team representative.

The SNMP protocol is used and must be configured as described below for proper operation of Command View.



Caution: Remote Control **cannot** reside on the Command View management station. It must be installed on a separate PC. When installing Remote Control, be sure that both the SNMP and SNMP Trap services are enabled.

Remote Control is supported only on PCs running Windows NT 4.0 SP4 or later.

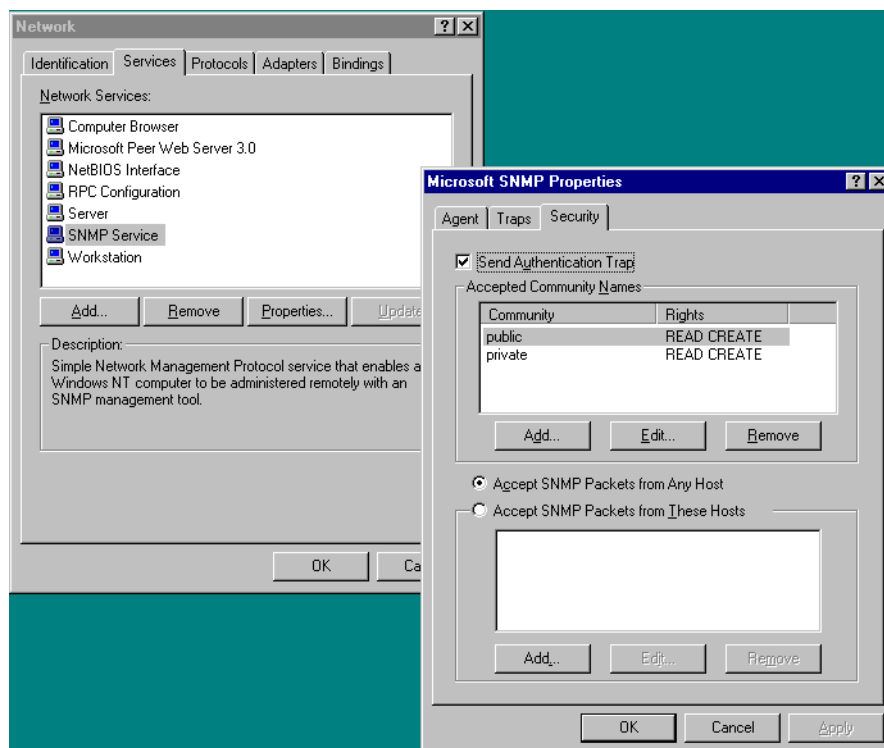
Verify the SNMP Configuration on Remote Control (XP256 Only)

If you are not managing an XP256, skip this section.

Verify that the Microsoft SNMP service is enabled on the PC executing Remote Control.

To verify the service is enabled on Windows NT 4.0:

1. From the Control Panel in Windows, click **Network > Services**.
2. Double-click **SNMP Services**.
3. Click the **Security** tab.

**Figure 2: Verifying the public community name and its attributes**

4. In the Accepted Community Names list, verify that one of the entries consists of the **public** community name with the **READ CREATE** attribute. If one does not exist, create it, apply the changes, and exit back to the Windows desktop.
5. From the Control Panel in Windows, click **Services**.
6. Double-click **SNMP** in the Services dialog box.
7. Verify that the Startup type is set to **Automatic**.

- Verify that the **System Account** option is selected and enable **Allow Service to Interact with Desktop** by selecting the check box.

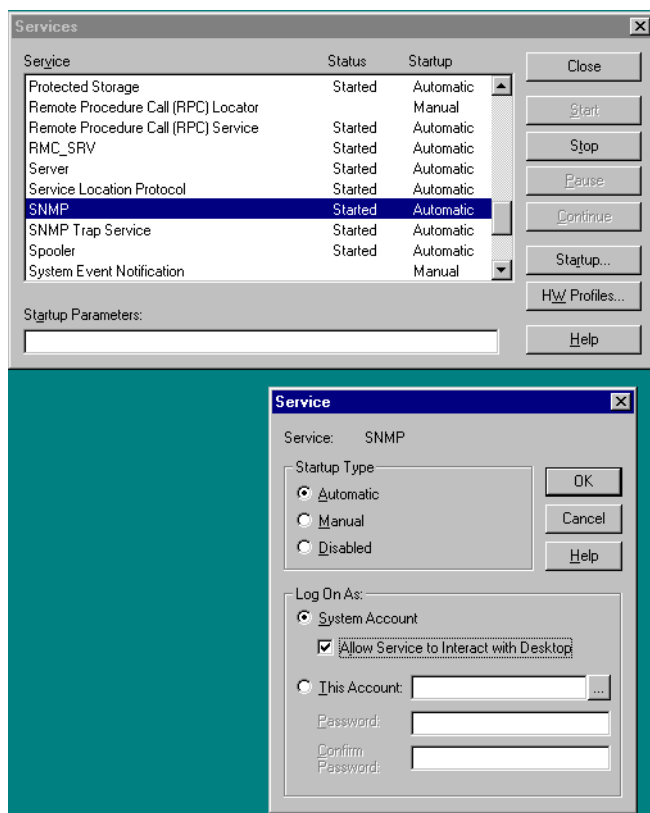


Figure 3: Configuring the SNMP service

- Click **OK**.
- Stop and start the SNMP service.
- Verify that the SNMP and the SNMP Trap Services are running and then exit back to the Windows desktop.

Install Command View

Refer to the following table to determine how to install Command View XP 1.8A.

Table 6: Command View installation process

If you have this version of Command View installed...	Action
Command View XP 1.11 or earlier	Refer to Uninstall Command View XP 1.11 or Earlier on page 33, and then follow the instructions in Installing Command View XP 1.8A on page 33.
Command View XP 1.30.00 or later	Refer to Upgrading from Command View XP 1.30.00 or Later to Command View XP 1.8A on page 35.
Command View XP is not currently installed	Follow the instructions in Installing Command View XP 1.8A on page 33.

Uninstall Command View XP 1.11 or Earlier

If you have Command View XP 1.11 or an earlier version installed, remove it before installing Command View XP 1.8A.

To uninstall Command View XP 1.11 or earlier:

1. From the Control Panel in Windows, click **Add/Remove Programs**.
2. Click **HP SureStore E Command View XP**.
3. Click **Remove**.
4. Install Command View 1.8A.

Installing Command View XP 1.8A

The following instructions explain how to install Command View XP 1.8A. If you have Command View XP 1.11 or an earlier version installed, you must uninstall the older version before installing Command View XP 1.8A. If you currently have Command View XP 1.30.00 or later installed, refer to [Upgrading from Command View XP 1.30.00 or Later to Command View XP 1.8A](#) on page 35.

To install Command View XP 1.8A:

1. Insert the Command View CD in the CD drive.
2. The CD browser menu should start automatically. If not, run *launch.exe* located on the CD.

3. From the CD browser menu, click **Install Command View XP**.

Note: Some of the links on the CD browser menu will not work until after installing Command View.

4. Click **Continue Install**.
5. Click **Next**.
6. Read the Software License Agreement and click **Yes**.
7. After viewing the System Recommendation dialog box, click **Next**.
8. If you have previously installed Command View XP 1.51 or later, you can preserve user-entered Path Connectivity data (hosts, switches, etc.) by installing in the same directory. To search for previous Command View installations, click **Yes**. To skip this step, click **No**.
9. At the **Destination Location** field, click **Next** to accept the default destination folder (C : \hps\$) or the application home found in the previous step. To choose a different folder, click **Browse**.
10. At the Setup Type dialog box, accept the Typical selection (default) and click **Next**.
11. Choose the operating systems that your hosts will be running and click **Next**.
12. The installation wizard asks for the management station's host name or IP address. If you have multiple LAN cards configured in the management station, enter the IP address of your corporate LAN and click **Next**.
13. Click **Next** to accept the default program folder.
14. The setup program transfers application files to the destination folder and configures Command View. When complete, click **Finish**.
15. Leave the CD in the CD drive and reboot the Command View management station.
16. After rebooting your computer, click **View Quick Start Guide** from the CD browser menu.

Upgrading from Command View XP 1.30.00 or Later to Command View XP 1.8A

If you currently have Command View XP 1.30.00 or later installed, upgrade from your previous version by completing the instructions in this section.

To upgrade from Command View XP 1.30.00 or later to Command View XP 1.8A:

1. Insert the Command View CD in the CD drive.
2. The CD browser menu should start automatically. If not, run *launch.exe* located on the CD.
3. From the CD browser menu, click **Install Command View XP**.
4. Click **Continue Install**.
5. The setup program detects a previous version of Command View. When asked to uninstall it, click **Yes**.
6. Click **Yes** to confirm.
7. After Command View has been uninstalled successfully, a confirmation dialog box is displayed. Click **OK**.
8. When asked to reboot, click **Yes**. The setup restarts automatically after the computer reboots.
9. Click **Next** to continue installing the application.
10. Read the Software License Agreement and click **Yes**.
11. After viewing the System Recommendation dialog box, click **Next**.
12. At the Setup Type dialog box, accept the Typical selection (default) and click **Next**.
13. Choose the operating systems that your hosts will be running and click **Next**.
14. The installation wizard asks for the management station's host name or IP address. If you have multiple LAN cards configured in the management station, enter the IP address of your corporate LAN and click **Next**.
15. Click **Next** to accept the default program folder.
16. The setup program transfers application files to the destination folder and configures Command View. When complete, click **Finish**.
17. Leave the CD in the CD drive and reboot the Command View management station.
18. After rebooting your computer, click **View Quick Start Guide** from the CD browser menu.

Modify or Repair Command View

Use the Modify option to install or uninstall components. Use the Repair option to reinstall Command View.

To modify or repair Command View XP 1.8A:

1. Insert the Command View CD in the CD drive.
2. The CD browser menu should start automatically. If not, run *launch.exe* located on the CD.
3. From the CD browser menu, click **Install Command View XP**.
4. Click **Continue Install**.
5. Click **Next**.
6. To modify Command View:
 - a. Click **Modify** and click **Next**.
 - b. Select the check boxes next to the components you want to install and clear the check boxes next to the components you want removed.
 - c. Click **Next**.
 - d. The setup program transfers and/or removes application files to and from the destination folder, and configures Command View. When complete, click **Finish**.
 - e. Reboot the Command View management station.
7. To repair Command View:
 - a. Click **Repair** and click **Next**.
 - b. The setup program transfers application files to the destination folder and configures Command View. When complete, click **Finish**.
 - c. Reboot the Command View management station.

Uninstall Command View

Complete the following instructions only if you need to uninstall Command View.

To uninstall Command View XP 1.8A:

1. From the Control Panel in Windows, click **Add/Remove Programs**.
2. Click **HP StorageWorks Command View XP**.
3. Click **Remove**.
4. Click **OK**.

Verify Command View Services

Verify that all the necessary Command View services are running. To view the services, from the Control Panel in Windows, click **Services** (for Windows NT) or **Administrative Tools > Services** (for Windows 2000 or Windows Server 2003).

Note: If you have elected **not** to install the Hpss Apache server (you installed the Apache Secure Socket Layer (SSL) server instead), the setup program will continue to install and configure the Hpss Apache files and service, but will not start the Hpss Apache service. For further instructions about installing an SSL-enabled (non-Hpss) Apache server, refer to the document *hpss_apache_whitepaper.pdf* located in the root directory of the Command View CD or under the **Support** tab in Command View.

The following table shows which services you need to verify.

Table 7: Command View services

Component	Service Name	Process Name(s)
Apache Web Server	HpssApache	<i>apache.exe</i>
Command View Trap Distributor	HpssCVTrapDistributor	<i>JWrapper_CVTrapdistributor.exe</i> <i>HpssCVTrapdistributor.exe</i>
Solid Database	HpssDb	<i>solid.exe</i>
Command View Management Server	HpssCVManagementServer	<i>JWrapper_CVManagementserver.exe</i> <i>HpssCVManagementserver.exe</i>
Command View Data Collector Service	HpssDataCollectorService	<i>JWrapper_DataCollectorService.exe</i> <i>HpssDataCollectorService.exe</i>

Table 7: Command View services

Component	Service Name	Process Name(s)
Array Manager servlet engine	HpssDMTomcat	<i>HpssDMTomcat.exe</i> <i>java.exe</i>
Path Connectivity servlet engine	HpssE2ETomcat	<i>HpssE2ETomcat.exe</i> <i>java.exe</i>
Command View Proxy SubAgent	HpssCVSubAgent	<i>JWrapper_CVSubAgent.exe</i> <i>HpssCVSubAgent.exe</i>
SMI-S XP Service See Set Up SMI-S XP on page 38.	hp StorageWorks SMI-S CIMOM hp SMI-S array providers Service Location Protocol	<i>hpSMIS_CIMOMService.exe</i> <i>hpSMIS_LicenseFrameworkService.exe</i> <i>java.exe</i>

Verify Command View Execution

To verify that Command View is running correctly:

1. Start the Web browser.
2. Enter the IP address of the Command View management station into your browser. The Command View login window is displayed.
3. Enter **administrator** in the **User Name** field.
4. Enter **administrator** in the **Password** field.

The main menu is displayed, indicating that Command View is running correctly.

If you are unsuccessful logging in, refer to [Troubleshooting](#) on page 67.



Caution: Please note that you cannot manage an XP disk array with more than one Command View management station at a time.

Set Up SMI-S XP

SMI-S XP provides the WBEM interface for the management of the XP48, XP128, XP512, and XP1024. SMI-S XP is a component of Command View and runs as a service. The XP disk array is modeled per the SNIA Storage Management Initiative Specification (SMI-S) version 1.0.

If you are not planning to use SMI-S XP, skip this section and continue to the next section. Otherwise, complete this section to:

1. Verify the SMI-S XP installation.
2. Modify the configuration files.
3. Enable the services used for SMI-S XP.

This section also discusses how to enable SSL and view the certificates ([SSL Support](#) on page 43) and uninstall SMI-S XP ([Uninstalling SMI-S XP](#) on page 44) in case you need to complete these tasks. Additional information about SMI-S XP is available in the *HP StorageWorks SMI-S XP Release Notes*, which is located from the **Support** tab in Command View.

Installing SMI-S XP

SMI-S XP is installed during the Typical (default) Command View installation. If you installed Command View in custom mode, the **hp StorageWorks SMI-S XP Service** check box must be selected to install SMI-S XP.

To verify that the SMI-S XP installation was successful, check the following:

- **hp StorageWorks SMI-S CIMOM, Licensing framework for hp SMI-S array providers**, and **Service Location Protocol** should have been added under Services and **Service Location Protocol** should be running.
- The `\Program Files\Hewlett-Packard\SMI-S\cimom` directory should have been created.

Configuring SMI-S XP

The configuration files for setting up the SMI-S XP service are located in the `\Program Files\Hewlett-Packard\SMI-S\cimom` directory.

Modify the following set of configuration files as needed:

- *XPprovider.properties*: Used for configuring the provider.
- *cim.properties*: CIMOM related parameters for enabling SSL, JAAS, and so on.
- *JAAS.policy*: Used for configuring an access control list. Use the script file *UserAccountsManager.bat* to manage this file.

Use a text editor to modify the configuration files. After changing any of the configuration parameters, be sure to restart the hp StorageWorks SMI-S CIMOM service. You do not need to restart the Licensing framework for hp SMI-S array providers service.

XPprovider.properties

The *XPprovider.properties* file is used to configure the provider. Configure the file as shown in the following table.

Table 8: Providers.list properties

Item	Description
Apiserver	The server name where Command View runs (usually localhost).
UserName	The user name used to connect to Command View.
Password	The password used to connect to Command View.
PortNumber	The port where Command View runs.
Namespace	The name space supported by the provider. The default value is root/XP.

cim.properties

The *cim.properties* file is used for setting CIMOM related parameters used for enabling SSL, JAAS, and so on. Only the fields listed in the following table should be edited. Do not modify any of the fields **not** listed in the following table.

Table 9: cim.properties parameters

Field	Purpose
EnableBasicAuthorization ("true" or "false")	Set to "true" for the basic level of authentication and authorization. The default is "true."
EnableCompleteAuthorization ("true" or "false")	Set to "true" for complete authentication and authorization. Each command must be authorized before it can be executed. If EnableCompleteAuthorization is set to "true," then the value of EnableBasicAuthorization is ignored. The default is "false."
EnableSSL ("true" or "false")	Set to "true" to enable SSL encryption for the data exchanged between the SMI-S server and the client.

UserAccountsManager.bat

User accounts are organized into groups, and a set of permissions are assigned to each group using JAAS. To manage the user accounts, use the script file *UserAccountsManager.bat* located in the home directory, which is the directory where the CIM Object Manager is installed. Typically, it is in the `\Program Files\Hewlett-Packard\SMI-S\cimom` directory. To find the list of the supported switch options, run the script file with the `-h` option.

To list the available groups and users:

- Enter this command: `UserAccountsManager -LG`

There are no other input parameters. Currently, the groups available are Administrator and User. There are no commands to add or remove the groups. User accounts in the Administrator group have complete control of all operations. User accounts in the User group can only execute read-only operations.

To add a user:

- Enter this command: `UserAccountsManager -AU -G <Group> -U <UserName> -P <Password>`
where:
 - G is the group name for the user
 - U is the user name
 - P is the password for the user

Example: `UserAccountsManager -AU -G Administrator -U Tom -P Vanilla2`

The Group parameter is one of the groups listed by the `-LG` option. A user name can exist in only one group.

To change a user password:

- Enter this command: `UserAccountsManager -CP -U <UserName> -O <OldPassword> -N <NewPassword>`
where:
 - U is the user name
 - O is the old password of the user
 - N is the new password for the user

Example: `UserAccountsManager -CP -U Tom -O Vanilla2 -N Chocolate3`

To remove a user:

- Enter this command: `UserAccountsManager -DU -U <UserName>`
where:
 - U is the user name

Example: `UserAccountsManager -DU -U Tom`

To display the help:

- Enter this command: `UserAccountsManager -h`
where:
-h is help
Example: `UserAccountsManager -h`

Starting and Stopping SMI-S XP

By default, the SMI-S CIMOM and Licensing framework for hp SMI-S array providers services are not enabled. To use SMI-S XP, you must enable both services. There are three states to which you can set the services:

- If the service is enabled to start **automatically**, the service starts when the Command View services are started or restarted, or when the machine is started.
- If the service is enabled to start **manually**, the service starts when the Command View services are started or restarted, but it does not start when the machine is started.
- If the service is **disabled**, which is the default, the service does not start when the Command View services are started or restarted, or when the machine is started.

To enable the services:

1. From the Control Panel in Windows, click **Services** (for Windows NT) or **Administrative Tools > Services** (for Windows 2000 or Windows Server 2003).
2. First, double-click the Licensing framework for hp SMI-S array providers service to open the service's Properties dialog box. You must enable the Licensing framework for hp SMI-S array providers service before enabling the hp StorageWorks SMI-S CIMOM service.
3. From the **Startup type** drop-down list, click **Automatic** or **Manual**, and click **OK** to save your changes.
4. Next, double-click the hp StorageWorks SMI-S CIMOM service to open the service's Properties dialog box.
5. From the **Startup type** drop-down list, click **Automatic** or **Manual**, and click **OK** to save your changes.

To disable the services:

1. From the Control Panel in Windows, click **Services** (for Windows NT) or **Administrative Tools > Services** (for Windows 2000 or Windows Server 2003).
2. Double-click the Licensing framework for hp SMI-S array providers or hp StorageWorks SMI-S CIMOM service to open the service's Properties dialog box. You can disable the services in any order.
3. From the **Startup type** drop-down list, click **Disable**, and click **OK** to save your changes.
4. Repeat [step 2](#) and [step 3](#) to disable the other service.

To stop and immediately restart the hp StorageWorks SMI-S CIMOM service:

1. From the Control Panel in Windows, click **Services** (for Windows NT) or **Administrative Tools > Services** (for Windows 2000 or Windows Server 2003).
2. Right-click the hp StorageWorks SMI-S CIMOM service and click **Restart**.

Note: If you restart the Licensing framework for hp SMI-S array providers service for any reason, you must start the licensing framework for hp SMI-S array providers service before starting the hp StorageWorks SMI-S CIMOM service.

SSL Support

SMI-S XP uses an SSL server-side certificate to help clients communicate with the SMI-S server in a secured manner. A self-signed certificate, *hpSMIS.cert*, is packaged with SMI-S XP. The certificate is located in the `\Program Files\Hewlett-Packard\SMI-S\cimom` directory. The administrator can replace the certificate with a different certificate if necessary. Be sure to retain the certificate name (*hpSMIS.cert*).

To use SSL, you must place a copy of the certificate file in its trust store. A trust store is a repository of trusted certificates that are recognized by the client program. Once the SMI-S certificate is "trusted" by a client program, the client communicates with the SMI-S server using SSL. SSL helps secure the client server communication by providing clients with the ability to authenticate the entity claiming to be the SMI-S server, and also by protecting the integrity of the transmitted data.

Enable SSL by setting the `EnableSSL` property in the `cim.properties` file to true. This file is located in the `\Program Files\Hewlett-Packard\SMI-S\cimom` directory. Once `EnableSSL` is set to true, all the client connections will use the https protocol.

To issue the certificate:

1. Import the server certificate into the client trust store.
 - a. Copy the server certificate to the client system.
 - b. Use the Java keytool to import the certificate into the client trust store.

```
$ keytool -import -alias hpsmis -file hpSMIS.cert -keystore mytruststore
```
2. When prompted, enter a password. This password is required for modifying `mytruststore` in the future. If a trust store does not currently exist, the keytool creates the trust store and then imports the specified certificate.
3. To specify a truststore, in the client application command line enter:

```
-Djavax.net.ssl.trustStore
```

Example:

```
$ java -Djavax.net.ssl.trustStore=mytruststore  
<MyClient> <system> root/cimv2 5988 ssl
```

4. If the client application is written to update the trust store file programmatically, then enter the password used to create the truststore:

```
-Djavax.net.ssl.trustStorePassword
```

Example:

```
$ java -Djavax.net.ssl.trustStore=mytruststore  
-Djavax.net.ssl.trustStorePassword=wbem01  
<MyClient> <system> root/cimv2 5989 ssl
```

To view certificates in a certificate file:

- Enter this keytool command:

```
$keytool -printcert -file hpSMIS.cert
```

To view all the certificates in a truststore:

- Enter this keytool command:

```
$keytool -list -v -keystore mytruststore
```

Uninstalling SMI-S XP

SMI-S XP is uninstalled as part of the Command View uninstallation procedure.

Set Up Event Notification and History Reporting

To set up event notification and reporting, use the instructions located in Command View under **Support > Integrating HP StorageWorks Command View XP with Other Products**. By setting up event notification, Command View can display events, which is communicated to other management applications through SNMP traps. For additional information, also refer to [Integrating with Miscellaneous Management Applications](#) on page 65.

Setting Up Command View

Migrate Data, Settings, and Preferences from a Different Management Station

If you are moving from an existing management station to a new management station, use the Backup Utility to migrate Command View data, settings, and preferences. You can use this tool to preserve your data and configuration preferences when upgrading hardware by saving your existing settings and then restoring them on the new management station.

To use the Backup Utility, both management stations must have Command View 1.8 or later installed. This tool is not compatible with older versions of Command View. In addition, the Backup Utility does not save the Windows registry.

To migrate your data using the Backup Utility:

1. If necessary, upgrade to Command View 1.8 or later on the existing management station.
2. Click **Start > Programs > HP StorageWorks Command View XP > Backup Utility**. The Backup Utility window is displayed.
3. Complete the backup process:
 - a. Click **Backup**. The Open File dialog box is displayed.
 - b. Choose a location, such as a network drive or shared file system, to save the backup file and click **Open**. A confirmation dialog box is displayed.
 - c. Click **Yes** to proceed. The Backup Progress status window is displayed.
 - d. When the backup process is completed, the **Finished** button becomes available. Click **Finished**. A confirmation message is displayed.
 - e. Click **OK**.
4. If necessary, install or upgrade to Command View 1.8 or later on the new management station.
5. Complete the restore process:
 - a. Click **Restore**. The Open File dialog box is displayed.
 - b. Navigate to where the backup file is located and click **Open**. A confirmation dialog box is displayed.
 - c. Click **Yes** to proceed. The Restore Progress status window is displayed.

- d. When the restore process is completed, the **Finished** button becomes available. Click **Finished**. A confirmation message is displayed.
- e. Click **OK**.

To save or restore your data from the Windows command line:

- To save your files, enter %HPSS_HOME%\bin\backup <target-path>. The *target-path* is the location, such as a network drive or shared file system, to where you want to save the backup file.
- To save your files, enter %HPSS_HOME%\bin\restore <target-path>. The *target-path* is the location of the backup file.

Disable the Web Proxy Service

When you are managing an XP128/XP1024, disable the Web proxy on the client by completing one of the following:

- Internet Explorer only: Disable the proxy server in your browser,
or
- Internet Explorer, Netscape, or Mozilla: Add the XP128/XP1024 IP address to the list of excluded addresses (that are **not** to be directed through a Web proxy service).

Disabling Proxy Service in the Internet Explorer Browser

To disable the proxy service:

1. In Internet Explorer, click **Tools > Internet Options > Connections > LAN Settings**.
2. Clear the **Use a proxy server** check box.
3. Click **OK**. Click **OK** again to exit and save changes.

Adding the IP Address of the Disk Array to the List of Web Proxy Excluded Addresses

To add IP addresses in Internet Explorer:

1. In Internet Explorer, click **Tools > Internet Options > Connections > LAN Settings > Advanced**.
2. Enter the IP address of the disk array in the **Exceptions** box. If you are entering more than one IP address, use semicolons to separate each IP address.
3. Click **OK**. Click **OK** again to exit and save changes.

To add IP addresses in Netscape or Mozilla:

1. In Netscape or Mozilla, click **Edit > Preferences > Advanced > Proxies**.
2. Click **Manual Proxy Configuration**.
3. Enter the IP address of the disk array in the **No Proxy for** field. If you are entering more than one IP address, use commas to separate each IP address.
4. Click **OK** to exit and save changes.

Verify the Internet Explorer Browser Requirements and Configuration

If you are using Internet Explorer, complete the procedures in this section to verify that the browser options are set correctly and any additional configurations are made. If you are using Netscape or Mozilla, skip to the next section, [Verify the Netscape or Mozilla Browser Requirements and Configuration](#) on page 49.

Verify Internet Explorer Browser Settings

If you are using Internet Explorer for your Command View browser client sessions, verify that the browser options are set correctly.

To verify and set the browser options for Internet Explorer:

1. In Internet Explorer, click **Tools > Internet Options > Advanced**.
2. Verify that the following settings are enabled:
 - **Browsing > Disable script debugging**
 - **HTTP 1.1 settings > Use HTTP 1.1**
 - **HTTP 1.1 settings > Use HTTP 1.1 through proxy connections**
 - **Use Java 2 v1.4.2 for <applet> (requires restart)**

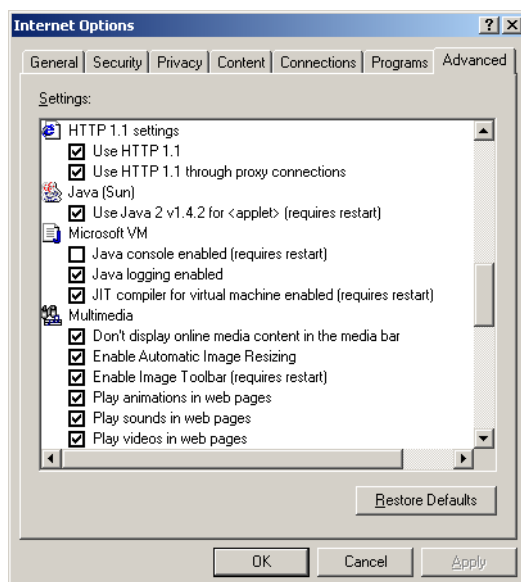


Figure 4: Internet Options dialog box (Internet Explorer)

3. Click **OK** to close the Internet Options dialog box and save your changes.

Verify the Netscape or Mozilla Browser Requirements and Configuration

If you are using Netscape or Mozilla for your Command View browser client sessions, verify that the correct JRE/RTE has been installed. You may also need to install Java Web Start.

Install Java on Clients Running Netscape or Mozilla on HP-UX

Verify that the correct Java software is installed on the client. For Command View to run correctly in Netscape or Mozilla, install both JRE/RTE 1.4.1.03 and JPI 1.4 for HP-UX on the computer running HP-UX. Download the software by going to <http://www.hp.com/products1/unix/java/>.

Install Java Web Start

If you are planning to use the Configuration File Loader or LDEV Guard, install Java Web Start 1.2 on the client computer. Java Web Start is a necessary component for using Configuration File Loader or LDEV Guard, and is part of the JRE/RTE 1.4.1.03 download. The Java Web Start file is located in the `jre` directory. To install Java Web Start 1.2, refer to the instructions in the release notes or go to http://www.hp.com/products1/unix/java/java2/webstart/infolibrary/notes_webstart_1-2.html.

Change the Session Timeout Value

After installing Command View, you may want to change the session timeout value. This value determines how long a session lasts after a user in Modify mode has not used the browser. The default is set to 60 minutes. To change the timeout, edit the `SESSION_TIMEOUT_PLAN` value in the *CommandView.properties* file.

To change the session timeout value:

1. Locate the *CommandView.properties* file in the `\hpss\dm\tomcat\webapps\hpstgmt\webroot\Stormgmt` directory.
2. Use a word processor or text editor to open the file. Look for the `SESSION_TIMEOUT_PLAN` setting by locating the following line:
`SESSION_TIMEOUT_PLAN=ONCE:60`
3. Replace `60` with the number of minutes you want a session to last before it times out due to inactivity. This setting is applicable to all XP disk arrays.
4. If you are managing an XP128/XP1024, also consider changing `ONCE` to `ALWAYS`. The default is `ONCE:60`.

Most users will want to choose the `ONCE` setting. Using this setting means that Command View checks the *CommandView.properties* file only once, when someone adds a device or restarts the server, and then sets the session timeout value at that time.

Certain users may find they need the flexibility of the `ALWAYS` setting, which ensures that Command View always determines the timeout value. Using this setting means that Command View checks the *CommandView.properties* file every time a user in Modify mode clicks a tab to manage an XP128/XP1024 (Identity and Status tabs excluded). You may want to consider using this setting if you or someone else needs to change the timeout value on the SVP,

but you want to override that when using Command View. Note that this setting adds an additional delay of approximately 45 seconds when loading a new screen.

If you are managing an XP48/XP256/XP512, Command View ignores the ONCE or ALWAYS setting because the ALWAYS setting is not available.

5. Save and close the file.
6. Restart Command View services by clicking **Start > Programs > HP StorageWorks Command View XP > Restart Services**.

Add Disk Arrays to Command View

To add disk arrays:

1. Start Command View.
2. Log on using **administrator** as the user ID and **administrator** as the password.
3. Click the **Device Administration** tab.
4. Enter the disk array's IP address in the **Agent IP Address** field.
For an XP256, enter the IP address of the computer running the Remote Control software. Each XP256 has a dedicated computer.
5. Press **Enter** or click **Submit**.
The **Serial Number**, **Product Type**, and **Product Number** fields are filled in automatically.
6. If the **Device Name** field is blank, enter a name for the disk array.
7. For an XP1024, click the left DKU type and right DKU type from the drop-down lists.
8. If the **Contact** and **Location** fields are blank, enter a contact name and a location.
9. Select the **Manage Array** check box. This check box is selected by default. If it is not selected, the disk array is added to Command View's list, but it will not be managed by Command View. No configuration data will be retrieved.
10. Click **Save** and then click **OK** to confirm. Repeat the previous steps to add more disk arrays.

Install License Keys

If you need to install any license keys that enable disk array product features such as Business Copy or Continuous Access, use the License Key Management (Install) screen in Command View to install them. For more information about license keys, refer to the *HP StorageWorks Command View XP User Guide*.

To install a license key:

1. Start Command View.
2. Log in, using **administrator** as the user ID and **administrator** as the password.
3. Click **Device Administration**. The Device Administration screen is displayed.
4. From the Device Administration screen, click **License Key Management**.
5. Click the disk array you want to access from the Serial Number column. The License Key Management main screen is displayed.
6. From the License Key Management main screen, click **Install**. The License Key Management (Install) screen is displayed.
7. Select the check box for each license key you want to install.
8. Enter the license key code(s).
9. Click **OK** to add the license key and return to the License Key Management main screen. Clicking **Cancel** returns you to the License Key Management main screen without installing the license.

Set Up Auto LUN (XP48/XP512 Only)

If you are using Auto LUN, set up the *DOParameters.cfg* file after installing the license key. Note that activating Auto LUN causes Command View to take significantly more time to retrieve data initially and after configuration changes for all XP48/XP512 disk arrays managed by the Command View server.

To set up Auto LUN on the Command View management station:

1. After installing the Auto LUN license key, locate the *DOParameters.cfg* file in the `\hpss\dm\tomcat\webapps\hpstmgmt\web-inf\cvapi\config` directory.
2. Use a word processor or text editor to open the file. Locate the following lines:

```
# Auto Lun enable/disable  
AUTO_LUN=OFF
```

OFF is the default setting (Auto LUN is not enabled).

3. Replace OFF with ON: `AUTO_LUN=ON`.
4. Save and close the file.
5. Restart Command View services by clicking **Start > Programs > HP StorageWorks Command View XP > Restart Services**.

Install the Command View Command Line Interface (CLI)

Command View has a Command Line Interface (CLI). Use the CLI to manage and monitor XP disk arrays from the operating system prompt of a system located anywhere on the network, including the Command View management station.

To download and install the CLI on the client:

1. Get the `cvcli.tar` file by navigating to the Command View **Support** tab. Click **Support > Download Page > Command View Command Line Interface (CV CLI) Download Section > CV CLI Client**.
2. Un-tar the file `cvcli.tar` to any location you want. For a Windows host, use WinZip 7.0 or later. For a UNIX host, use the command `tar xvf cvcli.tar`.
3. After you un-tar the file, the CLI components will be in `<your_path>/cvcli`. It doesn't matter where you un-tar the files, but all of the following files must be in the same directory:
 - `cli.jar`: CLI java classes.
 - `CVCLI.bat`: CLI execution Windows batch file.
 - `cvcli`: CLI execution UNIX script.
 - `CVCLI.properties`: CLI properties file.
 - `CVCLI.txt`: Installation instructions for the CLI client.
4. To complete the installation, follow the instructions found in the `CVCLI.txt` file.

Additional information about the CLI is in the *HP StorageWorks Command View XP Command Line Interface (CLI) Reference Guide*, located on the Command View CD, or from the **Support** tab in Command View.

Setting Up Path Connectivity

Path Connectivity identifies, maps, and diagnoses the connections (or paths) between your XP disk array and hosts that consumes storage on the disk array.

Path Connectivity is installed as part of the Command View installation, but it is not required to manage an XP disk array with Command View. However, you have to perform additional steps (primarily installing host agents) to make Path Connectivity active.

Path Connectivity runs on the Command View management station. Path Connectivity has a Command Line Interface (CLI) that can run on a host connected to the Command View management station.

Add Switches through Path Connectivity

Path Connectivity does not autodetect the switches in your SAN. Use the Path Connectivity Fibre Channel Switch Management screen to add switches.

To add switches:

1. Start Command View.
2. Click the **Path Connectivity** tab.
3. Click **Administration**.
4. Click **Switch Mgmt** in the navigation tree.
5. Enter the IP address or DNS name of the switch to be added in the **Enter IP Address or DNS name below** field.
6. Click **Add**. The list on the left displays the switch.
7. Repeat steps 5 and 6 until all switches are added.
8. Click **Apply**.

The Path Connectivity Data Collection Service will try to communicate with newly-added switches on its next scheduled switch polling cycle.

Install Path Connectivity Host Agents

Prerequisites

The following prerequisites are necessary for installing Path Connectivity host agents:

- One of the supported operating systems (see [Verify Host Agent Disk Space Requirements for Path Connectivity](#) on page 16).
- You must have administrator access to the remote host.
- The Command View management station must have a DNS name.
- A Linux host must be a rexec server (see page 57).
- Only one remote deployment tool may run at a given time.
- Review the online Host Software Installation checklist. To view the checklist, start the host agent deployment utility and click **Host Software Installation Checklist**. Click the link for the remote host's operating system.



Caution: Do not deploy Path Connectivity host agents and Command View SDM host agents to the same host system. They cannot coexist.

There are two ways to install Path Connectivity host agents:

- Use the Host Agent Deployment tool.
- Download the host agent to the remote host from the **Support** tab in Command View. Then, manually invoke the installation executable as described in [Installing or Updating Host Agents Using the Local Method](#) on page 60.



Caution: Please review the README file on the Command View CD to find a limitation regarding host agent installation.

Note: If your hosts already have CV 1.8 host agent installed, there is no need to update the CV 1.8 host agents. The CV 1.8A management station can communicate with the CV 1.8 host agents.

Preliminary Host Agent Installation Tasks

If you choose to use local install instead of remote deployment, you do not need to share the drive or set up services such as *rexec* and *rsh* on the hosts.

To prepare for installing on Microsoft Windows platforms:

1. Be sure you have root or superuser access to the system.
2. Share the system drive (for example, C\$).

To prepare for installing on UNIX platforms (HP-UX, Solaris, and AIX):

1. Be sure you have root or superuser access to the system.
2. Be sure the `exec/rexec` and FTP functions are enabled. On these platforms, the services should be enabled by default. For more details, consult the configuration instructions to enable `exec/rexec` from the corresponding operating system manual.
3. Configure the root/superuser account to allow remote access via the `exec/rexec` and FTP services.

To prepare for installing on UNIX platforms (Linux):

1. Be sure you have root or superuser access to the system.
2. Set up the `rexec` server on the Linux host. Verify that you have the `rsh` server package installed on the Linux host. For example, if you are using Red Hat Linux:
 - Enter `rpm -qa | grep rsh-ser*` at the command prompt.
 - If the command returns an entry, then go to [step 3](#).
 - If the command does not return an entry, install the package:
 - Insert the Red Hat CD in your CD-ROM.
 - Enter `rpm -Uvh /mnt/cdrom/RedHat/RPMS/rsh-ser*`. You may need to mount your CD-ROM if the OS cannot find the directory. The command `mount /dev/cdrom` should work.
3. Verify that the `rexec` service is started.
 - Enter `ntsysv` at command prompt.
 - Check the `rexec` and `rsh` services and click **OK**.
 - Restart the service by entering `service xinetd restart`.
 - Edit `/etc/pam.d/login`. Comment out (add “#” to the line):
`# auth required /lib/security/pam_securetty.so`
 - Edit `/etc/pam.d/rexec`. Comment out (add “#” to the line):
`# auth required /lib/security/pam_securetty.so`
 - Edit `/etc/pam.d/ftp`. Comment out (add “#” to the line):
`# auth required /lib/security/pam_listfile.so`
`item=user sense=deny file=/etc/ftpusers onerr=succeed`
 - Restart the service by entering `service xinetd restart`.

4. Configure the root/superuser account to allow remote access via the exec/rexec and FTP services.
 - Run the `/usr/sbin/ntsysv` command and enable `wu-ftpd`.
 - Edit `/etc/pam.d/ftp` by commenting out the following line with #:

```
auth required /lib/security/pam_listfile.so
item=user sense=deny file=/etc/ftpusers
onerr=succeed
```
 - Edit `/etc/ftpusers` by removing or commenting out the following line with #:

```
root
```
 - Edit `/etc/ftpd` as follows:

```
Change allow-uid ftp to allow-uid ftp root.
Change allow-gid ftp to allow-gid ftp root.
```
 - Run the `/sbin/service xinetd restart` command.

Installing or Updating Host Agents Using the Remote Deployment Tool

If a host agent with version 1.60 or later is already running on the host, update the host agent instead of installing it (see page 59).

To designate a single host:

1. Launch the remote deployment application by clicking **Start > Programs > HP StorageWorks Command View XP > Host Agent Deployment Tools > Install Host Agent**.
2. Add a single host by entering the host name or IP address, admin user name, and password.
3. Click **Add Host**.

To designate multiple hosts:

1. Launch the remote deployment application by clicking **Start > Programs > HP StorageWorks Command View XP > Host Agent Deployment Tools > Install Host Agent**.
2. Click **Add Multiple Hosts**. A dialog box displays a table.
3. In the table, enter the host name or the host name or IP address, admin user name, and password in their respective columns.
4. Click **Add All Hosts Now**.

To install the host agents:

1. The Managed Host list should now contain all the hosts previously added. From this list, click the hosts to which you want to deploy a host agent.
2. Click **Install on Selected Hosts**.

To uninstall the host agents using the Remote Deployment tool:

1. Launch the remote deployment application by clicking **Start > Programs > HP StorageWorks Command View XP > Host Agent Deployment Tools > Uninstall Host Agent**.
2. Click the hosts you want to remove from the Managed Host list.
If the Managed Host list does not contain the host agent you want to remove, manually add the host from the Add Single Host box, click **Add Host**, and then click the host from the Managed Host list.
3. Click **Uninstall from Selected Hosts**.

To update the host agents using the Remote Deployment tool:

Update the host agents only if you have a Command View XP 1.60 or later host agents already running on the host.

Note: The remote update feature is not supported for the Windows Host Agent. See page 60 to locally update the Windows Host Agent.

1. If the IP address of the management station being used to update the host is different from that of the management station used to install the existent host agent on the host, update the host agent access files (see the following procedure). Otherwise, go to step 2.
2. Launch the remote deployment application by clicking **Start > Programs > HP StorageWorks Command View XP > Host Agent Deployment Tools > Update Host Agent**.
3. From the Managed Host list, click the hosts you want to update.
If the Managed Host list does not contain the host agent you want to update, manually add the host from the Add Single Host box, click **Add Host**, and then click the host from the Managed Host list.
4. Click **Update on Selected Hosts**.

To update the host agent access files using the Remote Deployment tool:

By default, only the management station used to install the host agent has access to the host agent. If you want another management station to access the host, update the host access list by completing the following procedure.

1. Launch the remote deployment application by clicking **Start > Programs > HP StorageWorks Command View XP > Host Agent Deployment Tools > Update Host Agent Access File**.
2. From the Managed Host list, click the hosts you want to update.
If the Managed Host list does not contain the host you want to update, manually add the host from the Add Single Host box, click **Add Host**, and then click the host from the Managed Host list.
3. Click **Update Access on Selected Hosts**.

Installing or Updating Host Agents Using the Local Method**To download the host agent file:**

1. Access Command View from your workstation.
2. Click the **Support** tab.
3. Navigate to the Path Connectivity Host Agent Download section. A list of support host agents is provided.
4. Click the link for the desired host.
5. Download the *Host Agent tar* file (which contains all of the required software) to your computer.
6. FTP the *Host Agent tar* file to the `tmp` directory of the remote host.

To install or update the host agent locally:

1. Telnet to the remote host as root.
2. Navigate to the `tmp` directory.
3. Untar the host agent tar file by entering:
`tar -xvf hostagent_<os_name>.tar.`
4. Run the installation script:
UNIX: `unix_local_install.sh`.
Windows: `installha`.

To uninstall a host agent locally:

1. Telnet to the remote host as root.
2. Navigate to the `tmp` directory.
3. Untar the host agent tar file by entering:
`tar -xvf hostagent_<os_name>.tar.`
4. Run the uninstall script:
UNIX: `unix_local_uninstall.sh.`
Windows: `uninstallha.`

Add or Remove Host Agent Installation Files

If you have already installed Command View and Path Connectivity, but need to add or remove operating systems that your hosts will be running, complete the following procedures.

To install or uninstall host agent platform files on management station:

1. Insert the Command View CD in the CD drive.
2. From the Control Panel in Windows, click **Add/Remove Programs**.
3. Click **HP StorageWorks Command View XP**.
4. Click **Modify**.
5. Click **Next**.
6. Select or clear the check boxes next to the operating systems you want to install or uninstall, respectively.
7. Click **Next**.
8. Reboot the Command View management station.

Verify Data Collection from Disk Arrays, Hosts and Switches

Verify that Path Connectivity is working correctly by using the following procedure. After that, data is collected regularly on either a default schedule or a schedule you set.

To verify that Path Connectivity is working correctly:

1. Be sure the host agents are installed.
2. Be sure you have used Path Connectivity to add any switches.
3. Be sure the disk arrays you want to monitor have been added to Command View. Locate each disk array on the **Main > Device Administration** screen and be sure the **Manage Array** check box is selected.
4. If the Command View management station and the hosts are located on different subnets, use the **Path Connectivity > Administration > Host Discovery > Host Mgmt** screen to add the hosts.
5. Click **Administration > Data Collection > Collect Now**. Select all check boxes and click **Collect Now**.
6. Wait for 5-10 minutes. You should see new path connectivity data on the screens.

Install the Path Connectivity Command Line Interface (CLI)

Path Connectivity has a Command Line Interface (CLI). Use the Path Connectivity CLI to access path connectivity information from the system prompt of a system located anywhere in your network, including the Command View management station. *Path Connectivity CLI Installation Note*, which is located under the **Support** tab in Command View, has detailed installation instructions.

Integrating Snap-In Modules into Command View

This section provides additional information about integrating Performance Advisor (PA) and Application Policy Manager (APM) with Command View 1.8A. The following table shows which versions of PA and APM are compatible with Command View 1.8A.

Table 10: Command View compatibility with Performance Advisor and Application Policy Manager

Command View XP	Performance Advisor XP	Application Policy Manager XP
1.8A	1.7-2, 1.7A	3.0B

HP StorageWorks Performance Advisor XP

PA 1.7-2 can coexist with Command View 1.8A. For instructions on installing or upgrading PA on the Command View management station, refer to the PA documentation. The following items are some issues to consider:

- If you are upgrading PA, close all browser sessions of Command View and PA before performing the upgrade.
- Always use the JRE supported by Command View 1.8A.

Important: To solve any JRE compatibility issues, refer to the *readme.txt* file on the CD.

HP StorageWorks Application Policy Manager

APM 3.0B can coexist with Command View 1.8A. For instructions on installing APM on the Command View management station, refer to the APM documentation. The following items are some issues to consider:

- You must first install Command View before installing APM.
- After installing APM, initialize Path Connectivity if you didn't do so as part of the Command View installation. APM uses the SAN data that is collected and stored by Path Connectivity.

Integrating Command View with Other Platforms

Integrating with HP OpenView Storage Area Manager

Command View and Storage Area Manager should not be installed on the same management station. However, Storage Areas Manager provides a way for the users to run a browser to access Command View from a Storage Area Manager management station. Refer to the following instructions to run Command View from a Storage Area Manager management station.

Also, host agents with compatible versions of each software product can coexists on the same host. For more information, refer to [Coexistence of Command View and Storage Area Manager Host Agents](#) on page 64.

To run Command View from a Storage Area Manager management station:

1. Install Storage Area Manager. The *HP OpenView Storage Area Manager Installation Guide* provides the information to accomplish this task.
2. For Storage Area Manager 3.0 or earlier, install the DPI patch on the Storage Area Manager platform to integrate the disk arrays. To download the patch, go to <http://www.openview.com/products/dpi/index.html>. Installation instructions are provided with patch.
3. Refer to the Storage Area Manager documentation for further details on running Command View.

Coexistence of Command View and Storage Area Manager Host Agents

Only certain versions of the host agents from each software product can coexists on the same hosts. [Table 11](#) specifies the corresponding compatible versions.

Table 11: Command View host agent compatibility with Storage Area Manager host agents

Command View Version	Storage Area Manager Version
1.8A	3.1
1.7B	3.0 with patch SANMGR_00010
1.60.00 or 1.7A	3.0
1.51.00, 1.52.00, or 1.53.00	2.2, 2.2.1 with patch SANMGR_00006, or 2.2 with patch SANMGR_00007
1.40.04	2.2
1.40.01 or 1.30.00	2.1

Optional: Communicating with Storage Area Manager in an SSL Environment

If you are using Command View in SSL mode, refer to the Storage Area Manager documentation to properly link Command View to Storage Area Manager. In addition, additional information about SSL configuration is available under the **Support** tab in Command View.

Integrating with Miscellaneous Management Applications

The latest HP StorageWorks Command View integration information is available under the **Support** tab in Command View.

Integration can occur at the following levels:

- Graphical User Interface (GUI)
- Command Line Interface (CLI)
- Message or “event” notification using HP Enterprise Integrations or Trap Distributor

GUI Integration

Command View is a Web-based application. If an application supports a Web interface, you can configure it to reference the Command View URL.

CLI Integration

You can write scripts or batch files containing Command View CLI commands. Refer to the *HP StorageWorks Command View XP Command Line Interface (CLI) Reference Guide*. You can find this manual on the Command View CD or under Command View’s **Support > Reference Documents**.

Event Notification

Two tools are available to support the integration of Command View event notification messages into another applications: HP Enterprise Integrations and HP Trap Distributor. Installation and operation instructions for both tools are available under the **Support** tab in Command View.

Troubleshooting

2

This chapter contains troubleshooting information about installing, configuring, and logging on to Command View. This chapter also has suggestions for solving host agent installation and configuration problems. You will find recommended solutions to the following topics:

- [Unable to Start Command View](#) (page 67)
- [General Command View Connection Errors](#) (page 69)
- [Host Agent Deployment Errors](#) (page 71)

For other Command View troubleshooting topics, refer to the *HP StorageWorks Command View XP User Guide*. For troubleshooting information specific to Path Connectivity, refer to the *HP StorageWorks Command View XP Path Connectivity User Guide*.

Unable to Start Command View

Nothing happens when you try to start Command View or you are unable to start Command View.

Try the following solutions:

- Verify that all the Command View services are running in Command View management station.
- From the Control Panel in Windows, click **Services** and verify that all the Command View services have started.
- Verify that you are using the following URL:
<http://<Command View management station IP address>>.
- When managing the XP128/XP1024, disable the Web proxy on the client:
 - Disable the proxy server in your browser, **or**
 - Add the disk array IP address to the list of excluded addresses (that are **not** to be directed through a Web proxy service).

— For instructions, refer to [Disable the Web Proxy Service](#) on page 47.

- When managing the XP128/XP1024, Web applets are sent directly to the client browser bypassing the Command View management station. If your SAN topology includes firewall configurations, you must enable a connection through the firewall for each system that will attempt to monitor or manage the XP128/XP1024. For instructions, refer to [Verify Command View Services](#) on page 37.

A login failure message is displayed instead of a new login window.

You have probably entered an incorrect password and failed the first Command View login attempt. Close the browser and start a new one.

You have forgotten your password or the browser does not accept your password.

Assuming a default installation directory, go to `\hps\dm\tomcat\webapps\hpstmgmt\webroot\Stormgmt` and delete the *passwd.txt* file.

The browser displays the message, “Invalid user name or password,” but never displays a login box.

Your session authorization may have expired. The easiest way to resolve the problem is to close the Web browser displaying the error and restart your management session in a new Web browser.

If your session has expired, consider changing the timeout value. For instructions, refer to [Change the Session Timeout Value](#) on page 50.

You receive a “Web page not found on host” error message.

The Web server may not have been started correctly because of an unsupported host name format. Rename the computer’s host name if it has an unsupported name. For instructions, refer to [Verify the Host System Name](#) on page 28. You may also need to uninstall and then re-install Command View.

Internet Explorer displays the message, “To display this page correctly, you need to download and install the following components: Microsoft virtual machine,” and never displays a login box when you start Command View.

You need to install the Microsoft virtual machine for Command View to work correctly with Internet Explorer.

If the Install on Demand dialog box is displayed, click **Download**. Insert the Windows Update CD and click **OK**. If you do not have the CD, click **Internet** from the drop-down list, click **OK**, choose the location, and then click **Yes** in the Security Warning dialog box.

General Command View Connection Errors

Your browser crashes while running the application.

It is most likely related to the version of JRE running on your client system. Command View only supports JRE 1.4.2 (Windows) or JRE 1.4.1.03 (HP-UX). Because it is possible for a machine to have multiple JREs installed, verify that your browser is running the correct JRE version. If you are running the correct JRE and still experiencing browser runtime errors, uninstall the JRE and re-install the JRE.

The application begins loading, but then hangs, or the expected application does not load when its tab is clicked.

If the browser window displays “Loading Applet,” but the application ceases downloading, it is most likely due to the proxy settings on your browser. To correct this, disable the Web proxy on the client. For instructions, refer to [Disable the Web Proxy Service](#) on page 47.

If an application tab is clicked and the application fails to load under SSL, it could be because the Java component of the Command View management station is not configured to trust the Web server. This can happen if the Apache SSL Web server is configured with a self-signed certificate, but this self-signed certificate has not been installed or imported into the management station's Java certificate store.

If you decide to use a self-signed certificate, you must also install the certificate in the JRE certificate store. This is because the Java part of the application communicates with the Apache SSL Web server and must trust the Web server's certificate. This is not necessary for a CA signed certificate because the JRE comes with pre-installed certificates from the major CA companies. For a self-signed certificate, the JRE must be told to trust the server certificate by installing the server certificate into the JRE certificate file.

1. Copy the *server_domain_name.crt* file to `\Program Files\JavaSoft\JRE\JRE version\lib\security`.
2. Open a shell window.
3. Use the `cd` command to go to `\Program Files\JavaSoft\JRE\JRE version\lib\security`.
4. Type the following command: `"<drive>:\Program Files\JavaSoft\JRE\JRE version\bin\keytool" -import -alias server_domain_name -file server_domain_name.crt -keystore cacerts`
5. You will be prompted for a password; the default password is: `changeit`.

6. When asked if you want to trust this certificate, click **Yes**.

For more details on SSL configuration, refer to the *Apache Web Server SSL Configuration for Command View Applications* white paper. This document is located on the Command View installation CD (*hpss_apache_whitepaper.pdf*) or in Command View, under the **Support > Reference Documents**.

A Network Error '10-6027' occurs.

Verify that the proxy settings are disabled for IP address of disk array in question. For instructions, refer to [Disable the Web Proxy Service](#) on page 47.

There may be an issue with the client security settings regarding RMI communication, as set in the *Java.policy* file. If you have installed the JRE in the default directory, go to `\Program Files\JavaSoft\JRE\
<JRE version>\Security`, open the *Java.policy* file, and insert the following line before the closing of the last brackets:

```
permission java.net.SocketPermission "*" :1024-65535",
    "connect, accept, resolve";
```

Save the file and proceed to reload the applet.

Error Message: "A connection error occurred between the Remote Control and the controller.(Control: {Array #})"

If after clicking a disk array from Command View XP Main screen, you receive a connection error, do the following

- Verify the SVP of the disk array is not in Modify mode.
- Verify that another Remote Control has not locked the disk array.
- Verify that another Command View XP management application has not locked the disk array.

If none of the previous suggestions resolves the issue, try the following:

- Reboot Remote Control.
- Restart Command View XP services.
- Contact your HP representative.

A warning dialog is displayed when you attempt to connect to Command View using SSL.

A warning dialog indicates that your browser does not trust the certificate it received from the server. This can happen for several reasons:

- The certificate is a self-signed certificate. The browser will normally trust a certificate obtained from a Certificate Authority (CA) such as VeriSign or Thawte. If you create your own self-signed certificate, you must install the certificate in the browser's certificate store if you don't want to see the warning dialog. The Command View server must also have the self-signed certificate installed in the JRE certificate store. Some Command View applications may also require a self-signed certificate be installed into the client Java certificate store. This is not required for a CA signed certificate.
- The host name you used to initiate the request was an IP address or not a fully qualified DNS name. SSL trusted certification relies on the fully qualified DNS name (such as hostname.hp.com) to identify the request with the server certificate. An IP address or a partial "host name" will not work.
- The host name you used in your request did not match the server certificate's host name.
- Most browsers will let you continue passed a failed SSL authentication. However, the Command View application Java components require proper SSL authentication and will fail, for example, if an improper host name is used in an https request. Also make sure that the Java components trust the Apache Web server if you are using a self-signed server certificate by installing the server certificate into the Java certificate store.

Host Agent Deployment Errors

The host agent does not deploy successfully.

The network or host to which you are deploying may be down. Verify that the network and host to which you were attempting deployment are up and functional. If necessary, repeat deployment.

The deployment may have timed out due to network congestion. Deployment stops if it is not successful within 10 minutes. Increase the deployment timeout setting to allow for network congestion. To do this:

- In a word processor or text editor, open the *DeployServerConfig.prp* file located in `\hpss\CVmanagementserver\config`.
- Increase the timeout setting and save the file. The line in the file to change is: `InstallTimeout=900000`.
- Restart the Command View services for the change to take effect, and then try to deploy the host agent again.

CPU utilization may be too high on the host to allow for deployment. To solve this, close applications, services, or processes running on the host. If this is not possible, try to install the host agent from the Command View **Support** tab.

A third-party application might be preventing deployment. In some configurations, third-party applications that provide rexec/exec support for Windows prevent Command View from deploying the host agent. In these cases, an “Operating System is not Supported” error message is displayed. Install the host agent locally from the Command View **Support** tab.

Error messages about the hosts are displayed in the event log after uninstalling the host agent software.

Uninstalling the host agent software will not stop Path Connectivity from collecting data from a host. To stop data collection, you must remove this host from the database in the management station by going to **Path Connectivity > Administration > Host Management** to remove this host from the database in the management station. If you do not delete the host from the database, Path Connectivity will try to contact the host until the scheduled data removal time, which is 30 days by default.

Using the host deployment tools to deploy the host agent to a Windows host produces the following error message, “ERROR - Unknown Host: xx.xx.xx.xxx. Check and correct hostname and verify the host is accessible.”

If you enter the correct login and password for the host that the login window does not accept, the reason may be the “File and Printer Sharing for Microsoft Networks” (Windows 2000 or Windows Server 2003) or “Server” (Windows NT) component is not enabled. This component is installed and enabled by default.

To enable the “File and Printer Sharing for Microsoft Networks” (Windows 2000 or Windows Server 2003) or “Server” (Windows NT), complete the following:

Windows 2000 or Windows Server 2003:

1. Open the Network and Dial-up Connections window by right-clicking the **My Network Places** icon on the desktop and then click **Properties**.
2. Right-click the Local Area Connection that you want to configure.
3. Select the **File and Printer Sharing for Microsoft Networks** check box.

Windows NT:

1. From the Control Panel in Windows, click **Services**.
2. Click **Server** and click **Start**.

3. If the server startup option is not set to automatic, click **Startup** and change the startup type to **Automatic**.

The application does not run when I click Start > Programs > HP StorageWorks Command View XP > Deploy or Remove Host Agent Software (or Update Host Agent Software).

The JRE may be corrupted. Uninstall Command View XP and the JRE. Install JRE 1.4.2 (Windows) or JRE 1.4.1.03 (HP-UX), and then install Command View XP.

You are not able to reload the Emulex driver for the Linux host after installing the host agent.

When the host agent is running on Linux, it keeps contact with the HBA driver. You may receive a “lpfcdd: Device or resource busy” message when trying to rmmmod the driver. Try to stop the host agent and then reload the HBA driver.

To stop the host agent for UNIX host:

```
/opt/sanmgr/hostagent/sbin/HA_trigger stop  
/opt/sanmgr/hostagent/sbin/dial_trigger stop
```

To start the host agent for UNIX host:

```
/opt/sanmgr/hostagent/sbin/HA_trigger start  
/opt/sanmgr/hostagent/sbin/dial_trigger start
```

Installing the host agent has failed and reinstalling the host agent software does not solve the problem.

A partial installation may have occurred due to a network timeout or other similar reason. Instead of reinstalling the software, you may need to remove any partial host agent components on the host first and then retry the installation.

If you used the local installation method, run the uninstall script that comes with the local installation package. If you used the remote deployment tool, use the tool to uninstall the partially installed components.

Installation Checklist



This appendix contains a helpful installation checklist that you can print out and reference when installing and setting up Command View. For details about each task, refer to the [Installation](#) chapter on page 13.

Verifying the System Requirements

- Verify that the hardware and disk space requirements are met on the Command View management station and Web client (page 14).
- Verify that the firmware requirements are met on all disk arrays (page 16).
- If you plan to use Path Connectivity, verify that the host agent operating system and disk space requirements are met (page 16).
- Verify that supported HBAs are installed on the host (page 17).
- If you are installing the Command View CLI and/or Path Connectivity CLI, verify the requirements are met (page 25).

Installing Command View

- Implement the recommended network configuration (page 26).
- If you place a disk array behind a firewall, then set up the ports to bypass the firewall (page 27).
- If you are using multiple LAN cards, configure the first LAN card to communicate with the hosts and Command View API clients on the SAN and modify the *APIServer.cfg* file to point to the first LAN card. (page 27).
- Verify that the Command View management station system name does not contain spaces or illegal characters (page 28).
- If you are installing Command View in a secure SSL environment, verify the correct procedures are used. See [Install SSL for Secure Communication \(Optional\)](#) on page 29.

- Install the SNMP service, which is needed to view events in the Command View Event History screen. SNMP is also needed if you plan to integrate Command View with other management applications (page 29).
- Verify that the service is installed and running (page 30).
- If you are managing an XP256, install Remote Control (page 30). Remote Control **must** run on a different PC than the Command View management station. The Remote Control PC should be running Windows NT 4.0 with Service Pack 4 or later.
- Install or upgrade Command View on the management station (page 33).
- Verify Command View installation, services, and execution (page 37 and page 38). Please note that you cannot manage an XP disk array with more than one Command View management station at a time.
- Set up SMI-S XP (page 38).
- Set up event notification and history reporting (page 45).

Other Related Procedures

- Modify or repair Command View on the management station (page 36).
- Uninstall Command View on the management station (page 37).

Setting Up Command View

- If you are moving from an existing management station to a new management station, use the Backup Utility to migrate the Command View data, settings, and preferences from the previous management station (page 46).
- If you are managing an XP128/XP1024, disable the Web proxy for your Web browser (page 47).
- If you are using Internet Explorer for your Command View browser client session, verify that the browser has been configured correctly (page 48).
- If you are using Netscape or Mozilla for your Command View browser client session, verify that the browser has been configured correctly (page 49).
- If needed, change the session timeout value (page 50).
- Add the disk arrays to Command View (page 51).
- Install any license keys if you need to enable array product features such as Business Copy or Continuous Access (page 52).
- If you are managing an XP48/XP512 and want to use Auto LUN, enable Auto LUN after installing the license key (page 52).

- Install the Command View Command Line Interface (CLI) if needed (page 53).

Setting Up Path Connectivity

- Add FC switches through Path Connectivity (page 54).
- Install the host agents (page 55). If you have purchased HP StorageWorks Command View SDM, do not deploy Path Connectivity host agents and Command View SDM host agents on the same host system. They cannot co-exist.
- Verify Path Connectivity is working correctly and is able to collect data from the XP disk arrays, hosts, and switches (page 62).
- Install the Path Connectivity Command Line Interface (CLI) if needed (page 62).

Other Related Procedures

- Add or remove host agent installation files on the management station (page 61). If you have already installed Command View and Path Connectivity, but need to add or remove operating systems that your hosts will be running, complete this step.

Integrating Snap-In Modules into Command View

- Install Performance Advisor on the Command View management station (page 63).
- Install Application Policy Manager on the Command View management station (page 63).

Integrating Command View with Other Platforms

- Integrate Storage Area Manager with Command View (page 64).
- Integrate other management platforms and applications with Command View (page 65).

A

- adding
 - disk arrays [51](#)
 - host agent installation files [61](#)
 - switches [54](#)
- Apache Web Server [29](#)
- audience [8](#)
- authorized reseller, HP [11](#)
- Auto LUN setup [52](#)

B

- bypassing a firewall [27](#)

C

- changing the timeout value [50](#)
- checklist [75](#)
- Collect Data Now operation [62](#)
- Command View
 - CLI [53](#)
- Command View, setting up [46](#)
- connections through a firewall [27](#)
- conventions
 - document [9](#)
 - text symbols [9](#)

D

- disk array firmware levels [16](#)
- document
 - conventions [9](#)
 - prerequisites [8](#)
 - related documentation [8](#)

F

- firewall [27](#)
- firmware [16](#)

G

- getting help [11](#)

H

- help, obtaining [11](#)
- host agent disk space requirements [16](#)
- host agents [55](#)
- HP
 - authorized reseller [11](#)
 - storage website [11](#)
 - technical support [11](#)

I

- installation checklist [75](#)
- installation reference [13](#)
- installing
 - Command View [26, 33](#)
 - CV CLI [53](#)
 - host agents [55](#)
 - license keys [52](#)
 - Path Connectivity host agents [55](#)
 - PC CLI [62](#)
 - SMI-S XP [38](#)
 - SNMP [29](#)
- Internet Explorer [48](#)
 - browser settings for version 5.5 (SP2) or later [48](#)

J

Java Web Start [15](#), [50](#)

M

minimum requirements

 browser [14](#)

 client [14](#)

 management station [14](#)

modifying

 Command View [36](#)

modifying Command View [61](#)

Mozilla [49](#)

N

Netscape [49](#)

P

Path Connectivity

 CLI [62](#)

 host agents [55](#)

Path Connectivity host agents [55](#)

ports [27](#)

prerequisites [8](#)

R

reference [13](#)

related documentation [8](#)

Remote Control (for the XP256) [30](#)

removing

 host agent installation files [61](#)

repairing Command View [36](#)

S

setting up Command View [46](#)

SMI-S XP [38](#)

SNMP

 installing [29](#)

 verifying [30](#)

 verifying on Remote Control [30](#)

SSL [29](#)

switches, adding [54](#)

symbols in text [9](#)

system name [28](#)

T

technical support, HP [11](#)

text symbols [9](#)

timeout value [50](#)

U

uninstalling

 Command View [37](#)

V

verifying

 Command View execution [38](#)

 Command View services [37](#)

 disk array firmware levels [16](#)

 SNMP [30](#)

W

Web proxy configuration [47](#)

websites

 HP storage [11](#)

Figures

1	Example of a network with added security from a firewall	26
2	Verifying the public community name and its attributes	31
3	Configuring the SNMP service	32
4	Internet Options dialog box (Internet Explorer).	49



Tables

1	Document Conventions	9
2	Web client requirements	15
3	Host disk space requirements	16
4	HP-UX, Solaris, and AIX host directory requirements	17
5	Supported HBAs	18
6	Command View installation process	33
7	Command View services	37
8	Providers.list properties	40
9	cim.properties parameters	40
10	Command View compatibility with Performance Advisor and Application Policy Manager 63	
11	Command View host agent compatibility with Storage Area Manager host agents	64

