

HP

Storage Essentials 5.0 Installation Guide



T3710-96001

Part number: T3710-96001
First edition: September 2005



Legal and notice information

© Copyright 2005 ApplQ Inc.

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

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

Windows are registered trademarks of Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. Sun, Solaris, Sun StorEdge, and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. AIX and IBM are registered trademarks of International Business Machines Corporation in the United States, other countries or both. SGI and IRIX are registered trademarks of Silicon Graphics, Inc. Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries. HDS and HiCommand are registered trademarks of Hitachi Data Systems. HP-UX is a registered trademark of Hewlett-Packard Company.

UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Storage Essentials 5.0 Installation Guide

Contents

About this guide	xi
Intended audience	xi
Prerequisites	xi
Related documentation	xi
Document conventions and symbols	xii
HP technical support	xiii
HP-authorized reseller	xiii
Helpful web sites	xiii
1 Overview	1
About this Product	4
Storage Management Terms	4
Key Benefits	4
Key Features	4
Software Requirements	5
Web Browser Configuration Requirements.	5
2 Installing the Management Server on Microsoft Windows.	7
Step 1 - Install the Database for the Management Server	7
Installing the Oracle Patch (Windows)	8
Step 2 - Install the Management Server	9
Step 3 - Verify that Services Can Start	10
Configurations Required for Discovering EMC CLARiiON Storage Systems	11
Removing the Management Server	12
3 Installing the Storage Essentials Connector	13
4 Discovering Filers, Tape Libraries, Switches, and Storage Systems.	15
Step 1 - Discover Switches	16
Discovering Brocade Switches.	17
Verifying Brocade Rapid Program Is Set to 1	17
Discovering CNT Switches	18
Discovering Cisco Switches.	19
Discovering Sun StorEdge and QLogic Switches	19
Changing the SNMP Trap Listener Port for Sun StorEdge Switches	20
Discovering McDATA and EMC Connectrix Switches	20
SWAPI Setting Through a Proxy	22
Step 1 - (McDATA Switches Only) Install the Bridge Agent	22
Step 2 - Change the Discovery Setting for McDATA and Connectrix Switches to SWAPI	23
Step 3 - Discover the Proxy	23
CIM_ERR_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI	23

SNMP Setting Through a Proxy	24
Step 1 - Verify the Discovery Setting for Switches Is Set to SNMP	24
Step 2 - Discover the Proxy	24
Step 3 - Make Sure There Are No Port Conflicts for Receiving SNMP Traps.	25
Step 4 - Step Up the Proxy to Send Traps to the Correct Port	25
Contacting a McDATA or Connectrix Switch Directly.	25
Make Sure There Are No Port Conflicts for Receiving SNMP Traps.	25
Configure the SNMP Agent to Send Traps to the Correct Port	26
Changing the Discovery Settings.	26
Excluding McDATA and EMC Connectrix Switches from Discovery	27
Viewing Log Messages.	28
Duplicate Logs for Brocade Switches in Same Fabric.	28
Step 2 - Discover Storage Systems, Filers and Tape Libraries	28
Discovering EMC Solutions Enabler 5.1	31
Excluding EMC Symmetrix Storage Systems from Discovery	32
Discovering EMC CLARiiON Storage Systems.	33
Discovering HDS Storage Systems	33
Excluding HDS Storage Systems from Discovery	34
Discovering HP StorageWorks Arrays	35
Discovering Engenio Storage Systems	36
Discovering NetApp Filers	36
Discovering Sun StorEdge 3510 Storage Systems	37
Discovering Sun StorEdge 6920 Storage Systems	38
Discovering Sun StorEdge 6130 Storage Systems	38
Discovering IBM Storage Systems	38
Discovering IBM Tape Libraries	39
Modifying the Properties of a Discovered Address.	39
Deleting Elements from the Management Server	40
Deleting an Element Using System Manager or Chargeback Manager	41
Step 3 - Discovery Data Collection	41
Discovery Data Collection.	41
Stopping the Gathering of Details	43
Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh	43
Excluding HDS Storage Systems from Force Device Manager Refresh.	44
Managing McDATA and EMC Connectrix Switches	46
About Managing McDATA and EMC Connectrix Switches	46
Adding McDATA and EMC Connectrix Switches	46
Assigning a File Extension in Netscape 7	46
Updating the Database with Element Changes	47
Filtering Discovery Groups.	47
Moving Elements to Another Discovery Group	48
Placing an Element in Quarantine.	48
Removing an Element from Quarantine	49
5 Installing the CIM Extension for IBM AIX.	51
About the CIM Extension for IBM AIX	51

Prerequisites	51
Verifying SNIA HBA API Support	52
Installing the CIM Extension	53
Setting Up Monitoring	54
Starting the CIM Extension Manually	54
Changing the Port Number	55
Specifying the CIM Extension to Listen on a Specific Network Card	55
Finding the Version of a CIM Extension	56
Modifying the Boot Time RC Start Script (Optional)	57
Stopping the CIM Extension	57
How to Determine if the CIM Extension Is Running	57
Fulfilling the Prerequisites	57
Rolling Over the Logs	58
Removing the CIM Extension from AIX	59
6 Installing the CIM Extension for SGI ProPack for Linux	61
About the CIM Extension for SGI ProPack for Linux	61
Prerequisites	61
Verifying SNIA HBA API Support	62
Installing the CIM Extension	62
Starting the CIM Extension	63
Changing the Port Number	64
Specifying the CIM Extension to Listen on a Specific Network Card	65
Stopping the CIM Extension	66
How to Determine if the CIM Extension Is Running	66
Removing the CIM Extension from SGI ProPack for Linux	66
7 Installing the CIM Extension for HP-UX	69
About the CIM Extension for HP-UX	69
Prerequisites	69
HP-UX 11i and 11.0	69
Software Requirements	69
HP-UX 11i	70
Driver Bundle Version	70
Driver Patch	70
HP-UX 11.0	70
Driver Bundle Versions	70
Driver Patch	70
Required Disk Space	70
Network Port Must Be Open	70
Verifying SNIA HBA API Support	70
Installing the CIM Extension	71
Starting the CIM Extension Manually	72
Restricting the Users Who Can Discover the Host	73
Changing the Port Number	73

Specifying the CIM Extension to Listen on a Specific Network Card	74
Finding the Version of a CIM Extension	75
Combining Start Commands	75
Finding the Status of the CIM Extension	76
Modifying the Boot Time RC Start Script (Optional).	76
Stopping the CIM Extension	76
Rolling Over the Logs	76
Fulfilling the Prerequisites.	77
Removing the CIM Extension from HP-UX.	77
8 Installing the CIM Extension for SGI IRIX.	79
About the CIM Extension for SGI IRIX	79
Prerequisites	79
Verifying SNIA HBA API Support	80
Installing the CIM Extension	80
Starting the CIM Extension.	81
Changing the Port Number	81
Specifying the CIM Extension to Listen on a Specific Network Card.	82
Starting the CIM Extension by chkconfig	83
Finding the Version of a CIM Extension	83
Modifying the Boot Time RC Start Script (Optional).	84
Stopping the CIM Extension	84
Rolling Over the Logs	84
How to Determine if the CIM Extension Is Running	85
Removing the CIM Extension from SGI IRIX	85
9 Installing the CIM Extension for SUSE and Red Hat Linux	87
About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux.	87
Prerequisites	87
Verifying SNIA HBA API Support	88
Driver Information for Verifying SNIA Emulex Adapters on Red Hat Linux	88
Driver Information for Verifying QLogic SNIA Adapters on Red Hat Linux	88
Driver Information for Verifying QLogic SNIA Adapters on SUSE Linux	89
Installing the CIM Extension	89
Starting the CIM Extension Manually.	89
Changing the Port Number	90
Specifying the CIM Extension to Listen on a Specific Network Card.	91
Finding the Version of a CIM Extension	92
Finding the Status of the CIM Extension.	92
Modifying the Boot Time RC Start Script (Optional)	92

Stopping the CIM Extension	93
Rolling Over the Logs	93
Removing the CIM Extension from Red Hat or SUSE Linux	93
10 Installing the CIM Extension for Sun Solaris	95
About the CIM Extension for Solaris	95
Prerequisites	95
Verifying SNIA HBA API Support	96
Driver Information for Verifying SNIA Emulex Adapters	96
Driver Information for QLogic Adapters	96
Driver Information for AMCC/JNI Adapters	97
Driver Information for Sun Leadville branded QLogic or JNI Adapters	97
Installing the CIM Extension	97
Starting the CIM Extension Manually	98
Restricting the Users Who Can Discover the Host	99
Changing the Port Number	99
Specifying the CIM Extension to Listen on a Specific Network Card	100
Finding the Version of a CIM Extension	101
Combining Start Commands	101
Finding the Status of the CIM Extension	102
Modifying the Boot Time RC Start Script (Optional)	102
Stopping the CIM Extension	102
Rolling Over the Logs	102
Removing the CIM Extension from Solaris	103
11 Installing the CIM Extension for Microsoft Windows.	105
About the CIM Extension for Windows	105
Finding Applications Dependent on WMI	106
How to Determine If WMI Is Running	106
Verifying SNIA HBA API Support	107
Driver Information for Verifying SNIA Emulex Adapters	107
Driver Information for Verifying IBM Branded QLogic Adapters	108
Driver Information for Verifying QLogic Adapters	109
Driver Information for Verifying AMCC/JNI Adapters	109
Installation Steps	109
Installing the CIM Extension Using the Silent Installation	110
Removing the CIM Extension from Windows	110
12 Discovering Applications and Hosts	113
Step 1 - Discovering Your Hosts	113
Step A - Set Up Discovery for Hosts	114
Enabling Dynamic Disk Detection for Windows 2000 Hosts	114
Step B - Obtain Details	114
Step 2 - Setting Up Discovery for Applications	115

Monitoring Oracle	116
Step A - Create the APPIQ_USER Account for Oracle	116
Removing the APPIQ_USER Account for Oracle	117
Step B - Provide the TNS Listener Port	118
Step C - Set up Discovery for Oracle 10g	119
Discovering Oracle Clusters	120
Monitoring Microsoft SQL Server	121
Switching to Mixed Mode Authentication.	121
Step A - Create the APPIQ_USER for the SQL Server	121
Removing the APPIQ_USER Account for SQL Server	122
Step B - Provide the Microsoft SQL Server Name and Port Number	123
Deleting SQL Server Information	123
Monitoring Sybase Adaptive Server Enterprise	124
Step A - Create the APPIQ_USER account for Sybase	124
Removing the APPIQ_USER Account for Sybase	125
Step B - Provide the Sybase Server Name and Port Number.	126
Deleting Sybase Information.	127
Monitoring Microsoft Exchange	127
Adding Microsoft Exchange Domain Controller Access	127
Deleting a Microsoft Exchange Domain Controller	128
Step 3 - Discovering Applications	128
Step A - Detect the Applications.	129
Step B - Obtain Details	129
Changing the Oracle TNS Listener Port	130
Adding/Modifying Microsoft Exchange Domain Controller Access	130
Deleting a Microsoft Exchange Domain Controller	131
Changing the Password for the Managed Database Account.	132
Obtaining Disk Drive Statistics from Engenio Storage Systems	132
Assigning a File Extension in Netscape 7	133
13 Managing Security	135
About the Security for the Management Server.	135
About Roles	135
About Organizations	138
Planning Your Hierarchy.	141
Naming Organizations	141
Managing User Accounts	142
Adding Users	142
Editing a User Account.	143
Deleting Users.	144
Modifying Your User Profile	144
Modifying Your User Preferences.	145
System Manager and Element Topology Preferences.	145
Event Monitoring for Storage Essentials Preferences	145
Warnings for Slow Systems Operations.	146
Viewing the Properties of a Role	146
Viewing the Properties of an Organization	147

Managing Roles	147
Adding Roles	147
Editing Roles	148
Deleting Roles	149
Managing Organizations	149
Adding an Organization	150
Viewing Organizations	151
Editing Organizations	151
Deleting an Organization	152
Removing Members from an Organization	153
Accessing the Edit Organization Window	153
Accessing the Add Elements to Organization Window	153
Filtering Organizations	154
Changing the Password of System Accounts	155
14 Troubleshooting	157
“Data is late or an error occurred” Message	157
appiq.log Filled with Connection Exceptions	157
Receiving “HTTP ERROR: 503” When Accessing the Management Server	158
Errors in the Logs	159
Permanently Changing the Port a CIM Extension Uses (UNIX Only)	159
Configuring UNIX CIM Extensions to Run Behind Firewalls	160
Volume Names from Ambiguous Automounts Are Not Displayed	164
Installing the Software Security Certificate	165
Installing the Certificate by Using Microsoft Explorer 6.0	165
Installing the Certificate by Using Netscape Navigator 7	166
Changing the Security Certificate to Match the Name of the Server	166
Troubleshooting Discovery and Discovery Data Collection	167
Configuring E-mail Notification for Discovery Data Collection	167
Increasing the Time-out Period and Number of Retries for Switches	168
“Connection to the Database Server Failed” Error	170
DCOM Unable to Communicate with Computer	170
Duplicate Listings for Brocade Switches in Same Fabric	170
Element Logs Authentication Errors During Discovery	171
EMC Device Masking Database Does Not Appear in Topology (AIX Only)	171
Microsoft Exchange Drive Shown as a Local Drive	171

Unable to Discover Microsoft Exchange Servers	171
Nonexistent Oracle Instance Is Displayed	171
Requirements for Discovering Oracle	171
Unable to Find Elements on the Network	172
Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration	172
A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly	172
Unable to Monitor McDATA Switches	172
Unable to Detect a Host Bus Adapter	173
Navigation Tab Displays Removed Drives as Disk Drives	173
Unable to Obtain Information from a CLARiON Storage System	173
Discovery Fails Too Slowly for a Nonexistent IP Address	173
“CIM_ERR_FAILED” Message	174
Communicating with HiCommand Device Manager Over SSL	175
Unable to Discover a UNIX Host Because of DNS or Routing Issues	176
Troubleshooting Hardware	177
About Swapping Host Bus Adapters.	177
“Fork Function Failed” Message on AIX Hosts	177
Known Driver Issues	178
Known Device Issues	178
“mailbox command 17 failure status FFF7” Message	181
“Process Has an Exclusive Lock” Message	181

Index 183

Figures

1 Starting WMI (Microsoft Windows 2000).	107
2 Parent-Child Hierarchy for Organizations	139
3 Children in Multiple Organizations	140
4 Changing Your User Profile.	144
5 Accessing the User Preferences Tab	145
6 Viewing Organizations	151
7 Clicking the Organization Link	154
8 Active Organization.	155

Tables

1 Document conventions	xii
2 Roadmap for Installation and Initial Configurations	1
3 Discovery Requirements for Switches	16
4 Required Switch Models and InVsn Versions for Discovery	18
5 Discovery Settings for McDATA and Connectrix Switches	21
6 Discovery Requirements for Storage Systems and NAS Filers.	29
7 Default Role Privileges	136
8 Default Role Privileges with Elements	137
9 Changing User Preferences for Event Monitoring for Storage Essentials	145
10 Troubleshooting Firewalls	161

11	Time-out Properties	169
12	Retry Properties	169
13	Known Device Issues	178

About this guide

This guide provides information about:

- Installing the product
- Discovering elements
- Creating users
- Changing the admin password
- Installing JReport Designer

Intended audience

This guide is intended for:

- Network Engineers
- Administrators
- Any one that needs to monitor and/or manage their file servers

Prerequisites

Prerequisites for using this product include:

- Networking
- Storage Area Networks (SANs)
- The Common Information Model (CIM)

Related documentation

In addition to this guide, please refer to other documents for this product:

- Online help for HP Storage Essentials 5.0
- HP Storage Essentials 5.0 Integration Guide
- HP Storage Essentials 5.0 User Guide
- HP Storage Essentials 5.0 Application Guide
- HP Storage Essentials 5.0 CLI Guide
- HP Storage Essentials 5.0 for File Servers Guide

These and other HP documents can be found on the HP web site: <http://www.hp.com/support/>


Document conventions and symbols


Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

 **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

 **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

 **IMPORTANT:** Provides clarifying information or specific instructions.

 **NOTE:** Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site:

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

Collect the following information 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

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

HP strongly recommends that customers sign up online using the Subscriber's choice web site at

<http://www.hp.com/go/e-updates>.

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

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-345-1518.
- Elsewhere, visit the HP web site: <http://www.hp.com>. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For third-party product information, see the following HP web sites:

- <http://www.hp.com>
- <http://www.hp.com/go/storage>
- <http://www.hp.com/support/>

1 Overview

This chapter describes the following:

- ["About this Product"](#) on page 4
- ["Software Requirements"](#) on page 5
- ["Web Browser Configuration Requirements"](#) on page 5

Storage Essentials integrates tightly with HP Systems Insight Manager. The installation requires you to install Storage Essentials, HP System Insight Manager, and the Storage Essentials Connector. It highly recommended you follow the steps outlined in [Table 2](#) on page 1.

IMPORTANT: If you access HP Systems Insight Manager through HTTP over SSL (HTTPS), you must provide the full DNS name for the host to be able to access HP Storage Essentials. For example, you could access HP Systems Insight Manager by using `https://mycomputer.domainname.com:50000`, but you could not use `https://mycomputer:50000`. For non-secure connections (HTTP), the full DNS name does not need to be provided.

Table 2 Roadmap for Installation and Initial Configurations

Step	Description	Where to Find
1	Install the management server (Storage Essentials). This step requires you to install third-party software.	See "Installing the Management Server on Microsoft Windows" on page 7.

Table 2 Roadmap for Installation and Initial Configurations (continued)

Step	Description	Where to Find
2	<p>Install HP Systems Insight Manager.</p> <p>Important: When you install HP Systems Insight Manager, you must do the following:</p> <ul style="list-style-type: none"> • Select custom installation. • Make sure HP Systems Insight Manager is selected as a component to install. You may also want to select HP Systems Insight manager Installation Information. <p>When you are asked for the database configuration, select the Oracle option and provide the following information:</p> <ul style="list-style-type: none"> • Username - SIM_MANAGER • Password - quake Case sensitive for UNIX servers. • Host - Name of the server on which you installed Storage Essentials. Do not use local host. • Database - APPIQ • Port - 1521 • Jar File - %ORA_HOME%\jdbc\lib\ojdbc14.jar 	<p>See the <i>HP Systems Insight Manager Installation and User Guide</i>. Keep in mind you will need to do a custom installation and provide the information mentioned in the previous column.</p>
3	<p>Install the Storage Essentials Connector.</p> <p>After you install the Storage Essentials Connector, start AppStorManager, which is the service for StorageEssentials.</p>	<p>See "Installing the Storage Essentials Connector" on page 13.</p>
4	<p>Perform discovery for switches, filers, and storage systems. This step requires the management server to be connected to the network containing the switches, filers, and storage systems you want to manage.</p>	<p>See "Discovering Filers, Tape Libraries, Switches, and Storage Systems" on page 15.</p>

Table 2 Roadmap for Installation and Initial Configurations (continued)

Step	Description	Where to Find
5	<p>Install a CIM Extension on each host (other than the management server) from which you want the management server to be able to obtain information. The CIM Extension gathers information from the operating system and host bus adapters on the host. It then makes the information available to the management server.</p> <p>Important: CIM Extensions are required on UNIX hosts. If you do not install a CIM Extension on a UNIX host, the management server cannot obtain information from the host. On a Microsoft Windows host without a CIM Extension, the management server can only find information that is gathered from Windows Management Instrumentation. The CIM Extension is required to obtain information from the host bus adapter and manage applications on the Microsoft Windows host. Without the CIM Extension, the management server can determine if Oracle and Microsoft Exchange are on the host, but it cannot obtain further information about the applications.</p>	<ul style="list-style-type: none"> • IBM AIX - See "Installing the CIM Extension for IBM AIX" on page 51. • SGI ProPack for Linux - See "Installing the CIM Extension for SGI ProPack for Linux" on page 61. • HP-UX - See "Installing the CIM Extension for HP-UX" on page 69. • SGI IRIX - See "Installing the CIM Extension for SGI IRIX" on page 79. • SUSE and Red Hat Linux - See "Installing the CIM Extension for SUSE and Red Hat Linux" on page 87. • Sun Solaris - See "Installing the CIM Extension for Sun Solaris" on page 95. • Microsoft Windows - See "Installing the CIM Extension for Microsoft Windows" on page 105.
6	<p>Configure the applications and hosts for monitoring. This step includes discovering applications and hosts.</p>	<p>See "Discovering Applications and Hosts" on page 113.</p>
7	<p>If your license lets you collect disk drive statistics from Engenio storage systems, set up the management server to collect those statistics.</p> <p>You can determine if your license lets you collect this data, by accessing the feature list, which is accessible from the Documentation Center (Help > Documentation Center in Storage Essentials).</p>	<p>See "Obtaining Disk Drive Statistics from Engenio Storage Systems" on page 132.</p>

Table 2 Roadmap for Installation and Initial Configurations (continued)

Step	Description	Where to Find
8	Change the password of the system accounts.	See "Changing the Password of System Accounts" on page 155.

About this Product

This product can simplify your complex environment and lower your cost of management with CIM-based integrated storage management. The management software integrates the management of applications, servers, storage networks and storage subsystems in a single, easy to implement and intuitive solution.

The management software integrates the various components in the storage infrastructure into a CIM/WBEM/SMI-S standards based database so you can eliminate any vendor dependencies and view and manage your infrastructure as a whole.

By giving your administrators a single, integrated console to manage tactical activities such as provisioning storage, managing real time events, installing new applications, and migrating servers and storage, as well as strategic activities such as forecasting, planning and cost analysis, the management software's integrated storage management lowers your cost of acquiring and managing a heterogeneous storage environment.

Storage Management Terms

- **CIM** - A common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment.
- **Web-Based Enterprise Management (WBEM)** - An initiative based on a set of management and Internet standard technologies developed to unify the management of enterprise computing environments.

See the glossary in the management server User Guide or in the management server help system for additional definitions.

Key Benefits

- More efficient use of existing assets
- Increased application availability and performance
- Quicker deployment of storage infrastructure and business applications
- Protection of customer flexibility and investments with a standards-based interface

Key Features

- **End-to-end visibility of business applications** - Provides an interface for you to monitor your business applications, including their associated infrastructure and interdependencies.
- **Integrated storage management** - Lowers cost of acquiring and managing a heterogeneous storage environment using multiple disparate, point solutions.
- **Standards-based architecture** - Protects customer flexibility and investments with a standards-based interface for managing heterogeneous storage environments.

- **Storage server, network and subsystem provisioning** - Reduces manual processes and risk of downtime due to free-space outages with multi-level storage provisioning.
- **Reporting** - Offers flexible, in-depth report generation in both predefined and user defined formats, or export data to other management applications.
- **Integrated asset management and chargeback** - Centralizes all aspects of storage inventory for maximum asset utilization. Improves accountability and budgeting with cost accounting based chargeback on user defined utilization characteristics.
- **Web-based global management console** - Provides management of heterogeneous storage environments through a web-based user interface.

Software Requirements

To find the software requirements, refer to the release notes ([SupportMatrix.html](#)), which can be found:

- On the CIM Extension CD-ROM.
- On the management server. To access the support matrix on the management server, go to the Documentation Center (**Help > Documentation Center** in Storage Essentials).

Web Browser Configuration Requirements

Before you can use the management server, verify the following are enabled on your Web browser:

- cookies
- JavaScript
- Java

You can verify these settings by doing the following:

- **Microsoft Internet Explorer** - Go to the Internet Options window by selecting **Tools > Internet Options**.
 - **To verify if cookies are enabled** - Click the **Privacy** tab.
 - **To verify if JavaScript and Java are enabled** - Click the **Advanced** tab.
- **Netscape** - Go to the Preferences window by selecting **Edit > Preferences** in Netscape.
 - **To verify if cookies are enabled** - Expand the **Privacy & Security** category, and then click **Cookies**.
 - **To verify if Java is enabled** - Click **Advanced**.
 - **To verify if JavaScript is enabled** - Expand the **Advanced** category, and then click **Scripts & Plug-ins**.

For more information about enabling the items listed above, refer to the online help for your Web browser.

2 Installing the Management Server on Microsoft Windows

If you did not receive a computer with the management server installed on it, first complete the steps in this section.

Keep in mind the following:

- **All steps must be completed for the management server to work properly.**
- For optimal performance, install the management server on a dedicated computer. See the release notes for hardware requirements.
- Installation through a terminal server or using Virtual Network Computing (VNC) software is not supported.

This chapter describes the following:

- ["Step 1 - Install the Database for the Management Server"](#) on page 7
- ["Step 2 - Install the Management Server"](#) on page 9
- ["Step 3 - Verify that Services Can Start"](#) on page 10
- ["Configurations Required for Discovering EMC CLARiiON Storage Systems"](#) on page 11
- ["Removing the Management Server"](#) on page 11

Step 1 - Install the Database for the Management Server

IMPORTANT: Install the database for the management server on a computer that does not have Oracle.

The management server uses a database to store the data it collects from the hardware it monitors. The management server ships with a three-CD set for the management server database and an additional CD-ROM for Database Patch 9.2.0.6.0. During the installation of the database, you are prompted to change CD-ROMs. After the installation, you must install the database patch from the Database Patch CD-ROM.

Keep in mind the following:

- Once you have started the installation, do not exit out of it. Future installations of the management server database may think you have already installed the software if you exit several minutes into the installation and orauser has already been created.
- Install the database on the computer you plan to install the management server.
- For double-byte languages, the Oracle installation provides an extra dialog screen, which is for the Oracle Net Configuration Assistant. This screen requires the user to select the check box and click **Next**. Once you clicked **Next**, a command window appears. The command window will close itself once the operation running inside the command window completes.

To install the database:

1. Insert CD 1 of the database set that shipped with the management server.
2. Allow the CD to autorun. If you must run the installation manually, double-click **inst.cmd** found in the /AppIQ directory instead of `setup.exe`.
The installation is spread over several CD-ROMs. During the installation, you are asked to switch CD-ROMs.
3. When you are asked if you want to set the `ORA_HOME` environment variable, click **Yes** if it has not been set or you want to change the location.
4. Enter the directory and its path that will contain the database, for example: `D:\database` where `D:\database` is the directory that will contain the database.

IMPORTANT: Do not specify a directory with spaces, such as the Program Files directory or any directories under Program Files.

5. Select **No** when you are asked if you want to create a database.

Installing the Oracle Patch (Windows)

The steps provided in this section describe how to install Oracle Server Patch 9.2.0.6.0.

NOTE: If you are not sure if you have already installed the patch, access the Oracle Universal Installer (**Start > Programs > Oracle Installation Products > Universal Installer**). In the Oracle Universal Installer, click **Installed Products**. Then, expand the OraHome tree. The installed products are displayed. Look for the highest patch level. To exit the Oracle Universal Installer, click **Close**, and then click **Exit**. When asked if you want to exit, click **Yes**.

To install the Oracle patch:

1. Perform a complete backup and export the existing management server database if you are patching an existing management server database.
2. Change the service startup type of all Oracle services, AppStorManager and the Distributed Transaction Coordinator service to manual. The AppStorManager service is not available if you are installing the management server for the first time. Oracle services usually start with Oracle, for example:
 - OracleOraHome92Agent
 - OracleOraHome92ClientCache
 - OracleOraHome92SNMPPeerEncapsulator
 - OracleOraHome92SNMPPeerMasterAgent
 - OracleOraHome92TNSListener
 - OracleServiceAPPIQ

NOTE: Before you change the service startup types, make note of the services that are set to automatic, as you will need to restore the service startup settings when you are done with installing the patch.

3. Reboot the server.
4. Insert the Database Patch CD into the CD-ROM drive.
5. Open a command prompt window and go to the CD-ROM directory by entering the following:
d:
where d is the drive letter for the CD-ROM drive
6. Enter the following at the command prompt:
d:\>installPatch.cmd
where
d is the drive letter for the CD-ROM drive
If you are asked for the path to the Oracle home, provide the path. The path for the default Oracle installation is c:\oracle\ora92.
7. To accept the default settings in the File Locations dialog, click **Next**.
The patch is installed.
8. When you are asked to enter the SYS password, provide the password.
9. You receive an error if a database does not exist. Ignore the error.
10. Restore the Oracle services, AppStorManager and the Distributed Transaction Coordinator service to automatic so they automatically start the next time the server is rebooted.
11. Reboot the server.

Step 2 - Install the Management Server

Refer to the release notes for operating system requirements.

Keep in mind the following:

- Refer to the release notes for late breaking information.
- Make sure no other programs are running when you install the management server.
- If you are installing the management server in a production environment, you must install the management server on a machine with a static IP address.
- The management server uses the following ports. Make sure these ports are available:
 - 4444 - JBoss JRMPInvoker
 - 4445 - JBoss PooledInvoker
 - 8009 - JBoss EmbeddedTomcatService
 - 8083 - JBoss WebService
 - 8093 - JBoss UILServerILService
 - 5986 - RMI port for JwsMain (see JwsMain.java)
 - 5988 - WBEM HTTP

To install the management server:

1. (Double-byte operating systems only) Remove the `sqlnet.ora` file, which can be found in the `\oracle\ora92\network\admin` directory for a default Oracle installation.
2. Insert the Windows Manager CD-ROM and double-click **InstallManager.exe**.
3. When you see the introduction screen, click **Next**.
4. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, click the Choose button. You can always display the default directory by clicking the **Restore Default Folder** button. When you are done, click **Next**.
5. Read the important notes, such as disabling IIS before running the software. Click **Next**.
6. Check the pre-installation summary. You are shown the following:
 - Product Name
 - Installation Folder
 - Disk Space Required
 - Disk Space Available

NOTE: Refer to the Support Matrix for information about supported hardware.

7. Do one of the following:
 - Click **Install** if you agree with the pre-installation summary.
 - Click **Previous** if you want to modify your selections.

The management server is installed.

CAUTION: Do not click the **Cancel** button during the installation. You can always remove an unsatisfactory installation.

8. When the installation is complete, you are shown the directory containing the management server and the machine ID, which is used by technical support for licenses. You do not need to write down the machine ID. You can obtain it easily from the management server (**Security > Licenses**).
9. You must reboot the server. The AppStorManager service starts automatically after a reboot.

IMPORTANT: If you have any questions about the installation, you can look at the install logs, which are located in the `[installation_directory]\logs` directory.

Step 3 - Verify that Services Can Start

After you install the management server, verify the service for the management server has started. It may take some time for the service to start depending on the server's hardware. The service must

be running to monitor and manage your elements. Refer to the appropriate section for your operating system.

After you restart the management server, you can verify that the required services have started.

To verify services have started:

1. Access the Services window by doing the following:
 - a. Right-click **My Computer**.
 - b. Select **Manage** from the drop-down menu.
 - c. In the left pane of the Computer Management window, select **Services and Applications**.
 - d. In the right pane, double-click **Services**.
2. Verify that the following services have been started by looking under the Status column in the Services window.
 - AppStorManager (must be set to automatic)
 - OracleOraHome92TNSListener (must be set to automatic)
 - OracleServiceAPPIQ (must be set to automatic)
3. Verify that the following services are disabled or not installed by looking under the Status column in the Services window
 - OracleOraHome92HttpServer
 - IIS (Internet Information Server)

Configurations Required for Discovering EMC CLARiiON Storage Systems

The EMC Navisphere CLI is required for the management server to communicate with the CLARiiON storage system. At the time this documentation was created, EMC distributed the Navisphere CLI as part of the EMC Navisphere Software Suite. Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC. For Solaris, you must install the Navisphere Disk Array Management Tool CLI (NAVICLI).

Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC.

In Navisphere add the following to the privilege user section:

```
SYSTEM@name_of_my_management_server  
SYSTEM@IP_of_my_management_server
```

where

- `name_of_my_management_server` is the DNS name of the computer running the management server software

- `IP_of_my_management_server` is the IP address of the computer running the management server software

Removing the Management Server

This section describes how to remove the management server. Refer to the appropriate section for your operating system.

To remove the management server:

1. Remove the Storage Essentials Connector by going to Add/Remove programs and selecting SE Connector. Follow the directions for your Windows operating system for more information.
2. Stop the service for the management server by doing the following:
 - a. Go to the Services window (**Control Panel > Administrative Tools > Services**).
 - b. Right-click the **AppStorManager** service in the Services window.
 - c. Select **Stop** from the drop-down menu.
3. Open the Add/Remove Programs window, which is accessible from the Control Panel.
4. In the Add/Remove Programs window, select **AppStorM Management Server** and then click Change/Remove button.
5. In the InstallShield Wizard window, select the **Remove** option. Then, click **Next**.
6. When you are asked if you want to completely removed the selected application and all of its features, click **OK**.
7. If files were added or modified after the original installation, the `[Installation_Directory]` may still exist. You may need to reboot the management server before you can delete this directory.
8. Remove the OracleServiceAPPIQ database instance from Oracle, as described in the following steps:

NOTE: You can also use the Oracle Universal Installer to manually remove OracleServiceAPPIQ.

- a. Enter the following at a command prompt on the management server:

```
oradim -delete -SID APPIQ
```
- b. Delete the following directories and their contents on the management server:
 - `c:\oracle\oradata\APPIQ`
 - `c:\oracle\admin\APPIQ`
 - `%ORA_HOME%\rman` if applicable

The above deletes the database instance.

3 Installing the Storage Essentials Connector

This chapter describes how to install the Storage Essentials Connector, which lets you communicate with HP Systems Insight Manager. Install the Storage Essentials Connector on the same server running Storage Essentials.

To install the Storage Essentials Connector:

1. Start AppStorManager from the Services window on the server where you installed Storage Essentials.
2. Insert the CD-ROM for installing the management server (Storage Essentials).
3. Double-click **SIMConnectorInstall.exe** in the top-level directory.
4. Follow the instructions on the screen for completing the installation.
5. When you see the HP-SIM Information screen, provide the following information:
 - **HP-SIM Hostname** - Name of the server on which you installed HP Insight Manager. Do not use localhost.
 - **HP-SIM Administrator Name** - Provide the Administrator name that is used to access System Insight Manager. For Microsoft Windows systems, use domain\Administrator name format.
 - **HP-SIM Administrator Password** - Provide the password for the Administrator.
6. Complete the installation by following the instructions on the screen.
7. Start AppStorManager, which is the service for Storage Essentials.
8. Change the password for SIM_MANAGER, as described in the following steps.

The information Storage Essentials and HP Systems Insight Manager share is stored in a database with the user name SIM_MANAGER and the password quake. It is strongly recommended you change the password for this database.

To change the password:

- a. Log onto the server running HP Systems Insight Manager.
- b. Enter the following at the command prompt:

```
C:\> mxpassword -m -x MxDBUserPassword=mynewPass  
where mynewPass is your new password for the database.
```

4 Discovering Filers, Tape Libraries, Switches, and Storage Systems

Before you can use the management server, you must make the software aware of the elements on your network. An element is anything on the network that can be detected by the management server, such as a switch. This is done through the discovery process. Discovery obtains a list of discovered elements and information about their management interface and dependencies. The management server can discover only elements with a suitable management interface. Refer to the support matrix for supported hardware.

First discover the switches, storage systems, filers, and tape libraries on your network by using the tools in Storage Essentials. Refer to the documentation available from Storage Essentials. Then, run Discovery Data Collection. Discovery Data Collection is required to obtain information from your switches and storage systems. Discovery Data Collection takes some time. You might want to perform this process when the network and the managed elements are not busy. After Discovery Data Collection, install the CIM Extensions. Then, discover your hosts, as described in ["Discovering Applications and Hosts"](#) on page 113.

Discovery of switches, storage systems, filers and tape libraries consists of several steps:

1. Discover your switches by using HP Systems Insight Manager. See ["Step 1 - Discover Switches"](#) on page 16.
2. Discover your storage systems, filers and tape libraries by using HP Systems Insight Manager. See ["Step 2 - Discover Storage Systems, Filers and Tape Libraries"](#) on page 28.
3. Obtain details about the elements you previously discovered by using the Discovery Data Collection feature in Storage Essentials. See ["Step 3 - Discovery Data Collection"](#) on page 41.

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

To save time, make sure the user names and passwords are correct. The management server tries each of the default user names and passwords whenever it finds an element.

Keep in mind the following:

- After you discover an EMC Connectrix or McDATA switch, the IP address displayed next to the name of the switch is actually the IP address of the service processor for the switch in the Discovery Data Collection screens. To find the IP address of the switch, click the link for the switch in the Discovery Data Collection screen (**Options > Storage Essentials > Discovery > Run Discovery Data Collection**) and then click the Properties tab. The Properties tab can also be accessed by double clicking the switch in System Manager. Complete the steps in this chapter before you try to find the IP address of the switch.
- If you are having a problem with discovering an element, see ["Troubleshooting"](#) on page 157.
- The IP addresses of excluded elements appear in the Discovery Data Collection lists (**Options > Storage Essentials > Discovery > Run Discovery Data Collection**). The management server does not display additional information about excluded elements in the user interface. .
- To obtain information about the storage area network (SAN), include in the discovery the IP addresses for the following:

- **Fibre channel switch** The fibre channel switch contains a list of all elements within the fabric. The management server obtains a detailed listing of all elements connected to the switch fabric.
- **A host containing a Host Bus Adapter (HBA)** All fibre channel host adapters look for available elements attached to the HBA. This information is gathered by CIM Extensions and sent to the management server. Since you have not installed CIM Extensions yet, the management server obtains limited information on the hosts when you perform discovery this time around.
- **A proxy connected to the SAN** - Include a proxy that has a direct connection or a SAN connection to the management server. An example of a proxy is the EMC Solutions Enabler or Hitachi HiCommand Device Manager. Engenio storage systems do not require a proxy, as they can be accessed directly. Make sure the proxy service has started. On a computer running Windows, this can be determined by looking in the Services window. EMC Solutions Enabler version 5.1 requires additional steps for discovery. See "[Discovering EMC Solutions Enabler 5.1](#)" on page 30 for more information.

Step 1 - Discover Switches

This section describes the following:

- "[Discovering Brocade Switches](#)" on page 17
- "[Discovering CNT Switches](#)" on page 18
- "[Discovering Cisco Switches](#)" on page 19
- "[Discovering Sun StorEdge and QLogic Switches](#)" on page 19
- "[Changing the SNMP Trap Listener Port for Sun StorEdge Switches](#)" on page 20
- "[Discovering McDATA and EMC Connectrix Switches](#)" on page 20
- "[Excluding McDATA and EMC Connectrix Switches from Discovery](#)" on page 26

The following table provides an overview of the discovery requirements for switches.

Table 3 Discovery Requirements for Switches

Element	Discovery Requirements	Additional Information
Brocade switches	Enter the IP address/DNS name, user name and password of the Brocade switch to discover it. The user name (default admin) and password must be the Admin Account.	See " Discovering Brocade Switches " on page 17.
CNT Switches	Enter the IP address followed by the port number for the InVsn Software that manages the switch.	See " Discovering CNT Switches " on page 18.

Table 3 Discovery Requirements for Switches (continued)

Element	Discovery Requirements	Additional Information
Cisco Switches	Enter the IP address/DNS name of the Cisco switch. You do not need to enter a password.	See "Discovering Cisco Switches" on page 19.
Sun StorEdge and QLogic switches	Enter the IP address/DNS name of the Sun StorEdge or QLogic switch. You do not need to enter a password.	See "Discovering Sun StorEdge and QLogic Switches" on page 19.
McDATA and EMC Connectrix switches	Additional steps are required for discovering these switches, and the steps vary according to your network configuration.	See "Discovering McDATA and EMC Connectrix Switches" on page 20.

IMPORTANT: Make sure you do not have pop-up blocking software enabled. If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.

Discovering Brocade Switches

IMPORTANT: Verify that the Rapid program on the switch is set to 1. Rapid must be set to 1 so that the management server can communicate with the switch. See ["Verifying Brocade Rapid Program Is Set to 1"](#) on page 17 for more information.

To discover Brocade switches, provide the following information in HP Insight Manager:

- IP address or DNS name of the Brocade switch you want to discover.
- User Name for the switch
- Password for the switch

Verifying Brocade Rapid Program Is Set to 1

If you are discovering Brocade switches, verify that the Rapid program on the switch is set to 1.

1. (Optional) Set the command prompt window so that it displays many rows.

While completing the following steps, the command prompt window displays a large amount of data. You might want to expand the size and buffer of the command prompt window. To do this in Microsoft Windows 2000, click the upper-right corner of the command prompt window, click the **Layout** tab, and then modify the options under Screen Buffer Size and Window Size.

2. Access the Brocade switch by using the telnet option. For example,

```
telnet  
open 10.1.213.228
```

where 10.1.213.228 is the IP address of the switch.

3. When prompted for the user name and password, supply them.

4. Type the following to see what is supported on the switch:

```
supportshow
```

A large amount of output is displayed.

5. Select all of the output.

6. Paste the output in a text editor, for example Notepad. Use the Find command to search for `rpc.rapid`.

7. Verify Rapid is set to one, as displayed below:

```
rpc.rapid:      1
```

Discovering CNT Switches

The management server uses the CNT SMI-S provider to discover CNT switches. A provider is a small software program that is used by the management server to communicate with a device, such as a switch.

This provider communicates with CNT InVsn Enterprise Manager to obtain information about the switch. The provider requires a certain version of InVsn depending on the switch model. See the following table for more information.

Table 4 Required Switch Models and InVsn Versions for Discovery

Switch Model	InVsn Software Version
FC/9000	9.0 or later
UMD	9.5 or later

Keep in mind the following for CNT switches:

- SNMP is not supported for CNT switches.
- CNT InVsn Enterprise Manager must be running for the management server to discover it.
- The management server does not support provisioning for CNT switches. Only the active zone set and its zone members are reported.
- No ports are reported for uninstalled blades or GBICs.

To discover CNT switches:

1. Before you can discover a CNT switch, you must do the following in the CNT InVsn Enterprise Manager software:

a. Open the file `ProductInfo.ini` in a text editor, such as Notepad. If the software was installed in the default directory, this file should be in the following directory:

```
\Program Files\CNT\inVSN_EM
```

b. Change the following entry in the file:

```
cimomenabled=TRUE
```

- c. Save the file, then restart the InVsn software.
2. In the **IP Address/DNS Name** field in HP Insight Manager, type the primary IP address of the host running the InVsn software you want to discover followed by its port number. For example, if the InVsn software is running at 192.168.10.76 on port 5989, you would specify the IP Address and port number as follows:
192.168.10.76:5989
3. In the **User Name** field, type the user name for the login to the InVsn software.
4. In the **Password** field type the password for the login to the InVsn software.
5. In the **Verify Password** field type the password you provided previously.
6. Start discovery.

Discovering Cisco Switches

The management server discovers Cisco switches through an SNMP connection. When you discover a Cisco switch, you do not need to provide a password.

Keep in mind the following for Cisco switches:

- You can view zones, zone sets and zone aliases on a Cisco switch; however, you cannot use the management server to create, modify or remove them from a Cisco switch.
- The management server gathers information about the Cisco inactive database during Discovery Data Collection. You can change the amount of information that is collected by modifying a property. See the User Guide for more information.
- The management server groups active zone sets in all Virtual SANs (VSANs) in a fabric into a zone set called "ACTIVE", and the "ACTIVE" zone set is shown associated with the physical fabric. The members of the "ACTIVE" zone set (zones, zone sets, zone aliases) have the name of the VSAN prefixed to their name. For example, an active zone named "ZONE1" from a VSAN named "VSAN1" is displayed as a zone on the physical fabric with name "VSAN1:ZONE1".

To discover a Cisco switch in HP Insight Manager, you must provide the following:

- DNS name or primary IP address of the Cisco switch you want to discover
- User name for the switch. The password can be left blank.

Discovering Sun StorEdge and QLogic Switches

The management server discovers Sun StorEdge and QLogic switches through an SNMP connection. When you discover a Sun StorEdge or QLogic switch, you do not need to provide a password.

Keep in mind the following:

- The management server does not support provisioning for Sun StorEdge and QLogic switches. Only the active zone set and its zone members are reported.
- To manage a fabric of Sun StorEdge and/or QLogic switches, every switch in the fabric must be included in the discovery list. If a switch is not included in the discovery list, it may show up as a generic host system.
- No ports are reported for uninstalled blades or GBICs.

- The default SNMP trap listener port for all Sun StorEdge switches is 162. To change this port, see “[Changing the SNMP Trap Listener Port for Sun StorEdge Switches](#)” on page 20.
- To receive events from Sun StorEdge switches, verify the SNMP trap community string is set to public in SANbox Manager or via telnet. Also, make sure the SNMP traps are configured to be sent to the management server.

To discover a Sun StorEdge or QLogic switch in HP Insight Manager, provide the following:

- IP Address or DNS name of the Sun StorEdge or QLogic switch you want to discover.
- The user name for the switch. This is the public community SNMP string (read community password) for the switch. This field can be left blank if the element's user name and password are one of the default user names and passwords. You do not need to provide a password.

Changing the SNMP Trap Listener Port for Sun StorEdge Switches

The default SNMP trap listener port for all Sun StorEdge switches is 162. To change this port for all switches that are discovered through SNMP, modify the `cimom.snmpTrapListenerPort` property as described in the following steps:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.snmpTrapListenerPort` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Set the `cimom.snmpTrapListenerPort` property to the port you want, as shown in the following example:

```
cimom.snmpTrapListenerPort=162
```
8. When you are done, click **Save**.
9. Restart the service for the management server for your changes to take effect.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Discovering McDATA and EMC Connectrix Switches

McDATA and EMC Connectrix switches use the Fibre Channel Switch Application Programming Interface (SWAPI) to communicate with devices on the network. The management server can discover multiple instances of Enterprise Fabric Connectivity Manager.

Use one of the following techniques to discover McDATA and Connectrix switches:

Table 5 Discovery Settings for McDATA and Connectrix Switches

Discovery	SWAPI setting through a Proxy	SNMP setting Through a Proxy	Contacting the switch directly
Description	Use this option if you have Enterprise Fabric Connectivity (EFC) Manager. You will need to connect through the proxy instead of the switch. See "SWAPI Setting Through a Proxy" on page 22 for more information.	Contact the switch through a proxy. You can use this option with EMC Connectrix™ Manager and Enterprise Fabric Connectivity (EFC) Manager to contact the switch. See "SNMP Setting Through a Proxy" on page 24 for more information.	Contact the switch by its IP address or DNS name. This connection uses SNMP. See "Contacting a McDATA or Connectrix Switch Directly" on page 25.
Provisioning Limitations	The SWAPI setting lets you activate a zone set, in addition to creating, editing, and deleting zones and zone sets. You cannot manage or view information about zone aliases.	This SNMP setting through a proxy does not let you manage or access information about zones, zone sets or zone aliases.	This SNMP setting provides view only access to the active zone set and its members. You cannot create, modify, and/or delete zone sets or its members.

Keep in mind the following:

- If you change a discovery configuration from SNMP to SWAPI or vice versa, the user ID and password will no longer work. For this reason, it is recommended that you set this property before discovering any McDATA switches. If you must change the configuration, see ["Changing the Discovery Settings"](#) on page 26.
- After you discover a McDATA or Connectrix switch through a proxy, the IP address displayed next to the name of the switch is actually the IP address of the proxy for the switch in the Discovery, and Discovery Data Collection screens. To find the IP address of the switch, click the link for the switch in the Discovery Data Collection screen (**Discovery > Details**) and then click the **Properties** tab. The **Properties** tab can also be accessed by double clicking the switch in System Manager.
- If you want to add, remove, or replace McDATA or Connectrix switches after you have discovered the service processor, you must perform additional steps, see ["About Managing McDATA and EMC Connectrix Switches"](#) on page 45.

- If you have problems obtaining information from McDATA or Connectrix switches during discovery and/or Discovery Data Collection, see ["Step 2 - Discover Storage Systems, Filers and Tape Libraries"](#) on page 28.
- All McDATA switches in a fabric must be managed by the same EFC Manager. Do not have more than one EFC Manager to a fabric for McDATA switches. If you do use more than one EFC Manager in a fabric, you must use the same EFC Manager for your zoning. Do not use the other EFC Managers for zoning, as this will create zoning database problems.
- All Connectrix switches in a fabric must be managed by the same Connectrix Manager. Do not have more than one Connectrix Manager to a fabric for Connectrix switches. If you do use more than one Connectrix Manager in a fabric, you must use the same Connectrix Manager for your zoning. Do not use the other Connectrix Managers for zoning, as this will create zoning database problems.
- If you want the management server to receive SNMP events from Connectrix or McDATA switches, do one of the following:
 - If you discovered Connectrix Manager or EFC Manager, only enable SNMP trap forwarding to the management server on the Connectrix Manager or EFC Manager, not on the individual switches. Connectrix Manager or EFC Manager should be configured to forward SNMP traps to the IP address of the management server, and the community string should match the user ID you used to discover Connectrix Manager or EFC Manager.
 - If you discovered Connectrix or McDATA switches directly, enable SNMP trap forwarding on the switches, not on any other management software. The switches should be configured to forward SNMP traps to the IP address of the management server, and the community string should match the user ID you used to discover the Connectrix or McDATA switches.

SWAPI Setting Through a Proxy

With the SWAPI setting, the management server contacts a proxy to obtain information about the switches connected to it. Use Enterprise Fabric Connectivity (EFC) Manager for this option. If you do not have EFC Manager, see ["SNMP Setting Through a Proxy"](#) on page 24. EFC Manager versions 7.0 and later can communicate with the management server and the switch. EFC Manager accesses the switch through a SWAPI connection. This configuration lets multiple instances of the management server or other clients contact EFC Manager, which in turn provides information about the switch.

IMPORTANT: This option only supports McDATA switches. If you want to discover EMC Connectrix switches, you must discover them through the SNMP provider, either directly or through a proxy. See ["SNMP Setting Through a Proxy"](#) on page 24 for more information about using the SNMP provider to discover switches through a proxy. See ["Contacting a McDATA or Connectrix Switch Directly"](#) on page 25 for more information discovering switches by their IP address.

Step 1 - (McDATA Switches Only) Install the Bridge Agent

To communicate with EFC Manager, the management server requires the Bridge Agent. Refer to your McDATA representative for more information about the Bridge Agent.

Step 2 - Change the Discovery Setting for McDATA and Connectrix Switches to SWAPI

To change the discovery settings to SWAPI:

1. Click **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.

```
cimom.useSnmPmcDataProvider=FALSE
```

4. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Uncomment the `cimom.useSnmPmcDataProvider` property by removing the number sign (#) in front of `cimom.useSnmPmcDataProvider`.
7. Verify the `cimom.useSnmPmcDataProvider` property is set to false.
8. When you are done, click **Save**.
9. Restart the service for the management server for your changes to take effect.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Step 3 - Discover the Proxy

To discover the proxy, you must provide the following information to HP Insight Manager:

- IP address or DNS name of the EFC Manager/Connectrix Manager you want to discover
- User name - Type the user name for EFC Manager/Connectrix Manager.
This field can be left blank if one or more of the following conditions are fulfilled:
 - The element's user name and password are one of the default user names and passwords.
 - The element does not require authentication.
- Password - Type the corresponding password for EFC Manager/Connectrix Manager.
This field can be left blank if one or more of the following conditions are fulfilled:
 - The element's user name and password are one of the default user names and passwords.
 - The element does not require authentication.

CIM_ERR_FAILED When Trying to Activate a Zone Set Using McDATA SWAPI

When the user tries to activate a zone set using McDATA SWAPI, the operation may return CIM_ERR_FAILED with one of the following detailed messages:

```
Cannot activate zone set. SWAPI Handle is not valid for fabric  
Cannot activate zone set. Active zone set information is out of date for  
fabric
```

```
There is no active SWAPI connection for fabric
Fabric is not in the cache
```

These error messages indicate that the SWAPI connection to the EFCM managing the fabric is no longer valid, or the active zone information was changed on the fabric without using the management server. The management server does not activate a zone set under these conditions.

To fix this problem, re-discover the EFCM to re-establish the SWAPI connection.

Once the connection is working, the provisioning operation should succeed. If it continues to fail because the active zone set information is out of date, do a Discovery Data Collection for this element to update the zoning information.

SNMP Setting Through a Proxy

This SNMP setting through a proxy does not let you manage or access information about zones, zone sets or zone aliases.

This option is required if you want to discover McDATA or Connectrix switches through a proxy using the SNMP provider. You can use this option with EMC Connectrix™ Manager and Enterprise Fabric Connectivity (EFC) Manager to contact the switch.

Step 1 - Verify the Discovery Setting for Switches Is Set to SNMP

By default the discovery settings for McDATA and Connectrix switches is set to SNMP. If you believe it has been changed to SWAPI, you can perform the following steps to change it back to SNMP.

1. Click **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click the **Edit** button at the bottom of the page.
3. Comment out the `cimom.useSnmpMcDataProvider` property by placing the number sign (#) in front of `cimom.useSnmpMcDataProvider`.
`#cimom.useSnmpMcDataProvider=false`
4. Restart the service for the management server.
5. Verify the following on the proxy and the switches accessible from the proxy:
 - The SNMP agent is enabled.
 - The read-only community string is configured.

Step 2 - Discover the Proxy

To discover the proxy, you must provide the following information to HP Insight Manager:

- IP address or DNS name of the EFC Manager/Connectrix Manager you want to discover
- User name - The default user name, which is “public” (the read-only community string). This is the user name of the proxy.

IMPORTANT: To access a Windows-based device, prepend the user name with the Windows domain name, as shown in the following example.

```
domain_name\user_name
```


where

- `domain_name` is the domain name of the machine
- `user_name` is the name of your network account
- Password - You can leave the password field blank, where it is being accessed through SNMP.

Step 3 - Make Sure There Are No Port Conflicts for Receiving SNMP Traps

When the management server is configured to contact the proxy by SNMP, the management server receives events from the proxy in the form of SNMP traps. By default, the management server uses port 162 to receive SNMP traps. If another software package is using that port, the management server is unable to receive the traps. To change the port the management server uses:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click the **Edit** button at the bottom of the screen.
3. Set the `cimom.snmpTrapListenerPort` to another port, as shown in the following example:

```
cimom.snmpTrapListenerPort=1234
```

where 1234 is the new port

4. When you are done making your changes, click the **OK** button.
5. Restart the service for the management server for your changes to take effect.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Step 4 - Step Up the Proxy to Send Traps to the Correct Port

When you are using the SNMP setting to discover a proxy, you must configure the SNMP agent on the proxy manager to send traps to the management server using the port you selected. This configuration sends traps from all switches managed by that proxy. Refer to your documentation for your proxy for more information.

Contacting a McDATA or Connectrix Switch Directly

To discover a McDATA or Connectrix switch directly, provide the following to HP Insight Manager:

- The IP address or DNS name of the switch you want to discover.
- The user name for accessing the switch. The default user name is "public" (the read-only community string).
- No password. The password does not matter since the management server is not doing any configurations through SNMP.

Make Sure There Are No Port Conflicts for Receiving SNMP Traps

When the management server is configured to contact a switch by SNMP, the management server receives events from the switch in the form of SNMP traps. By default, the management server uses port 162 to receive SNMP traps. If another software package is using that port, the management server is unable to receive the traps. To change the port the management server uses:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click the **Edit** button at the bottom of the screen.
3. Set the `cimom.snmpTrapListenerPort` to another port, as shown in the following example:

```
cimom.snmpTrapListenerPort=1234  
where 1234 is the new port
```

4. When you are done making your changes, click the **OK** button.
5. Restart the service for the management server for your changes to take effect.
While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Configure the SNMP Agent to Send Traps to the Correct Port

When you are using the SNMP setting to discover a switch, you must configure the SNMP agent on the switch to send traps to the management server using the port you selected. Refer to your documentation for your switch for more information.

Changing the Discovery Settings

To change the discovery settings from SWAPI to SNMP or vice versa:

1. Delete all McDATA and Connectrix switches in the application.
2. Click **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
3. Click the **Edit** button at the bottom of the page.
4. Change the `cimom.useSnmpMcDataProvider` property as follows:
 - **SNMP setting** - Comment out the `cimom.useSnmpMcDataProvider` property by placing a number sign (#) in front of the `cimom.useSnmpMcDataProvider` property as follows: `#cimom.useSnmpMcDataProvider=false`
 - **SWAPI setting** - Remove the number sign (#) in front of the `cimom.useSnmpMcDataProvider` property.
5. Restart the service for the management server.
6. Add new elements in the Discovery screen.
 - **SWAPI connection** - Enter the IP address, user name and password for the proxy.
 - **SNMP connection** - Enter the IP address of the proxy. The default user name is "public" (the read-only community string). The password does not matter since the management server is not doing any configurations through SNMP.
7. Verify the following on the proxy and the switches accessible from the proxy:
 - The SNMP agent is enabled.
 - The read-only community string is configured.
8. Start discovery in HP Insight Manager.
9. Perform Discovery Data Collection.

Excluding McDATA and EMC Connectrix Switches from Discovery

Specific McDATA and Connectrix switches can be excluded from discovery by using system properties.

To exclude one or more switches from discovery, you must modify the `cimom.mcddata.exclude` property. Set the property `cimom.mcddata.exclude` to a comma separated list of Worldwide Names of the McDATA and Connectrix switches you want excluded, as shown in the following example:

```
cimom.mcddata.exclude=1000080088A07024,1000080088A0D0B6
```

The management server excludes the switches with one of the following Worldwide Names: 1000080088A07024 and 1000080088A0D0B6

If the `cimom.mcddata.exclude` property is not modified, the management server discovers and obtains details from all McDATA and Connectrix switches.

IMPORTANT: The IP addresses of excluded elements appear in the Discovery Data Collection lists. The management server does not display additional information about excluded elements in the user interface.

To modify the `cimom.mcddata.exclude` property:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.mcddata.exclude` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Add the Worldwide Names corresponding to the switches you want to exclude from discovery. Separate additional Worldwide Names with a comma, as shown by the following example:

```
cimom.mcddata.exclude=1000080088A07024,1000080088A0D0B6
```

where 1000080088A07024 and 1000080088A0D0B6 are the Worldwide Names for McDATA and Connectrix switches.

8. When you are done, click **Save**.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Viewing Log Messages

Use the **View Logs** tab to obtain the status of the following:

- Discovery Data Collection

During these operations, the management server displays its status at regular intervals.

To view logs for these operations:

1. Click the **Tasks & Logs > View Storage Essentials Log**.
2. To obtain the latest status, click the **Get Latest Messages** button.

If the software is unable to discover or obtain information about a device, the log messages might provide some information as to where the problem occurred.

For example, if a host was not discovered, the log messages might indicate the provider configuration for that device was never created. This could mean the software was given the wrong user name and/or password for that host. As a result, the software logged onto the host with a guest account, which does not have enough permissions to start WMI.

IMPORTANT: Look at Event Monitoring for Storage Essentials for additional information. See ["About Event Manager"](#) on page 532 for more information.

Duplicate Logs for Brocade Switches in Same Fabric

If you discover more than one Brocade switch in the same fabric, the discovery log displays duplicate listings for the Brocade switches. Each Brocade switch is listed multiple times with the IP address of the other switches and its own.

For example, assume you are discovering Brocade switches QBrocade2 and QBrocade5 in the same fabric, two duplicate entries are displayed in the log. QBrocade2 is listed twice, once with its own IP address, the other time with the IP address of QBrocade5, as shown below.

```
[Nov 27, 2002 8:45:05 AM] Discovered Switch: QBrocade2 at 192.168.10.22
[Nov 27, 2002 8:45:09 AM] Discovered Switch: QBrocade5 at 192.168.10.22
[Nov 27, 2002 8:45:09 AM] Enabling provider configuration:
APPIQ_BrocadeElementManagerConfig
[...]
[Nov 27, 2002 8:45:37 AM] Discovered Switch: QBrocade2 at 192.168.10.25
[Nov 27, 2002 8:45:42 AM] Discovered Switch: QBrocade5 at 192.168.10.25
[Nov 27, 2002 8:45:42 AM] Enabling provider configuration:
APPIQ_BrocadeElementManagerConfig
192.168.10.22 Switch QBrocade2, QBrocade5 admin
192.168.10.25 Switch QBrocade2, QBrocade5 admin
```

Step 2 - Discover Storage Systems, Filers and Tape Libraries

- ["Discovering EMC Solutions Enabler 5.1"](#) on page 30
- ["Excluding EMC Symmetrix Storage Systems from Discovery"](#) on page 31
- ["Discovering EMC CLARiiON Storage Systems"](#) on page 32

- ["Discovering HDS Storage Systems"](#) on page 33
- ["Excluding HDS Storage Systems from Discovery"](#) on page 34
- ["Discovering HP StorageWorks Arrays"](#) on page 35
- ["Discovering Engenio Storage Systems"](#) on page 35
- ["Discovering NetApp Filers"](#) on page 36
- ["Discovering Sun StorEdge 3510 Storage Systems"](#) on page 37
- ["Discovering Sun StorEdge 6920 Storage Systems"](#) on page 38
- ["Discovering Sun StorEdge 6130 Storage Systems"](#) on page 38
- ["Discovering IBM Storage Systems"](#) on page 38
- ["Discovering IBM Tape Libraries"](#) on page 39

Table 6 Discovery Requirements for Storage Systems and NAS Filers

Element	Discovery Requirements	Additional Information
EMC CLARiiON storage systems	The EMC Navisphere CLI is required for the management server to communicate with the CLARiiON storage system.	See "Discovering EMC CLARiiON Storage Systems" on page 32 for more information.
EMC Symmetrix storage system (Including EMC Symmetrix DMX storage systems)	Discover the server running the EMC Solutions Enabler.	See "Discovering EMC Solutions Enabler 5.1" on page 30 for more information.
HDS storage systems	Discover the server running HiCommand Device Manager.	See "Discovering HDS Storage Systems" on page 33 for more information.
HP storage systems	Discover the server running the HP CIMOM.	See "Discovering HP StorageWorks Arrays" on page 35.

Table 6 Discovery Requirements for Storage Systems and NAS Filers (continued)

Element	Discovery Requirements	Additional Information
Engenio storage systems	<p>Can be discovered two ways:</p> <ul style="list-style-type: none"> • Entering the IP address/DNS name, user name and password of a controller for an Engenio storage system. Discovers only the corresponding IP address of the controller. • Entering the IP address/DNS name, user name and password of a proxy that is used to manage an Engenio storage system. Discovers all controllers known to the proxy. 	See "Discovering Engenio Storage Systems" on page 35.
NetApp Filer	Discover the filer directly.	See "Discovering NetApp Filers" on page 36.
Sun StorEdge 3510	Discovered through proxy software called Sun StorEdge™ Configuration Service. On the discovery page the user should enter the hostname or IP address of the computer running the Sun StorEdge 3510 SMI-S provider.	See "Discovering Sun StorEdge 3510 Storage Systems" on page 37.
Sun StorEdge 6920	Discover the storage system directly.	See "Discovering Sun StorEdge 6920 Storage Systems" on page 38.
Sun StorEdge 6130	Discover the storage system directly. The username does not matter. The password matters only for provisioning.	See "Discovering Sun StorEdge 6130 Storage Systems" on page 38.
IBM Storage Systems	Discover the CIMOM that talks to the IBM storage systems you want to monitor.	See "Discovering IBM Storage Systems" on page 38.
IBM Tape Libraries	Provide the IP address, namespace, user name and password for the tape library.	See "Discovering IBM Tape Libraries" on page 39

Discovering EMC Solutions Enabler 5.1

EMC Solutions Enabler restricts access to itself through the nethost file. If present, the nethost file is located in the same directory as the netcnfg file. If you are using a nethost file, edit it to allow the management server to discover the Solutions Enabler and the Symmetrix storage systems that it manages.

IMPORTANT: Use a nethost file unless you are running a version of the Solutions Enabler earlier than the 5.1 version. You must have the license installed for the Solutions Enabler. The nethost file provides access to the Solutions Enabler API.

Sometimes you can access an EMC Symmetrix storage system through several Solutions Enabler servers. In this case if you do not have access to a particular Solutions Enabler, you may still be able to access the Symmetrix storage system through another Solutions Enabler.

If you do not have a nethost file, you may need to create one. For example, assume you are running Solutions Enabler on a Solaris server, you would create a nethost file as described in the following steps. Refer to the documentation for Solutions Enabler for other operating systems.

1. Create a file called "nethost" in the `/opt/emc/API/symapi/config` directory.
2. Add the following lines to the nethost file:

```
<management server name> SYSTEM  
<management server IP> SYSTEM
```

where

- `<management server name>` is the DNS name of the management server
- `<management server name>` is the IP address of the management server

3. Add the following line to the `/opt/emc/API/symapi/config/netcnfg` file:

```
SYMAPI_SERVER - TCPIP <IP of SymAPI server> 2707
```

4. Use the following command to start the daemon:

```
/opt/emc/SYMCLI/V5.5.0/bin/symapisrv -service SYMAPI_SERVER start  
-background
```

5. Use the following command to stop the daemon:

```
/opt/emc/SYMCLI/V5.5.0/bin/symapisrv stop
```

6. You may need to discover the Symmetrix arrays the SymAPI server can see by running the following command:

```
/opt/emc/SYMCLI/V5.5.0/bin/symcfg discover
```

IMPORTANT: If error 214 is present in the discovery log and/or cimom.log during discovery, this means the SymAPI server is not licensed for remote connections. The end-user will have to acquire and install the license before discovery can occur.

Required Licenses

If you want to use all of the features of the management server, such as provisioning, with an EMC Symmetrix storage system, you must have licenses for the following products:

- BASE
- DeltaMark
- SERVER
- DevMasking
- Config Manager
- Mapping (SOLUTION_4)

Excluding EMC Symmetrix Storage Systems from Discovery

When multiple EMC Symmetrix storage systems are managed through a single Solutions Enabler, specific storage systems may be excluded from discovery by using system properties.

To exclude one or more Symmetrix storage systems from discovery, you must modify the `cimom.symmetrix.exclude` property. Set the property `cimom.symmetrix.exclude` to a comma separated list of serial numbers of the storage systems you want excluded, as shown in the following example:

```
cimom.symmetrix.exclude=000183500570,000183610580
```

The management server excludes the storage systems with one of the following serial numbers: 000183500570 and 000183610580.

If the `cimom.symmetrix.exclude` property, the management server discovers and obtains details from all EMC Symmetrix Storage Systems managed by discovered Solutions Enablers.

IMPORTANT: The IP addresses of excluded elements appear in the Discovery Data Collection lists (**Discovery > Details**). The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Discovery > View Logs**) that a provider instance has been created for an excluded element. You can ignore this message that appears in the logs.

To modify the `cimom.symmetrix.exclude` property:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.


```
#cimom.symmetrix.exclude=000183500570,000183500575
```
4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the Symmetrix storage systems you want to

exclude from discovery. Separate additional serial numbers with a comma, as shown by the following example:

```
cimom.symmetrix.exclude=000183500570,000183500575
```

where 000183500570 and 000183500575 are serial numbers for Symmetrix storage systems.

7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect.
While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Discovering EMC CLARiiON Storage Systems

The EMC Navisphere® CLI must be installed on the management server for the management server to communicate with the CLARiiON® storage system. At the time this documentation was created, EMC distributed the Navisphere CLI as part of the EMC Navisphere Software Suite. Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC. For Solaris, you must install the Navisphere Disk Array Management Tool CLI (NAVICLI).

Contact your EMC representative for more information about obtaining the Navisphere CLI. Distribution rights for the Navisphere CLI belong to EMC.

IMPORTANT: Before you discover your CLARiiON storage systems, you must have already installed all required software components for your CLARiiON storage system, such as the Navisphere Host Agent. Refer to the documentation for your storage system for more information.

In Navisphere Manager add one of the following to the privilege user section:

```
SYSTEM@name_of_my_management_server  
SYSTEM@IP_of_my_management_server
```

where

- `name_of_my_management_server` is the DNS name of the computer running the management server software
- `IP_of_my_management_server` is the IP address of the computer running the management server software

When you use the management server to discover the CLARiiON storage system, provide the IP address for the CLARiiON storage system and the user name and password used to log into Navisphere.

Discovering HDS Storage Systems

HiCommand Device Manager is required for the management server to communicate with an HDS storage system. To discover an HDS storage system, enter the IP address, user name and password

for the server running HiCommand Device Manager. Do not point to the disk array for the storage system.

To obtain information about HDS storage systems, the management server must be able to access the port HiCommand Device Manager uses to listen. By default, HiCommand Device Manager listens on port 2001, and the management server assumes this configuration at discovery time. If HiCommand Device Manager uses a different port, specify this other port when you discover HiCommand Device Manager.

Keep in mind the following:

- You cannot scan an IP range to discover an instance of HiCommand Device Manager that listens on a port other than 2001. The management server does not allow port numbers in the scanning of IP ranges, and thus, you are not able to specify the port.
- The management server communicates with HiCommand Device Manager through a nonsecure connection. If you want the management server to communicate with HiCommand Device Manager through a secure sockets layer (SSL) connection, you must modify an internal property or use HTTPS when you discover HiCommand Device Manager. See [“Communicating with HiCommand Device Manager Over SSL”](#) on page 175.

To discover an HDS storage system that listens on a port other than 2001, you must provide the following information to HP Insight Manager:

- The name of the server and the port HiCommand Device Manager uses to listen separated by a colon, as shown in the following example:

```
proxy2:1234  
where
```

- `proxy2` is the name of the server running HiCommand Device Manager
- `1234` is the port HiCommand Device Manager uses to listen
- User name for HiCommand Device Manager.
- Password for HiCommand Device Manager.

Excluding HDS Storage Systems from Discovery

When multiple HDS storage systems are managed through a single HiCommand Device Manager, specific storage systems may be excluded from discovery by using system properties.

To exclude one or more HDS storage systems from discovery, you must modify the `cimom.hds.exclude` property. Set the property `cimom.hds.exclude` to a comma separated list of serial numbers of the storage systems you want excluded, as shown in the following example:

```
cimom.hds.exclude=61038,61037
```

The management server excludes the storage systems with one of the following serial numbers: 61038 and 61037.

If the `cimom.hds.exclude` property is not specified, the management server discovers and obtains details from all HDS storage systems managed by the discovered HiCommand Device Manager.

The IP addresses of excluded elements appear in the Discovery Data Collection lists (**Discovery > Details**). The management server does not display additional information about excluded elements in the user interface. To modify the `cimom.hds.exclude` property:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.

```
#cimom.hds.exclude=61038,61037
```

4. Return to the Advanced page.
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the HDS storage systems you want to exclude from discovery. Separate additional serial numbers with a comma, as shown by the following example:

```
cimom.hds.exclude=61038,61037
```

where 61038 and 61037 are serial numbers for HDS storage systems.

7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect.
While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

Discovering HP StorageWorks Arrays

HP CIMOM is required to discover HP StorageWorks XP Arrays, Enterprise Virtual Arrays (EVA) and Modular Smart Arrays (MSA). To discover an HP XP, EVA, or MSA storage system, you must enter the following information for the instance of the HP CIMOM used to manage the storage system. For XP storage systems, HP CIMOM is used to communicate with Command View.

- user name and password used for accessing the HP CIMOM
- IP address of the server containing the HP CIMOM

The following should be installed on a server before you discover an HP storage system:

- HP Storage Management Appliance software
- HP OpenView Storage Operations Manager
- HP StorageWorks Command View EVA, XP or MSA
- One of the following providers:
 - **XP Arrays** - HP StorageWorks SMI-S XP
 - **EVA Arrays** - HP StorageWorks SMI-S EVA
 - **MSA Arrays** - HP StorageWorks SMI-S MSA

Provisioning is supported for HP XP storage systems, but not completely for HP MSA and EVA storage systems. See [Table 10-3](#) on page 437 and [Table 10-4](#) on page 438.

To discover HP storage systems, provide the following information in HP Insight Manager:

- IP address or DNS name of the HP CIMOM you want to discover.
- User name for accessing the HP CIMOM
- Password for accessing HP CIMOM.

(XP arrays only) If you have Command View version 2.0 or later, the default password is administrator. If you have Command View earlier than version 2.0, refer to the documentation that shipped with Command View for the default password.

Discovering Engenio Storage Systems

Keep in mind the following when discovering an Engenio storage system:

- Discover all controllers on an Engenio storage system by entering the IP address of each controller.
- The management server must have the User Name field populated to discover the Engenio storage system. If your Engenio storage system does not have a user name set, you must enter something in the **User Name** field, even though the storage system has no user name.
- Discover both controllers for the Engenio storage system. Each controller has its own IP address. In Step 1 of discovery, specify all the IP addresses for all the controllers (usually two). The management server discovers these controllers as one single storage system.
- To obtain drive-related statistics, install a proxy host. Ensure the proxy host has at least one LUN rendered by each controller of the array. See the topic, "[Obtaining Disk Drive Statistics from Engenio Storage Systems](#)" on page 132 for more information.
- A license key is required for each storage system and that the key is obtained from the Web site specified on the Activation Card that shipped with your storage system.
- Engenio storage systems do not require a password for Discovery Data Collection. If you want do not want to use the management server for provisioning on Engenio storage systems, you can leave the password field blank and select the **Do Not Authenticate** option. The management server will still monitor the Engenio storage system; however, you will not be able to do provisioning tasks.

To discover Engenio storage systems, provide the following information in HP Insight Manager:

- IP address or DNS name of the controller or proxy you want to discover.
- User name for the storage system. If your Engenio storage system does not have a user name, you must enter something in the **User Name** field, even though the storage system has no user name.
- Password for the controller or proxy.

Discovering NetApp Filers

Keep in mind the following:

- SNMP must be enabled on the NetApp Filer before it can be discovered.

- If you want the management server to be able to receive events from a NetApp Filer, you must add the IP address of the management server to the NetApp configuration. The management server runs on the same computer running the management server by default.
- You must provide a privileged login, which is one of the following:
 - the root user
 - a user belonging to the “Administrators” group. This is a predefined group by NetApp.
 - a user belonging to a group that has the following roles: api-*, cli-*, login-http-admin, and at least one of the following: login-console, login-telnet, login-rsh, or login-ssh
- Administrative HTTP access to the device can be restricted through the httpd.access and httpd.admin.access options. If that is the case, then the management server needs to be registered with the device. This is done by adding the IP addresses of the management server to the httpd.admin.access option. More information related to this option is available in the NetApp documentation.

To discover a NetApp Filer, provide the following information in HP Insight Manager:

- IP address or DNS name of the NetApp Filer you want to discover.
- User name of the NetApp Filer. You must provide a privileged login.
- Password used to access the NetApp Filer.

Discovering Sun StorEdge 3510 Storage Systems

Before you can discover a Sun StorEdge 3510 storage system, you must set up a Sun StorEdge 3510 SMI-S provider and a Sun StorEdge™ Configuration Service. The provider cannot be installed on the same computer as the management server due to a port conflict.

The Sun StorEdge™ Configuration Service can be installed in one of the following locations:

- on the same computer as the Sun StorEdge 3510 SMI-S provider
- on the management server
- on a separate computer

To install the Sun StorEdge™ Configuration Service you must install the following packages:

- Sun StorEdge™ Configuration Service Console (SUNWscsu)
- Sun StorEdge™ Configuration Service Agent (SUNWscsd)
- Sun StorEdge™ Diagnostic Reporter Agent (SUNWscsa)

You must also install the following packages. Contact Sun technical support for information on how to obtain and configure these packages.

- WBEM Solutions J WBEM Server 1.0
- Sun StorEdge™ CIM/WBEM Provider SDK (SUNWagsdk package) - A readme file is installed as part of SUNWagsdk package. Follow the instructions in that readme file.
- Sun StorEdge™ 3510 SMI-S Provider (SUNW3x10a package) - A readme file is installed as part of SUNW3x10a package. Follow the instructions in that readme file.

To discover Sun StorEdge 3510 storage systems, you must discover the Sun StorEdge 3510 SMI-S provider. To discover a Sun StorEdge 3510 storage system, you must enter the following information for the instance of the Sun StorEdge 3510 SMI-S provider.

- user name and password used for the system running Sun StorEdge 3510 SMI-S provider
- IP address of the system running Sun StorEdge 3510 SMI-S provider

IMPORTANT: The management server is unable to display logical volumes configured on Sun StorEdge 3510 storage systems. Any logical volumes as well as the logical drives that comprise them will not appear in the UI. There will be no indication that this happened.

To discover Sun StorEdge 3510 storage systems, provide the following information in HP Insight Manager:

- IP address or DNS name of the system running the Sun StorEdge 3510 SMI-S provider you want to discover.
- User Name of the system running the Sun StorEdge 3510 SMI-S provider.
- Password of the Sun StorEdge 3510 SMI-S provider.

Discovering Sun StorEdge 6920 Storage Systems

To discover Sun StorEdge 6920 storage systems, provide the following information in HP Insight Manager:

- IP address or DNS name of the Sun StorEdge 6920 you want to discover.
- User name of the Sun StorEdge 6920 you want to discover.
- Password of the Sun StorEdge 6920 you want to discover.

Discovering Sun StorEdge 6130 Storage Systems

To discover Sun StorEdge 6130 storage systems, provide the following information in HP Insight Manager:

- IP address or DNS name of the controller or proxy you want to discover.
- The user name can be left blank.
- Password for the controller or proxy.

Discovering IBM Storage Systems

Before you can discover an IBM storage system, you must install:

- The IBM CIMOM, which is used to communicate with IBM storage systems. The IBM CIMOM can be installed on any host that has access to the IBM storage system. Obtain the IBM CIMOM from IBM.
- The IBM CIM Agent on a host and configured to manage one or more Enterprise Storage Server (ESS) devices. Do not install the IBM CIM Agent on the management server. Refer to the CIM Agent for the ESS - Installation and Configuration Guide for details on configuring the CIM Agent. In short, this procedure entails:

- a. Installing the software. The installation checks for the existence of the ESSCLI. If the ESSCLI is not installed, installation of the CIM Agent cannot proceed. The ESSCLI is typically pre-installed on the ESS management server that was configured by the IBM field technician.
- b. Configuring of protocol and ports used to communicate with the CIM Agent. You can change the CIM Agent port value, protocol (HTTP/HTTPS), and enable or disable the debug option.
- c. Using the setuser command to configure a user to access the CIM Agent. The user credentials specified here are used to access the CIMOM and are specified in the Discovery Step 1. The credentials are not necessarily the same as those used to login to the ESS Specialist management utility.
- d. Using the setdevice command to configure the ESS devices that are managed through the CIM Agent. The setdevice command requires a valid user that has the necessary privileges to access and configure the ESS storage system.
- e. Verifying that the CIM Agent is able to communicate with the ESS devices.

NOTE: Elements that were discovered through the IBM CIMOM cannot be moved to another discovery group.

To discover an IBM storage system, provide the following information in HP Insight Manager:

- In the **IP Address/DNS Name** field, enter one of the following for the system running the IBM CIMOM you want to discover.
 - <host> - CIM Agent has been configured to use the HTTP protocol
 - https://<host>:5989 - CIM Agent has been configured to use the HTTPs protocol
- Provide the interop namespace as described in the online help for HP Systems Insight Manager. The namespace for an IBM storage system is usually /root/ibm.
- User name of the system running the IBM CIMOM.
- Password of the system running the IBM CIMOM.

Discovering IBM Tape Libraries

To discover a tape library, provide the following information in HP Systems Insight Manager:

- In the **IP Address/DNS Name** field, enter the IP address or DNS Name for the tape library.
- Provide the interop namespace as described in the online help for HP Systems Insight Manager. The namespace for an IBM tape library is usually /root/ibm.
- User name of the tape library.
- Password of the tape library.

Modifying the Properties of a Discovered Address

You can modify the following properties for discovering an device:

- **User name and password** - You can change the user name and password the management server uses to access a device. Whenever a user name and/or password has changed on a device the management server monitors, the management server must be made aware of the


change. For example, assume the password for a host was changed. You would need to update the management server database with the new password.

- **Discovery group** - All elements are initially placed in the Default discovery group. You can then move elements from the Default discovery group to other discovery groups. You can use discovery groups to break up Discovery Data Collection. For example, you could specify that the management server gets Discovery Data Collection for only the elements in Discovery Group 1, thus, saving you time. This feature is sometimes referred to as segmented replication because you can specify getting Discovery Data Collection for a segment of the discovered elements.

Keep in mind the following:

- You can use this window to change the user name and password stored in the management server's database. It does not change the device's user name and password.
- Discovery groups cannot be renamed or created. You must use the existing discovery groups.
- You can also use the **Move to Discovery Group** button to move multiple elements to another discovery group. See ["Moving Elements to Another Discovery Group"](#) on page 47 for more information.

To change the discovery properties of an element:

1. Click **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. Click the  button corresponding with the element you want to modify.
3. To change the user name, type the new user name in the **User Name** field.
4. To move an element to another discovery group, select its new discovery group from the **Discovery Group** drop-down menu.
5. To change the password:
 - a. Click **Change Password**.
 - b. Type the new password in the **New Password** field.
 - c. Type the password again in the **Verify Password** field.
 - d. Click **OK** in the Change Password window.
6. Click **OK** in the Edit Discovered Element window.

Deleting Elements from the Management Server


When you delete an element, all of its information is removed from the management server. This includes asset information, zoning, events, statistics, and fabrics assigned to switches.

To completely delete an element from the management server you must remove the elements, such as a switch or proxy that were used to discover the element. If you do not delete all switches and proxies that were used to discover the element, the element may reappear the next time you Discovery Data Collection.

For example, assume you want to delete Switch_A. Switch_B and Switch_C were used to discover Switch_A. If you delete only Switch_B and Switch_A, Switch_A will most likely reappear when you Discovery Data Collection because it is still accessible by Switch_C.

Deleting an Element Using System Manager or Chargeback Manager

To delete an element using System Manager or Chargeback Manager:

1. Do one of the following:
 - **In System Manager** - Right-click an element and select **Delete Element** from the drop-down menu. Right-click an element and select **Delete Element** from the drop-down menu.
If you are blocking pop-ups and you use the right-click menu to delete an element from System Manager, the Delete window is blocked and you are unable to delete the element. You must disable the popup blocker before you can delete the element.
 - **In Chargeback Manager** - Click the  button for the element you want to delete.
2. If the element has multiple access points, you are asked which want to delete. Do one of the following:
 - **Delete the element and its access points.** This option lists not only the switch you want to delete, but also the other elements that use the same switches and proxies as the element you want to delete. For example, assume you want to delete Switch_A. Switch_B was used to discover Switch_A. Let's assume Switch_B is also the only path to Switch_D. If you delete Switch_B, you will no longer have access to Switch_D. This option would list Switch_D as one of the other elements that need to be deleted.
An access point is the intersection of the IP address and the provider that discovered the IP address. A provider is software that is used to gather information about an element.
 - **Delete the element.** The element may reappear the next time you obtain element details. This is because not all switches and proxies connected to the element have not been removed. For example, assume you want to delete Switch_A. Switch_B is connected to Switch_A. If you do not delete Switch_B, the next time you obtain element details Switch_B will most likely find Switch_A again.
3. Click **OK**.

Step 3 - Discovery Data Collection

This section describes the following:

- ["Discovery Data Collection" on page 41](#)
- ["Stopping the Gathering of Details" on page 42](#)
- ["Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh" on page 43](#)
- ["Excluding HDS Storage Systems from Force Device Manager Refresh" on page 44](#)

Discovery Data Collection

Discovery Data Collection is required to obtain detailed information from discovered elements. Discovery Data Collection must be performed before you can do provisioning and/or obtain provisioning information, such as data about zone sets and LUN numbers.

Keep in mind the following:

- Discovery Data Collection takes some time. You might want to perform this process when the network and the managed elements are not busy.
- If you have problems obtaining information from Connectrix and McDATA switches during Discovery Data Collection, see the topic, [“Step 2 - Discover Storage Systems, Filers and Tape Libraries”](#) on page 28.
- You can use discovery groups to break up getting Discovery Data Collection. For example, instead of Discovery Data Collection for all of the elements, you could specify that the management server Discovery Data Collection for only the elements in Discovery Group 1, thus, saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See [“Moving Elements to Another Discovery Group”](#) on page 47 for information on how to move one or more multiple elements to a discovery group. You can also move an element to another discovery group when you modify its discovery properties. See [“Modifying the Properties of a Discovered Address”](#) on page 39.
- When an element in a given discovery group is updated, its dependent elements are also updated. For example, assume Host_A is the only element in Discovery Group 1. Host_A is connected through a switch and storage system. When you Discovery Data Collection for Discovery Group 1, you also obtain details from the switch and storage system.
- You can quarantine elements to exclude them from Discovery Data Collection. See [“Placing an Element in Quarantine”](#) on page 48 for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.
- If you want to receive status reports about Discovery Data Collection, see [“Configuring E-mail Notification for Discovery Data Collection”](#) on page 167 for information about how to configure this option.
- If the management server unable to obtain information from a UNIX host during Discovery Data Collection as a result of a CIM Extension hanging, the management server places the access point where the CIM Extension is located in quarantine. The management server then moves onto getting details for the next element in the Discovery Data Collection table. These UNIX hosts appear as missing until they are removed from quarantine. See [“Removing an Element from Quarantine”](#) on page 48 for information on how to remove an element from quarantine.

To obtain details about the devices on the network:

1. Click **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. Select **Include infrastructure details**, which gathers information about SAN details.
3. The management server obtains most of the information from HDS and EMC Symmetrix storage systems from their device managers. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for HDS and EMC storage systems to obtain the latest information. See the following topics for more information: [“Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh”](#) on page 43 and [“Excluding HDS Storage Systems from Force Device Manager Refresh”](#) on page 44.

NOTE: If you plan to have File SRM scan a host, make sure you have 220 to 230 MB for each set of 1 million files.

4. Select the discovery group from which you want to obtain Discovery Data Collection. If you are obtaining Discovery Data Collection for the first time, make sure **All Discovery Groups** is selected.
5. Click the **Get Details** button.

While getting element details, the software changes its status light from green to red. You can view the progress of gathering details by clicking **Discovery > View Logs**.

When the software completes getting all elements details, it displays "GETTING ALL DETAILS COMPLETED" on the **View Logs** page.
6. See the User Guide for information about automating the gathering of all element details.
7. To add more IP addresses, IP Ranges or application information for discovery before completing the following step, click the **Discovery > Setup** link displayed below the logs screen.

Once you add more elements to be discovered, obtain Discovery Data Collection.

Stopping the Gathering of Details

Obtaining details takes some time. If the network and managed elements are busy, you might need to stop the gathering of details and reschedule it for another time.

IMPORTANT: If you stop the gathering of details, you should reschedule it. This type of collection obtains detailed information of devices in the network.

To stop the gathering of details:

1. Click **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. On the **View Logs** tab, click the "Click here" portion of the following message:
`Click here if you wish to stop getting details.`
3. When you are asked if you are sure you want to stop Discovery Data Collection, click **OK**.
The management server stops gathering details.
4. Schedule a time to resume getting details.

Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh

The management server obtains most of its information about Symmetrix storage systems from the EMC Solutions Enabler (proxy server) it discovered. If the EMC Solutions Enabler does not have the latest information, the management server also displays the outdated information.

To make the management server aware of any changes, make sure the Solutions Enabler it discovered has the latest information. This can be done by forcing the Solutions Enabler to refresh its data. The management server is then made aware of these changes.

When the **Force Device Manager Refresh** option is selected, the management server refreshes discovered EMC Solutions Enabler (proxy server), unless specified. If you do not want an EMC Solutions Enabler to be refreshed, you must assign the Symmetrix storage systems that use the Solutions Enabler to the `cimom.emc.skipRefresh` property, as described in the steps in this section.

To exclude EMC Symmetrix storage systems from a forced refresh:

1. Select **Options >Storage Essentials > Manage Product Health > Advanced**.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.

```
#cimom.emc.skipRefresh=000183500570,000183500575
```
4. Return to the Advanced page (**Options >Storage Essentials > Manage Product Health > Advanced**).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the Symmetrix storage systems you want the refresh to skip. Separate additional serial numbers with a comma, as shown by the following example:

```
cimom.emc.skipRefresh=000183500570,000183500575
```

where 000183500570 and 000183500575 are serial numbers for Symmetrix storage systems. One of the ways to find the serial number is to double-click the storage system in System Manager. Then, click the **Properties** tab.
7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect:
 - a. Go to the Services window on the management server.
 - b. Right-click **AppStorManager**.
 - c. Select **Restart** from the drop-down menu.While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.
9. To perform the forced refresh, select the **Force Device Manager Refresh** option on the Discovery Data Collection page (**Discovery > Details**).
10. Click **Get Details**.

Excluding HDS Storage Systems from Force Device Manager Refresh

The management server obtains most of its information about the HDS storage systems from the HiCommand Device Manager (proxy server) it discovered. If HiCommand Device Manager, does not have the latest information, the management server also displays the outdated information.

To make the management server aware of any changes, make sure the HiCommand Device Manager it discovered has the latest information. This can be done by forcing the HiCommand Device Manager to refresh its data. The management server is then made aware of these changes.

When the **Force Device Manager Refresh** option is selected, the management server refreshes discovered HiCommand Device Manager (proxy server), unless specified. If you do not want a HiCommand Device Manager to be refreshed, you must assign the HDS storage systems that use HiCommand Device Manager to the `cimom.HdsSkipRefresh` property, as described in the steps in this section.

IMPORTANT: Before performing any provisioning operations, you should perform a forced refresh.

To exclude HDS storage systems from a forced refresh:

1. Select **Options >Storage Essentials > Manage Product Health > Advanced**.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.

```
# cimom.HdsSkipRefresh=61038,61037
```
4. Return to the Advanced page (**Options >Storage Essentials > Manage Product Health > Advanced**).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. Add the serial numbers corresponding to the HDS storage systems you want the refresh to skip. Separate additional serial numbers with a comma, as shown by the following example:

```
cimom.HdsSkipRefresh=61038,61037
```

where 61038 and 61037 are serial numbers for HDS storage systems. One of the ways to find the serial number is to double-click the storage system in System Manager. Then, click the **Properties** tab.
7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect:
 - a. Go to the Services window on the management server.
 - b. Right-click **AppStorManager**.
 - c. Select **Restart** from the drop-down menu.While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.
9. To perform the forced refresh, select the **Force Device Manager Refresh** option on the Discovery Data Collection page (**Discovery > Details**).

10. Click **Get Details**.

Managing McDATA and EMC Connectrix Switches

This section describes the following:

- “[About Managing McDATA and EMC Connectrix Switches](#)” on page 45
- “[Adding McDATA and EMC Connectrix Switches](#)” on page 45

About Managing McDATA and EMC Connectrix Switches

Whenever you add, McDATA or EMC Connectrix switches in an already discovered service processor, you must make the management server aware of those changes. After you add these switches to the service processor, you must perform “Discovery Data Collection” in the management server. The management server obtains information about the new switches from the service processor. See the topic, “[Adding McDATA and EMC Connectrix Switches](#)” on page 45 for more information about adding switches.

Adding McDATA and EMC Connectrix Switches

After you add switches to an existing service processor, you must perform Discovery Data Collection, as described in the following steps. If you are adding switches to a service processor that has not been discovered yet, see the topic, “[Discovering McDATA and EMC Connectrix Switches](#)” on page 20.

IMPORTANT: Obtaining details takes some time. You might want to perform this process when the network and the managed elements are not busy.

To Discovery Data Collection:

1. Click **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. Click the **Get Details** button.

While getting element details, the software changes its status light from green to red.

Assigning a File Extension in Netscape 7

Netscape 7 automatically assigns unknown files an HTML extension. To make Netscape 7 recognize the type of file, you must assign a file extension.

To assign a MIME type:

1. Click the download file link or button in the software.
2. Click the **Advanced** button in the lower-left corner.
3. In the **Description of type** field, delete the existing text and type a description of the file.
4. In the **File extension** field, delete the existing text and type the file extension.
5. Click **OK**.

The next time Netscape 7 sees the associated MIME type, it will assign the extension you typed in the **File Extension** field.

For example, in the following figure, the zip extension was assigned to a MIME type of application/unknown. The next time Netscape sees that MIME type, it will automatically assign the zip extension to the file.

6. Click **OK**.

Updating the Database with Element Changes

After you have initially discovered the elements, information about them might change. To update database with these changes, perform the steps described in this section.

Keep in mind the following:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list. Then, you must stop and restart the CIM Extension running on that host.
- If you are adding McDATA or Connectrix switches, you must perform different steps. See the topic, ["Adding McDATA and EMC Connectrix Switches"](#) on page 45.

To update the database:

1. Click **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. Make sure the File Server SRM option is selected.
3. Select **Include infrastructure details**, which gathers information about SAN details.
4. The management server obtains most of the information from HDS and EMC Symmetrix storage systems from their device managers. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for HDS and EMC storage systems to obtain the latest information. See the following topics for more information: ["Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh"](#) on page 43 and ["Excluding EMC Symmetrix Storage Systems from Force Device Manager Refresh"](#) on page 43.
5. Click the **Get Details** button on the Discovery Data Collection page.
6. View the status of the gathering of element details by looking in the **View Logs** tab. See the topic, ["Viewing Log Messages"](#) on page 27 for more information about the messages viewed in this tab.
7. Verify the topology is displayed correctly by accessing System Manager. To access System Manager, click the **System Manager** button in the left pane.

Filtering Discovery Groups

You can determine which discovery groups are displayed on the Discovery Data Collection (**Options > Storage Essentials > Discovery > Run Discovery Data Collection**) page by modify the discovery filter, as described in the following steps:

1. Access the Discovery Data Collection page (**Options > Storage Essentials > Discovery > Run Discovery Data Collection**).
2. Click the **Custom** button.
3. Select the discovery groups you want to include in Discovery Data Collection. Deselect the discovery groups you do not want to be included in Discovery Data Collection.
4. Click **OK**.

Elements in the selected discovery groups are selected on the Discovery Data Collection page. The management server obtains information from the selected elements during Discovery Data Collection. To learn how to add an element to a different discovery group, see [“Modifying the Properties of a Discovered Address”](#) on page 39.

Moving Elements to Another Discovery Group

All elements are initially placed in the Default discovery group. You can then move elements from the Default discovery group to other discovery groups. You can use discovery groups to break up getting Discovery Data Collection. For example, you could specify that the management server gets Discovery Data Collection for only the elements in Discovery Group 1, thus, saving you time. This feature is sometimes referred to as segmented replication because you can specify getting Discovery Data Collection for a segment of the discovered elements.

Keep in mind the following:

- Discovery groups cannot be renamed or created. You must use the existing discovery groups.
- You can also use move an element to another discovery group when you modify its discovery properties. See [“Modifying the Properties of a Discovered Address”](#) on page 39 for more information.

To move an element to another discovery group:

1. Select the check boxes for the elements you want to move in the Discovery Data Collection page.
2. Click the **Move to Discovery Group** button.
3. In the Select Discovery Group window, select the new discovery group for the selected elements.
4. Click **OK**.

The elements are moved to the new discovery group.

Placing an Element in Quarantine


When you click the **Get Details** button on the Discovery Data Collection page, the management server automatically obtains details for the elements in the selected discovery group. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.

NOTE: After you perform Discovery Data Collection for the discovery group containing the quarantined elements, the quarantined elements appear as missing throughout the product. The management server marks the quarantined elements as missing because it cannot obtain details from the quarantined element.

To quarantine an element:

1. Select the check boxes for the elements you want to quarantine on the Discovery Data Collection page.

2. Click the **Set Quarantine** button.
3. When you are asked if you want to quarantine the selected elements, click **OK**.


The elements you quarantine appear with a flag () in the Quarantined column on the Discovery Data Collection page.

The elements are excluded from discovery until you clear them from quarantine.

Removing an Element from Quarantine

To remove an element from quarantine:

1. Select the check boxes for the elements you want to remove from quarantine on the Discovery Data Collection page.

Quarantined elements appear with a flag () in the Quarantined column on the Discovery Data Collection page.

2. Click the **Clear Quarantine** button.
3. When you are asked if you want to remove the selected elements from quarantine, click **OK**.
The next time you perform Discovery Data Collection for the element, the management server gathers data from the element.

5 Installing the CIM Extension for IBM AIX

This chapter describes the following:

- “About the CIM Extension for IBM AIX” on page 51
- “Prerequisites” on page 51
- “Verifying SNIA HBA API Support” on page 52
- “Installing the CIM Extension” on page 53
- “Setting Up Monitoring” on page 54
- “Starting the CIM Extension Manually” on page 54
- “Modifying the Boot Time RC Start Script (Optional)” on page 57
- “Stopping the CIM Extension” on page 57
- “How to Determine if the CIM Extension Is Running” on page 57
- “Fulfilling the Prerequisites” on page 57
- “Rolling Over the Logs” on page 58
- “Removing the CIM Extension from AIX” on page 59

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

About the CIM Extension for IBM AIX

The CIM Extension for IBM AIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

The installation creates the following directories in the `/opt/APPQcime` directory:

- **jre** - The Java run time necessary to run the CIM Extension
- **lib** - The executables for the CIM Extension
- **tools** - The files to stop, start and show the status of the CIM Extension

Prerequisites

The installation checks for the following. If the installation fails, see “[Fulfilling the Prerequisites](#)” on page 57.

AIX 5.1

- Maintenance level 03 or later
- bos.rte.libc.5.1.0.36 or later

Both AIX 5.1 and 5.2

xlC.rte.5.0.2.1 or later

AIX 5.3

- bos.rte.libc 5.3.0.0
- xlC.rte 6.0.0.0

Required Disk Space

The CIM Extension for AIX requires 40 MB.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your AIX host for more information. If you need to use a different port, see [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159.

bos.perf.libperfstat Required for Performance Data

The file bos.perf.libperfstat is required for the management server to obtain performance data. Without bos.perf.libperfstat, the following occurs:

- 32-bit kernel - You do not receive information about the amount of virtual memory used.
- 64-bit kernel
 - You are shown zero on the navigation page for “Total Physical Memory.”
 - You are shown the following error message in the log:

```
bos.perf.libperfstat not installed - required for 64-bit Kernel to get disk or cpu statistics.
```

- You do not obtain information for the following in Performance Manager:
 - statistics on the operating system
 - disk (disk utilization, disk read, disk write)
 - CPU (processor utilization)

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API. In some instances hbatest may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run hbatest:

1. Go to the `AIX/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`

The program runs its diagnostics.

IBM Adapters FCXXX SNIA comes from the package `devices.common.IBM.fc.hba-api`. To find its library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

```
com.ibm.df1000f7 /usr/lib/libHBAAPI.a  
com.ibm.df1000f9 /usr/lib/libHBAAPI.a
```

Installing the CIM Extension

IMPORTANT: The following steps assume you know how to use `smit`. If you are unfamiliar with `smit`, refer to the documentation that accompanies the AIX host.

To install the CIM Extension for AIX:

1. Insert the CIM Extensions CD-ROM into the CD-ROM drive.
2. Mount the CD-ROM drive by entering the following at the command prompt:

```
# mount -rv cdrfs /dev/cd0 /cdrom
```

where `/dev/cd0` is the name of the CD-ROM drive.
If necessary, create a `/cdrom` directory first.
3. Enter the following at the command prompt:

```
# smit -C
```
4. Select **Software Installation and Maintenance**.
5. Select **Install and Update Software**.
6. Select **Install Software**.
7. For INPUT device/directory for software, enter the following:

```
cdrom/Aix
```

where `/cdrom` is the directory where you mounted the CD-ROM.
8. To install the software, activate the list command (F4) and select the following:

```
APPQcime CIM Extensions
```
9. Press **ENTER** to install.
10. If you see error messages when you install the CIM Extension for AIX, see ["Fulfilling the Prerequisites"](#) on page 57.
11. Unmount the CD-ROM by entering the following at the command prompt:

```
# umount /cdrom
```

where `/cdrom` is the name of the directory where you mounted the CD-ROM.
12. Complete the following:
 - Turn on Monitoring. See ["Setting Up Monitoring"](#) on page 54.
 - Start the CIM Extension. See ["Starting the CIM Extension Manually"](#) on page 54.

- (Optional) On some versions of AIX, the CIM Extension cannot start automatically after the host is rebooted. To see if your version of AIX supports the automatic startup, see ["Fulfilling the Prerequisites"](#) on page 57.

Setting Up Monitoring

If you want the management server to be able to monitor the AIX host, `iostat` must be set to true. When `iostat` is set to true, disk activity history is retained for all disks. The retention of disk activity is required for the management server to accurately monitor the AIX host.

To verify if disk activity history is being retained:

1. Enter the `iostat` command in the command prompt:

```
# iostat
```

2. If you see the message "Disk history since boot not available", enter the following at the command prompt to enable the retention of disk activity history:

```
# chdev -l sys0 -a iostat=true
```

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running. To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory:

```
# ./start
```

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls"](#) on page 160.
- If you see a "Fork Function Failed" message when you start the CIM Extension, the AIX host is running low on physical or virtual memory. See ["Fork Function Failed" Message on AIX Hosts](#) on page 177.

The following is displayed:

```
Starting CIM Extension for AIX
.....
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Sep 22 10:23:15 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
```

where

- `xxxx` is the year.
- `x.x.x.x` is the version of CIM Extension

- 192.168.1.5 is the IP address of the host

NOTE: Depending on your terminal type and processor speed, the message, “CXWS x.x.x.x on /192.168.1.5 now accepting connections,” may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, use the `./start -port port_number` command to change the port the CIM Extension will access. For example, if you are running a J2EE server, such as BEA WebLogic or IBM WebSphere, the J2EE server might already be using port 4673.

IMPORTANT: The steps provided in the section provide information about temporarily changing the port of the CIM Extension. If you want to permanently change the port the CIM Extension uses, see “[Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#)” on page 159.

To change the port, enter the following:

```
./start -port 1234
```

where 1234 is the port the CIM Extension will listen on for all available network cards

You can tell the port is in use by entering the following at the command prompt:

```
netstat -a | grep 1234
```

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM Extension to listen on only on a specific network interface card (NIC) by using the “-on” command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM Extension listens only on the NIC that has the IP address 192.168.99.37.

The “-on” command line option may be repeated as often as desired to direct the CIM Extension to listen on multiple NICs, for example:

```
./start -on 192.168.2.2 -on 192.168.1.1
```

The CIM Extension listens only on the NICs that have the IP address 192.168.2.2 or 192.168.1.1.

The “-on” command line option may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
./start -on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The “-port” command line option may be used in conjunction with the “-on” option. Any “-on” arguments that do not specify an explicit port number use the “-port” option argument as the port number, for example:

```
./start -on 192.168.1.1:3456 -on 192.168.2.2 -port 1170
```

This command tells the CIM Extension to listen on the following ports:

- Port 3456 on the NIC with the IP address 192.168.1.1
- Port 1170 on the NIC with the IP address 192.168.2.2

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the NIC
- 1234 is the new port number

If you have already added the NIC to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the NIC with different ports.

Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:

```
# ./start -version
```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
CXWS for mof/cxws/cxws-aix.mof  
CXWS version xxxx, built on Fri xx-March-xxxx 12:29:49 by dmaltz
```


Modifying the Boot Time RC Start Script (Optional)

When you install the CIM Extension, its start script is put in the `/etc/rc.d/rc2.d` directory with the file name `S99appqcime`. The CIM Extension uses this script to start at boot time. You can modify this script if you want to add parameters. Any parameter you can add when you manually start the CIM Extension, such as `-port`, can be added to the start script.

To modify the file:

1. Open `S99appqcime` in a text editor.
2. Find the following line of code:
`${APPIQ_HOME}/tools/start`
3. Add the parameter after `/start`. For example, assume you want to change the port for the CIM Extension to port 1234. You would add `-port 1234` after `/start`, as shown in the following example:

```
${APPIQ_HOME}/tools/start -port 1234
```

4. Save the file.

The changes take effect the next time the script executed when the host reboots.

Stopping the CIM Extension

To stop the background process for the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The process for the CIM Extension is displayed.

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

Fulfilling the Prerequisites

If your installation failed, you may be missing the following prerequisites. Refer to the information below on the required maintenance level and file sets.

IMPORTANT: Installation of the `devices.common.IBM.fc.hba-api.5.1.0.0` file set is optional. If you do not install this file set, you will be able to discover the AIX host, but you will not see any information about your host bus adapters or any information they provide. For example, the Navigation page for the host will not show results for host bus adapters, HBA ports, or bindings. Also if you do not install the `devices.common.IBM.fc.hba-api.5.1.0.0` file set, the host is displayed in the topology, but devices attached to the host are not displayed, such as switches. This information also applies to the `devices.common.IBM.fc.hba-api.5.3.0.0` file set for AIX 5.3.

AIX 5.1

- **Maintenance level 03 or later** - This is required for the HBAAPI. The operating system level can be found by entering the following command at the command prompt:

```
oslevel -r
```
- **bos.rte.libc.5.1.0.36 or later** - This is required for Java 1.4 support. The file can be downloaded from the IBM Technical Support Web site at the following URL:
<https://techsupport.services.ibm.com>

Both AIX 5.1 and 5.2

xlC.rte.5.0.2.1 or later - The C++ runtime. To obtain the C++ runtime, go to the IBM Technical Support Web site at the following URL:
<https://techsupport.services.ibm.com>

AIX 5.3

- **bos.rte.libc.5.3.0.0*** - This is required for Java 1.4 support.
- **xlC.rte.6.0.0.0*** - The C++ runtime.

*Go to the IBM Technical Support Web site at the following URL to obtain information about obtaining these file:

<https://techsupport.services.ibm.com>

On the Web page do the following:

1. Under the **Refine Your Search Section** select **Tools/Utilities** from the **Limit by Type** drop-down menu.
2. Select **AIX** from the **Limit by Platform or Operating System** drop-down menu.
3. Select **5.0** from the **Limit by Version** drop-down menu.
4. In the **Limit by Adding Search** terms field, type the following:

```
Download the VisualAge C++ for AIX V5 Runtime libraries
```
5. Install the `xlC.rte` file set, not the `.rte` file for AIX 4.x.

Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the `cxws.log` file. The `cxws.log` files roll over once the files become more than 30 MB. The information in `cxws.log` is

moved to `cxws.log.1`. If `cxws.log.1`, already exists, `cxws.log.2` is created. The numbering for the files continues sequentially, for example, `cxws.log.3`, `cxws.log.4`, etc.

The `cxws.out` file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The `cxws.out` file is rewritten each time the CIM Extension restarts.

Removing the CIM Extension from AIX

Make sure “preview” is set to “No”. Refer to your documentation for AIX for more information.

To remove the CIM Extension for AIX:

1. Stop the CIM Extension as mentioned in “[Stopping the CIM Extension](#)” on page 57.
2. Type the following at the command prompt:

```
# smit -C
```
3. Select **Software Installation and Maintenance**.
4. Select **Software Maintenance and Utilities**.
5. Select **Remove Installed Software**.
6. In the SOFTWARE name, press F4 and select:

```
APPQcime CIM Extensions
```
7. On the same page you selected `APPQcime CIM Extensions`, select “No” for Preview by pressing the tab key.
8. Press ENTER to remove the software.

6 Installing the CIM Extension for SGI ProPack for Linux

This chapter describes the following:

- “About the CIM Extension for SGI ProPack for Linux” on page 61
- “Prerequisites” on page 61
- “Verifying SNIA HBA API Support” on page 62
- “Installing the CIM Extension” on page 62
- “Starting the CIM Extension” on page 63
- “Stopping the CIM Extension” on page 66
- “How to Determine if the CIM Extension Is Running” on page 66
- “Removing the CIM Extension from SGI ProPack for Linux” on page 66

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

About the CIM Extension for SGI ProPack for Linux

The CIM Extension for SGI ProPack for Linux gathers information from the operating system and host bus adapters on an Altix host. It then makes the information available to the management server.

IMPORTANT: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

SGI ProPack 3.0 for Linux

The system must also be PCP (Performance Co-Pilot) enabled to be able to collect information about it.

The CIM Extension requires at least one of the following configurations for authentication:

- Shadow passwords encrypted using the Data Encryption Standard (DES). This configuration is the default for Altix systems.
- Shadow passwords using MD5. The CIM Extension does not support pure MD5 passwords, which are missing the `/etc/shadow` file.
- `/etc/passwd`

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Altix host for more information. If you need to use a different port, see “[Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#)” on page 159.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the `hbatest` program, which is accessible from the CIM Extension CD-ROM. The program, `hbatest`, lists the name and number for all HBA's that support the SNIA HBA API. In some instances `hbatest` may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

1. Go to the `Irix/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`

The program runs its diagnostics.

The SGI-branded QLogic Adapter SNIA is built into the operating system kernel. To find its location, enter the following at the command prompt:

```
# ls
```

The following is displayed:

```
/usr/include/hba_api.h
```

Installing the CIM Extension

IMPORTANT: You must have root privileges to install this software.

You are provided several installation options. One is an interactive option, which lets you select the installation directory. Another is a silent installation, which installs with no user input. The silent installation assumes the default installation directory. Both options install on computers with or without X Windows.

To install a CIM Extension on SGI ProPack for Linux:

1. Go to the `/Altix` directory on the CIM Extensions CD-ROM by entering the following at the command prompt:

```
# cd /cdrom/Altix
```

where `/cdrom` is the directory where you mounted the CD-ROM.
2. To install the software, do one of the following:

IMPORTANT: If you receive a message saying there is not enough room in the temp directory to perform the installation, set the IATEMPDIR variable to another directory. The installation uses this directory to extract the installation files. Refer to the documentation for your operating system for information on how to set this variable.

- **Interactive Installation (Without X Windows or telnet terminal session)** - You must type `-i` console; otherwise, you are shown a `NoClassDefFoundError` message. Enter the following at the command prompt:

```
# ./InstallCIMExtensions.bin -i console
```

- **Interactive Installation (With X Windows)** - Enter the following at the command prompt:

```
# ./InstallCIMExtensions.bin
```

- **Silent Installation (X Windows not required)** - Enter the following at the command prompt. Then, go to Step 4. You cannot change the installation directory.

```
# ./InstallCIMExtensions.bin -i silent
```

The CIM Extension is automatically installed in the `/opt/APPQcime` directory.

3. During the installation you are asked for the installation directory. Choose the default installation directory for best results.

4. Go to a directory other than one on the CD-ROM.

5. Unmount the CD-ROM by entering the following at the command prompt:

```
# umount /cdrom
```

where `/cdrom` is the name of the directory where you mounted the CD-ROM

6. Use `chkconfig --list appqcime` to verify the installation.

7. Start the CIM Extension. See ["Starting the CIM Extension"](#) on page 63.

You must restart the CIM Extension after you have rebooted the server. This is because there is no support for `/etc/rc` scripts, which the CIM Extension uses to start.

Starting the CIM Extension

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see ["Configuring UNIX CIM Extensions to Run Behind Firewalls"](#) on page 160.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory:

1. Before starting the CIM Extension, make sure PCP is enabled by executing the following command:

```
ps -ef | grep pmcd
```

This should display a message resembling the following:

```
root      2699      1  0 14:42 ?                00:00:00 /usr/share/pcp/bin/pmcd
root      2831    1988  0 14:44 pts/1          00:00:00 grep pmcd
```

The first line above indicates that pmcd is running. If not, execute the following commands:

```
chkconfig pcp on
service pcp start
```

These commands start the pmcd daemon and also ensure the pmcd daemon starts whenever the system reboots.

2. To start the CIM Extension, type the following at the command prompt:

```
# ./start
```

The following is displayed:

```
Starting CIM Extension for ALTIX
```

```
.....
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Jan 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
```

where

- xxxx is the year.
- x.x.x.x is the version of CIM Extension
- 192.168.1.5 is the IP address of the host

Keep in mind the following:

- Depending on your terminal type and processor speed, the message, "CXWS x.x.x.x on /192.168.1.5 now accepting connections," may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.
- When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information. You can also access information about these topics by typing the following:

```
./start -help
```

Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, use the `./start -port port_number` command to change the port the CIM Extension will access. For example, if you are running a J2EE server, such as BEA WebLogic or IBM WebSphere, the J2EE server might already be using the 4673 port.

IMPORTANT: The steps provided in the section provide information about temporarily changing the port of the CIM Extension. If you want to permanently change the port the CIM Extension uses, see [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159.

To change the port, enter the following:

```
./start -port 1234
```

where 1234 is the port the CIM Extension will listen on for all available network cards

You can tell the port is in use by entering the following at the command prompt:

```
netstat -a | grep 1234
```

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM Extension to listen on only on a specific network interface card (NIC) by using the “-on” command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM Extension listens only on the NIC that has the IP address 192.168.99.37.

The “-on” command line option may be repeated as often as desired to direct the CIM Extension to listen on multiple NICs, for example:

```
./start -on 192.168.2.2 -on 192.168.1.1
```

The CIM Extension listens only on the NICs that have the IP address 192.168.2.2 or 192.168.1.1.

The “-on” command line option may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
./start -on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The “-port” command line option may be used in conjunction with the “-on” option. Any “-on” arguments that do not specify an explicit port number use the “-port” option argument as the port number, for example:

```
./start -on 192.168.1.1:3456 -on 192.168.2.2 -port 1170
```

This command tells the CIM Extension to listen on the following ports:

- Port 3456 on the NIC with the IP address 192.168.1.1
- Port 1170 on the NIC with the IP address 192.168.2.2

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the NIC
- 1234 is the new port number

If you have already added the NIC to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the NIC with different ports.

Stopping the CIM Extension

To stop the background process for the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
# ./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
# ./status
```

The process for the CIM Extension is displayed.

The CIM Extension is running when a message resembling the following is displayed:

```
CIM Extension Running
```

Removing the CIM Extension from SGI ProPack for Linux

To remove the CIM Extension for SGI ProPack for Linux:

1. Go to the following directory by entering the following at the command prompt:

```
# cd [InstallationDirectory]/Uninstall_CIMExtensions
```

where `InstallationDirectory` is the directory containing the CIM Extension

2. Remove the CIM Extension by entering the following at the command prompt:

```
# ./Uninstall_SGI_CIMExtensions
```

7 Installing the CIM Extension for HP-UX

This chapter describes the following:

- "About the CIM Extension for HP-UX" on page 69
- "Prerequisites" on page 69
- "Verifying SNIA HBA API Support" on page 70
- "Installing the CIM Extension" on page 71
- "Starting the CIM Extension Manually" on page 72
- "Finding the Status of the CIM Extension" on page 75
- "Modifying the Boot Time RC Start Script (Optional)" on page 76
- "Stopping the CIM Extension" on page 76
- "Rolling Over the Logs" on page 76
- "Fulfilling the Prerequisites" on page 76
- "Removing the CIM Extension from HP-UX" on page 77

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

About the CIM Extension for HP-UX

The CIM Extension for HP-UX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

IMPORTANT: Install the CIM Extension on each host you want the management server to manage.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The installation checks for the following. If the installation fails, see "[Fulfilling the Prerequisites](#)" on page 76.

HP-UX 11i and 11.0

Software Requirements

Following software driver bundles must be installed on HP-UX 11i and 11.0 hosts. FC SNIA HBA API software is bundled with the driver and is installed at the same time the driver is installed.

HP-UX 11i

Driver Bundle Version

B.11.11.09 PCI/HSC FibreChannel;Supptd HW=A6684A,A6685A,A5158A,A6795A (FibrChanl-00 Bundle).

This driver Bundle is automatically selected for installation with the HP-UX 11i Operating Environments.

Driver Version = @(#) PATCH_11.11: libtd.a : Jun 28 2002, 11:08:35, PHSS_26799 or later

Driver Patch

Tachyon Fibre Channel Driver Patch: PHKL_23626 or later (only for HP-UX 11i)

HP-UX 11.0

Driver Bundle Versions

B.11.00.10 PCI Tachyon TL/TS Fibre Channel (Bundle A5158A).

B.11.00.10 PCI Tachyon TL/TS/XL2 Fibre Channel (Bundle A6795A)

Driver Version = @(#) PATCH_11.00: libtd.a : Jul 15 2002, 11:34:12, PHSS_26798

Driver Patch

Tachyon Fibre Channel Driver Patch: PHKL_23939 or later (only for HP-UX 11.00)

Required Disk Space

The CIM Extension for HP-UX requires 105 MB.

Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your HP-UX host for more information. If you need to use a different port, see "[Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#)" on page 159.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the `hbatest` program, which is accessible from the CIM Extension CD-ROM. The program, `hbatest`, lists the name and number for all HBA's *that support the SNIA HBA API*. In some instances `hbatest` may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run `hbatest`:

1. Go to the `HPUX/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`

The program runs its diagnostics.

HP SNIA Adapters AXXXXA comes from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during installing the operating system, filesets are there by default. To view the location of the library, enter the following at the command prompt:

```
# more /etc/hba.conf
```

The following is displayed:

- ```
com.hp.fcms32 /usr/lib/libhbaapihp.sl #32 bit lib names end in '32'
com.hp.fcms64 /usr/lib/pa20_64/libhbaapihp.sl #64 bit lib names end in '64'
```
- com.hp.fcd32 /usr/lib/libhbaapifcd.sl
  - com.hp.fcd64 /usr/lib/pa20\_64/libhbaapifcd.sl

## Installing the CIM Extension

Keep in mind the following:

- The instructions in this section apply if you are doing a local installation of the CIM Extension, as compared to a scripted or push installation. If you want to perform a scripted or push installation of the CIM Extension, first install the CIM Extension locally by using the instructions in this section. Then, perform the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.
- You must install the CIM Extension for HP-UX to the default directory.

To install the CIM Extension using CLI:

1. Login as root.
2. Place CIM Extension CD-ROM into the CD-ROM on HP-UX server.
3. Create the /cdrom directory on HP-UX host by entering the following at the command prompt:  

```
mkdir /cdrom
```
4. Mount the CIM Extension CD-ROM by enter the following at the command prompt:  

```
mount /dev/dsk/c#t#d# /cdrom
```

where c, t and d numbers correspond to CD-ROM device numbers  
To find out c#t#d# of your CD-ROM, run "ioscan -fnC disk" command on the HP-UX host.
5. To install the CIM Extension, enter the following at the command prompt:  

```
swinstall -s /cdrom/HPUX/APPQcime.depot APPQcime
```

The installation is complete when you are told the "analysis and execution succeeded."
6. Eject/unload the CD-ROM by unmounting the CD-ROM and pressing eject/unload button on the CD-ROM drive:  

```
umount /cdrom
```

where /cdrom is the name of the directory where you mounted the CD-ROM
7. Press the Eject button on the CD-ROM drive to take the CD out of the CD-ROM drive.

The CIM Extension for HP-UX starts automatically at boot time by using `/sbin/rc2.d` scripts. The CIM Extension uses port 4673 when it starts automatically after a reboot. Type the following at the command prompt to find the status of the CIM Extension: `./status`

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: Data is late or an error occurred.
- To configure UNIX CIM Extensions to run behind a firewall, see [“Configuring UNIX CIM Extensions to Run Behind Firewalls”](#) on page 160.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./start
```

The following is displayed:

```
Starting CIM Extension for HP-UX
.....
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
```

where

- `xxxx` is the year.
- `x.x.x.x` is the version of CIM Extension
- `192.168.1.5` is the IP address of the host

Keep in mind the following:

- Depending on your terminal type and processor speed, the message, “CXWS x.x.x.x on /192.168.1.5 now accepting connections,” may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.
- When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information. You can also access information about these topics by typing the following:

```
./start -help
```



## Restricting the Users Who Can Discover the Host

The `./start -users user_name` command provides greater security by restricting access. When you use the management server to discover the host (**Discovery > Setup**), provide a user name that was specified in the `-users` parameter in the start command. The following is an example of the command:

```
./start -users myname
```

where `myname` is a valid HP-UX user name that must be used to discover this HP-UX host.

For example, assume you want to use the management server to discover a HP-UX host, but you do not want to provide the password to the root account. You can provide the password to another valid HP-UX user account that has less privileges, for example `jsmythe`. You would log into the HP-UX host as root and start the CIM extension by using the following command:

```
./start -users jsmythe
```

where `jsmythe` is a valid HP-UX user name.

You would then logon to the management server, access the Discovery page (**Discovery > Setup**), and click the **Add Address** button. In the **Add Address for Discovery** page, provide the user name and password for `jsmythe`. Only the user name and password for `jsmythe` can be used to discover the HP-UX host. This is because you used `jsmythe` in the `./start -users` command.

Another variation of the start command lets you provide multiple users in a colon-separated list, for example:

```
./start -users myname:jsmythe
```

One of the names listed (`myname` or `jsmythe`) must be used to discover the HP-UX host

(**Discovery > Setup** on the management server). Other user names and passwords, including root will not work.

## Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, use the `./start -port port_number` command to change the port the CIM Extension will access. For example, if you are running a J2EE server, such as BEA WebLogic or IBM WebSphere, the J2EE server might already be using the 4673 port.

---

**IMPORTANT:** The steps provided in the section provide information about temporarily changing the port of the CIM Extension. If you want to permanently change the port the CIM Extension uses, see ["Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)"](#) on page 159.

---

To change the port, enter the following:

```
./start -port 1234
```

where 1234 is the port the CIM Extension will listen on for all available network cards

You can tell the port is in use by entering the following at the command prompt:

```
netstat -a | grep 1234
```

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

---

**IMPORTANT:** If you specify a port in the `./start` command, the host can be discovered by any account that has access to the HP-UX server.

---

## Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM Extension to listen on only on a specific network interface card (NIC) by using the “-on” command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM Extension listens only on the NIC that has the IP address 192.168.99.37.

The “-on” command line option may be repeated as often as desired to direct the CIM Extension to listen on multiple NICs, for example:

```
./start -on 192.168.2.2 -on 192.168.1.1
```

The CIM Extension listens only on the NICs that have the IP address 192.168.2.2 or 192.168.1.1.

The “-on” command line option may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
./start -on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The “-port” command line option may be used in conjunction with the “-on” option. Any “-on” arguments that do not specify an explicit port number use the “-port” option argument as the port number, for example:

```
./start -on 192.168.1.1:3456 -on 192.168.2.2 -port 1170
```

This command tells the CIM Extension to listen on the following ports:

- Port 3456 on the NIC with the IP address 192.168.1.1

- Port 1170 on the NIC with the IP address 192.168.2.2

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the NIC
- 1234 is the new port number

If you have already added the NIC to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the NIC with different ports.

## Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:

```
./start -version
```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
Starting CIM Extension for HP-UX
CXWS for mof/cxws/cxws-HPUX.mof
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

where

- xxxx is the year.
- x.x.x.x is the version of the CIM Extension

## Combining Start Commands

You can also combine the `-users` and `-port` commands as follows:

```
./start -users myname -port 1234
```

or

```
./start -port 1234 -users myname
```

where

- myname is the user name that must be used to discover this HP-UX host
- 1234 is the new port

## Finding the Status of the CIM Extension

You can always check the status of the CIM Extension by entering the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

## Modifying the Boot Time RC Start Script (Optional)

When you install the CIM Extension, its start script is put in the `/sbin/rc2.d` directory with the file name `S99appqcime`. The CIM Extension uses this script to start at boot time. You can modify this script if you want to add parameters. Any parameter you can add when you manually start the CIM Extension, such as `-port`, can be added to the start script.

To modify the file:

1. Open `S99appqcime` in a text editor.
2. Find the following line of code:  

```
`${APPIQ_HOME}/tools/start
```
3. Add the parameter after `/start`. For example, assume you want to change the port for the CIM Extension to port 1234. You would add `-port 1234` after `/start`, as shown in the following example:

```
`${APPIQ_HOME}/tools/start -port 1234
```

4. Save the file.

The changes take effect the next time the script executed when the host reboots.

## Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

## Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the `cxws.log` file. The `cxws.log` files roll over once the files become more than 30 MB. The information in `cxws.log` is moved to `cxws.log.1`. If `cxws.log.1`, already exists, `cxws.log.2` is created. The numbering for the files continues sequentially, for example, `cxws.log.3`, `cxws.log.4`, etc.

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The cxws.out file is rewritten each time the CIM Extension restarts.

## Fulfilling the Prerequisites

Use the commands mentioned in this section to determine if you have the required software.

To verify driver bundle version, enter the following at the command prompt:

```
swlist
```

To verify installed patches, enter the following at the command prompt:

```
show_patches
```

To find the HBA driver version, after HBA software bundles are installed and patches applied to the operating system, enter the following at the command prompt:

```
fcmsutil /dev/td0
```

If host has more than one HBA, enter the following at the command prompt:

```
fcmsutil /dev/td1
```

Number in `td#` corresponds to the HBA number.

## Removing the CIM Extension from HP-UX

To remove the CIM Extension for HP-UX as root:

1. Login as root.
2. Stop the CIM Extension, as described in "[Stopping the CIM Extension](#)" on page 76.
3. Make sure you are not in the APPQcime directory. As a precaution, go to the root directory.
4. Enter the following at the command prompt:

```
swremove APPQcime
```

When you see the following message, the CIM Extension has been removed:

```
* Beginning Execution
* The execution phase succeeded for hpuxqaX.dnsxxx.com:/.
* Execution succeeded..
```

5. To remove the APPQcime directory, enter the following at the command prompt:

```
rm -r APPQcime
```



---

## 8 Installing the CIM Extension for SGI IRIX

This chapter describes the following:

- “About the CIM Extension for SGI IRIX” on page 79
- “Prerequisites” on page 79
- “Verifying SNIA HBA API Support” on page 80
- “Installing the CIM Extension” on page 80
- “Starting the CIM Extension” on page 81
- “Modifying the Boot Time RC Start Script (Optional)” on page 84
- “Stopping the CIM Extension” on page 84
- “Rolling Over the Logs” on page 84
- “How to Determine if the CIM Extension Is Running” on page 85
- “Removing the CIM Extension from SGI IRIX” on page 85

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

### About the CIM Extension for SGI IRIX

The CIM Extension for SGI IRIX gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

---

**IMPORTANT:** Install the CIM Extension on each host you want the management server to manage.

---

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web Site: [http://www.snia.org/tech\\_activities/hba\\_api/](http://www.snia.org/tech_activities/hba_api/)

### Prerequisites

The installation requires the SGI Origin system and 120 MB of disk space. It also requires one of the following operating systems:

- IRIX version 6.5.22, limited to internal processors 27 and 35
- IRIX version 6.5.20, patch required. Contact customer support for the patch.

#### Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your IRIX host for more information. If you need to use a different port, see “[Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#)” on page 159.

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the `hbatest` program, which is accessible from the CIM Extension CD-ROM. The program, `hbatest`, lists the name and number for all HBA's that support the SNIA HBA API. In some instances `hbatest` may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

1. Go to the `Irix/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`  
The program runs its diagnostics.

SGI Branded QLogic SNIA Adapters are built into the operating system kernel starting with IRIX 6.5.22 and later. To find the library, enter the following at the command prompt:

```
ls
```

The following is displayed:

```
/usr/include/sys/hba_api.h
```

## Installing the CIM Extension

To install the CIM Extension for IRIX:

1. Insert the CIM Extensions CD-ROM into the CD-ROM drive.
2. Go to the CD-ROM by entering the following at the command prompt:  
`cd /CDROM`
3. Enter the following at the command prompt:  
`inst`
4. Enter the following at the `Inst` command prompt:  
`Inst> open`
5. When you are asked for the location of the installation, enter the following:  
`Inst> /CDROM/Irix`
6. Enter the following:  
`Inst> install`
7. When asked which subsystem, enter the following:  
`APPQcime`
8. To begin the installation, enter the following:  
`Inst> go`  
The IRIX CIM Extension is installed in the `/opt/APPQcime` directory.
9. Enter the following to restart the ELF files and to exit the installation program:  
`Inst> quit`  
You must start the CIM Extension for the management server to obtain information about the host. See "[Starting the CIM Extension](#)" on page 81



# Starting the CIM Extension

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late` or `an error occurred`.
- To configure UNIX CIM Extensions to run behind a firewall, see [“Configuring UNIX CIM Extensions to Run Behind Firewalls”](#) on page 160.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory:

```
./start
```

The following is displayed:

```
Starting CIM Extension for IRIX
.....
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
```

where

- `xxxx` is the year.
- `x.x.x.x` is the version of CIM Extension
- `192.168.1.5` is the IP address of the host

---

**NOTE:** Depending on your terminal type and processor speed, the message, `“CXWS x.x.x.x on /192.168.1.5 now accepting connections,”` may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.

---

## Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, use the `./start -port port_number` command to change the port the CIM Extension will access. For example, if you are running a J2EE server, such as BEA WebLogic or IBM WebSphere, the J2EE server might already be using the 4673 port.

---

**IMPORTANT:** The steps provided in the section provide information about temporarily changing the port of the CIM Extension. If you want to permanently change the port the CIM Extension uses, see [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159.

---

To change the port, enter the following:

```
./start -port 1234
```

where 1234 is the port the CIM Extension will listen on for all available network cards

You can tell the port is in use by entering the following at the command prompt:

```
netstat -a | grep 1234
```

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM Extension to listen on only on a specific network interface card (NIC) by using the “-on” command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM Extension listens only on the NIC that has the IP address 192.168.99.37.

The “-on” command line option may be repeated as often as desired to direct the CIM Extension to listen on multiple NICs, for example:

```
./start -on 192.168.2.2 -on 192.168.1.1
```

The CIM Extension listens only on the NICs that have the IP address 192.168.2.2 or 192.168.1.1.

The “-on” command line option may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
./start -on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The “-port” command line option may be used in conjunction with the “-on” option. Any “-on” arguments that do not specify an explicit port number use the “-port” option argument as the port number, for example:

```
./start -on 192.168.1.1:3456 -on 192.168.2.2 -port 1170
```

This command tells the CIM Extension to listen on the following ports:

- Port 3456 on the NIC with the IP address 192.168.1.1
- Port 1170 on the NIC with the IP address 192.168.2.2

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the NIC
- 1234 is the new port number

If you have already added the NIC to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the NIC with different ports.

## Starting the CIM Extension by chkconfig

After installation, appqcime chkconfig is on by default. This means the appqcime service starts automatically after the host is rebooted. The appqcime service must be running for the management server to obtain information about the host. You can disable the appqcime service so that it does not start automatically after a reboot.

---

**NOTE:** You can only disable appqcime from starting automatically after a reboot if you are at run level 2.

---

To check the appqcime chkconfig status, enter the following at the command prompt:

```
chkconfig | grep appqcime
```

If appqcime is capable of starting after a reboot, it is shown to be on, as displayed in the following output:

```
appqcime on
```

To disable appqcime from starting after a reboot, enter the following at the command prompt:

```
chkconfig appqcime off
```

If you have disabled the automatic start-up of appqcime and you want to enable appqcime so it will start after a reboot, enter the following at the command prompt:

```
chkconfig appqcime on
```

## Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:

```
./start -version
```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
CXWS for mof/cxws/cxws-irix.mof
```

```
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

where

- `x.x.x.x` is the version of the CIM Extension
- `xxxx` is the year.

## Modifying the Boot Time RC Start Script (Optional)

When you install the CIM Extension, its start script is put in the `/etc/rc2.d` directory with the file name `S99appqcime`. The CIM Extension uses this script to start at boot time. You can modify this script if you want to add parameters. Any parameter you can add when you manually start the CIM Extension, such as `-port`, can be added to the start script.

To modify the file:

1. Open `S99appqcime` in a text editor.
2. Find the following line of code:

```
${APPIQ_HOME}/tools/start
```

3. Add the parameter after `/start`. For example, assume you want to change the port for the CIM Extension to port 1234. You would add `-port 1234` after `/start`, as shown in the following example:

```
${APPIQ_HOME}/tools/start -port 1234
```

4. Save the file.

The changes take effect the next time the script executed when the host reboots.

## Stopping the CIM Extension

To stop the background process for the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory:

```
./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

## Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the `cxws.log` file. The `cxws.log` files roll over once the files become more than 30 MB. The information in `cxws.log` is moved to `cxws.log.1`. If `cxws.log.1`, already exists, `cxws.log.2` is created. The numbering for the files continues sequentially, for example, `cxws.log.3`, `cxws.log.4`, etc.

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The cxws.out file is rewritten each time the CIM Extension restarts.

## How to Determine if the CIM Extension Is Running

You can determine if the CIM Extension is running by entering the following command at the command prompt:

```
./status
```

The process for the CIM Extension is displayed.

The CIM Extension is running when a message resembling the following is displayed:

```
CIM Extension Running
```

## Removing the CIM Extension from SGI IRIX

To remove the CIM Extension for IRIX:

1. Stop the CIM Extension as mentioned in "[Stopping the CIM Extension](#)" on page 84.
2. Enter the following at the command prompt:

```
inst
```

3. Enter the following at the Inst command prompt:

```
Inst> remove
```

4. When you are asked which subsystem you want to remove, enter the following:

```
APPQcime
```

5. To begin the removal of the CIM Extension, enter the following at the Inst command prompt:

```
Inst> go
```

The CIM Extension is removed from IRIX.

6. To exit the Inst Main Menu, enter the following:

```
Inst> quit
```



---

## 9 Installing the CIM Extension for SUSE and Red Hat Linux

This chapter describes the following:

- “About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux” on page 87
- “Prerequisites” on page 87
- “Verifying SNIA HBA API Support” on page 88
- “Installing the CIM Extension” on page 89
- “Starting the CIM Extension Manually” on page 89
- “Finding the Status of the CIM Extension” on page 92
- “Stopping the CIM Extension” on page 93
- “Rolling Over the Logs” on page 93
- “Removing the CIM Extension from Red Hat or SUSE Linux” on page 93

---

**IMPORTANT:** Make sure you have reviewed the table, [Table 2](#) on page 1 in the Overview chapter to ensure you are at the correct step.

---

### About the CIM Extension for Red Hat Linux Advanced Server and SUSE Linux

The CIM Extension for Red Hat and SUSE Linux gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

---

**IMPORTANT:** Install the CIM Extension on each host you want the management server to manage.

---

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web site:

[http://www.snia.org/tech\\_activities/hba\\_api/](http://www.snia.org/tech_activities/hba_api/)

### Prerequisites

#### **Red Hat Linux Advanced Server 3.0 Update 2**

(may just be i386.rpm on certain customer configurations)  
requires glibc-2.3.2-95.20.i686.rpm (update2 CD2)  
requires laus-0.1-54RHEL3.i386.rpm (update2 CD2)  
requires compat-libstdc++-7.3-2.96.128.i386.rpm (update2 CD3)  
requires libgcc-3.2.3-34.i386.rpm (update2 CD2)

### **Red Hat Linux Advanced Server 2.1 Update 4**

(may just be i386.rpm on certain customer configurations)  
requires glibc-2.2.4-32.15.i686.rpm (update4 CD1)  
requires compat-libstdc++-6.2-2.9.0.16.i386.rpm (update4 CD1)

### **SUSE 8**

compat-2003.1.10-0

### **SUSE 9**

compat-2004.7.1-1.2

### **Required Disk Space**

75 MB

### **Network Port Must Be Open**

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Linux host for more information. If you need to use a different port, see "[Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#)" on page 159.

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the hbatest program, which is accessible from the CIM Extension CD-ROM. The program, hbatest, lists the name and number for all HBA's that support the SNIA HBA API.

To run hbatest:

1. Go to the `linux/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`

The program runs its diagnostics.

## Driver Information for Verifying SNIA Emulex Adapters on Red Hat Linux

Emulex Adapters SNIA comes from package HBAnyware. To view the library location, enter the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

## Driver Information for Verifying QLogic SNIA Adapters on Red Hat Linux



QLogic SNIA Adapters comes from package qlapi-vX.XXX-rel.tgz found in the QLogic driver. The adapters are installed separately after driver. To view the location of the library, enter the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
qla2x00 /usr/lib/libqlsdrm.so
```

## Driver Information for Verifying QLogic SNIA Adapters on SUSE Linux

QLogic SNIA Adapters comes from package qlapi-vX.XXX-rel.tgz found in the QLogic driver. The adapters are installed separately after driver. To view the location of the library, enter the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
qla2x00 /usr/lib/libqlsdrm.so
```

## Installing the CIM Extension

Keep in mind the following:

- The instructions in this section apply if you are doing a local installation of the CIM Extension, as compared to a scripted or push installation. If you want to perform a scripted or push installation of the CIM Extension, first install the CIM Extension locally by using the instructions in this section. Then, perform the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.

To install the CIM Extension:

1. Login as root.
2. Go to the Linux directory on the CIM Extension CD-ROM by entering the following at the command prompt:

```
cd /cdrom/linux
```

where /cdrom is the name of the CD-ROM drive

3. Enter the following at the command prompt:

```
rpm -idvh APPQcime.rpm
```

The output is the following:

```
Preparing... ##### [100%]
 1:APPQcime ##### [100%]
```

The installation is done when you are returned to the command prompt.

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late` or `an error occurred`.
- To configure UNIX CIM Extensions to run behind a firewall, see [“Configuring UNIX CIM Extensions to Run Behind Firewalls”](#) on page 160.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./start
```

The following is displayed:

```
Starting CIM Extension for LINUX
.....
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
```

where

- `xxxx` is the year.
- `x.x.x.x` is the version of CIM Extension
- `192.168.1.5` is the IP address of the host

Keep in mind the following:

- Depending on your terminal type and processor speed, the message, `“CXWS x.x.x.x on /192.168.1.5 now accepting connections,”` may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.
- When you start the CIM Extension, you can change the port number the CIM Extension uses. See [“Changing the Port Number”](#) on page 90 for more information.

## Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, use the `./start -port port_number` command to change the port the CIM Extension will access. For example, if you are running a J2EE server, such as BEA WebLogic or IBM WebSphere, the J2EE server might already be using the 4673 port.

---

**IMPORTANT:** The steps provided in the section provide information about temporarily changing the port of the CIM Extension. If you want to permanently change the port the CIM Extension uses, see [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159.

---

To change the port, enter the following:

```
./start -port 1234
```

where 1234 is the port the CIM Extension will listen on for all available network cards

You can tell the port is in use by entering the following at the command prompt:

```
netstat -a | grep 1234
```

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM Extension to listen on only on a specific network interface card (NIC) by using the “-on” command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM Extension listens only on the NIC that has the IP address 192.168.99.37.

The “-on” command line option may be repeated as often as desired to direct the CIM Extension to listen on multiple NICs, for example:

```
./start -on 192.168.2.2 -on 192.168.1.1
```

The CIM Extension listens only on the NICs that have the IP address 192.168.2.2 or 192.168.1.1.

The “-on” command line option may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
./start -on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The “-port” command line option may be used in conjunction with the “-on” option. Any “-on” arguments that do not specify an explicit port number use the “-port” option argument as the port number, for example:

```
./start -on 192.168.1.1:3456 -on 192.168.2.2 -port 1170
```

This command tells the CIM Extension to listen on the following ports:

- Port 3456 on the NIC with the IP address 192.168.1.1
- Port 1170 on the NIC with the IP address 192.168.2.2

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the NIC
- 1234 is the new port number

If you have already added the NIC to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the NIC with different ports.

## Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:

```
./start -version
```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
CXWS for mof/cxws/cxws-linux.mof
CXWS version 3.6.0.39, built on Thu 7-October-2004 03:05:44 by dmaltz
```

## Finding the Status of the CIM Extension

You can always check the status of the CIM Extension by entering the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
where 93 is the process ID running the CIM Extension
```

## Modifying the Boot Time RC Start Script (Optional)

The CIM Extension uses the `S99appqcime` script to start at boot time. You can modify this script if you want to add parameters. Any parameter you can add when you manually start the CIM Extension, such as `-port`, can be added to the start script.

The S99appqcime script is in the following directories so that the CIM Extension can start when the ASCII or graphic user interface (GUI) mode is enabled:

- /etc/rc3.d - The directory for when the host starts in ASCII mode
- /etc/rc5.d - The directory for when the host starts in the GUI mode

To modify the file:

1. Open S99appqcime in a text editor.
2. Find the following line of code:

```
/${APPIQ_HOME}/tools/start
```

3. Add the parameter after /start. For example, assume you want to change the port for the CIM Extension to port 1234. You would add -port 1234 after /start, as shown in the following example:

```
/${APPIQ_HOME}/tools/start -port 1234
```

4. Save the file.

The changes take effect the next time the script executed when the host reboots.

## Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the /opt/APPQcime/tools directory, where /opt is the directory into which you installed the CIM Extension:

```
./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

## Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the cxws.log file. The cxws.log files roll over once the files become more than 30 MB. The information in cxws.log is moved to cxws.log.1. If cxws.log.1, already exists, cxws.log.2 is created. The numbering for the files continues sequentially, for example, cxws.log.3, cxws.log.4, etc.

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The cxws.out file is rewritten each time the CIM Extension restarts.

## Removing the CIM Extension from Red Hat or SUSE Linux

To remove the CIM Extension for Red Hat or SUSE Linux as root:

1. Login as root.
2. Stop the CIM Extension, as described in the topic, “[Stopping the CIM Extension](#)” on page 93.

3. Enter the following at the command prompt:

```
rpm -e APPQcime
```

The removal of the CIM Extension is complete, when you are returned to the command prompt.

---

# 10 Installing the CIM Extension for Sun Solaris

This chapter describes the following:

- "About the CIM Extension for Solaris" on page 95
- "Prerequisites" on page 95
- "Verifying SNIA HBA API Support" on page 96
- "Installing the CIM Extension" on page 97
- "Starting the CIM Extension Manually" on page 98
- "Finding the Status of the CIM Extension" on page 102
- "Stopping the CIM Extension" on page 102
- "Rolling Over the Logs" on page 102
- "Removing the CIM Extension from Solaris" on page 103

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

## About the CIM Extension for Solaris

The CIM Extension for Sun Solaris gathers information from the operating system and host bus adapters. It then makes the information available to the management server.

---

**IMPORTANT:** Install the CIM Extension on each host you want the management server to manage.

---

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). The management server only supports communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web site: [http://www.snia.org/tech\\_activities/hba\\_api/](http://www.snia.org/tech_activities/hba_api/)

## Prerequisites

The management server requires certain packages and patches. The installation checks for the required packages listed in the following section and verifies that Solaris 8 has been installed.

You need the core set SUNWCreq. If you have only the core environment packages installed, install the following manually in the **exact** order:

1. SUNWlibC - Sun Workshop Compilers Bundled libC
2. SUNWlibCf - SunSoft WorkShop Bundled libC (cfront version)
3. SUNWlibCx - Sun Workshop Bundled 64-bit libC

---

**IMPORTANT:** Verify you have the latest patches installed. The patches can be obtained from the Sun Microsystems Web site at <http://www.sun.com>.

---

You must have the following space:

- **CIM Extension** - The CIM Extension requires 90 MB of disk space.
- **Logs** - Make sure you have 100 MB for log files.
- **File SRM** - If you plan to have File SRM scan this host, make sure you have 220 to 230 MB for each set of 1 million files.

### Network Port Must Be Open

The CIM Extension uses port 4673 by default to communicate with the management server. Verify the network port is open. Refer to the documentation accompanying your Sun Solaris host for more information. If you need to use a different port, see "[Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)](#)" on page 159.

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the `hbatest` program, which is accessible from the CIM Extension CD-ROM. The program, `hbatest`, lists the name and number for all HBA's that support the SNIA HBA API. In some instances `hbatest` may report it cannot find an HBA driver even though an HBA driver is installed. Try installing a different version of the HBA driver that is SNIA compliant.

To run `hbatest`:

1. Go to the `Solaris/tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `./hbatest`

The program runs its diagnostics.

## Driver Information for Verifying SNIA Emulex Adapters

The SNIA Library comes from a separate package `HBAAnyware`. If you installed SNIA Emulex adapter, you can find its library by entering the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

## Driver Information for QLogic Adapters

The SNIA HBA package comes from a separate package `QLSDMLIB`. If you installed the QLogic Adapter, you can find its library by entering the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
qla2x00 /usr/lib/libqlsdm.so
```



## Driver Information for AMCC/JNI Adapters

The SNIA HBA driver for AMCC/JNI adapters comes from a separate package JNIsnia. You can find its library by entering the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so
JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so
```

## Driver Information for Sun Leadville branded QLogic or JNI Adapters

The SNIA HBA comes from the Sun StorEdge SAN Foundation Suite. Package SUNWfchba installed as part of suite. You can find its library by entering the following at the command prompt:

```
more /etc/hba.conf
```

The following is displayed:

```
com.sun.fchba /usr/lib/libsun_fc.so.1
com.sun.fchba64 /usr/lib/sparcv9/libsun_fc.so.1
```

## Installing the CIM Extension

Keep in mind the following:

- The instructions in this section apply if you are doing a local installation of the CIM Extension, as compared to a scripted or push installation. If you want to perform a scripted or push installation of the CIM Extension, first install the CIM Extension locally by using the instructions in this section. Then, perform the scripted or push installation. The instructions in this section only need to be performed once if you are doing a scripted or push installation. Contact customer support for information about performing a scripted or push installation.
- The server must be running sh, ksh or bash shell. C shell is not supported.

To install the CIM Extension:

1. Login as root.
2. Go to the Solaris directory on the CIM Extension CD-ROM by entering the following at the command prompt:

```
cd /cdrom/cdrom0/Solaris
```

where /cdrom/cdrom0 is the name of the CD-ROM drive
3. Enter the following at the command prompt:

```
pkgadd -d .
```

The APPQcime package is added.
4. When you are asked for the name of the package to install, type the corresponding number for the APPQcime package.
5. When you are asked for an installation directory, enter the path to the directory into which you want to install the CIM Extension.

If you want to install the CIM Extension into the default directory (/opt), press ENTER.

6. When you are asked if you want to continue the installation, enter **y**.  
The CIM Extension is installed.
7. When you are asked if you want to add another package, enter **q** to quit the installation.
8. If you see error messages when you install the CIM Extension, see [“Removing the CIM Extension from Solaris”](#) on page 103.
9. Unmount the CD-ROM by entering the following at the command prompt:  

```
umount /cdrom
```

 where `/cdrom` is the name of the directory where you mounted the CD-ROM
10. Start the CIM Extension. See [“Starting the CIM Extension Manually”](#) on page 98.

## Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM Extension is running.

Keep in mind the following:

- You must have root privileges to run the CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with root privileges, the management server will display messages resembling the following: `Data is late or an error occurred.`
- To configure UNIX CIM Extensions to run behind a firewall, see [“Configuring UNIX CIM Extensions to Run Behind Firewalls”](#) on page 160.

To start the CIM Extension, type the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./start
```

The following is displayed:

```
Starting CIM Extension for Solaris
.....
```

The CIM Extension is ready to be contacted by the management server when it displays a message resembling the following:

```
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5 now accepting connections
```

where

- `xxxx` is the year.
- `x.x.x.x` is the version of CIM Extension
- `192.168.1.5` is the IP address of the host

---

**NOTE:** Depending on your terminal type and processor speed, the message, “CXWS x.x.x.x on /192.168.1.5 now accepting connections,” may not display all the network interface IPs on the host. Use the `/opt/APPQcime/tools/cxws.out` file to view the output from the CIM Extension.

---

When you start the CIM Extension, you can restrict the user accounts that can discover the host. You can also change the port number the CIM Extension uses. See the following topics for more information.

## Restricting the Users Who Can Discover the Host

The `./start -users user_name` command provides greater security by restricting access. When you use the management server to discover the host (**Discovery > Setup**), provide a user name that was specified in the `-users` parameter in the start command. The following is an example of the command:

```
./start -users myname
```

where `myname` is a valid Solaris user name that must be used to discover this Solaris host.

For example, assume you want to use the management server to discover a Solaris host, but you do not want to provide the password to the root account. You can provide the password to another valid Solaris user account that has less privileges, for example `lesspriv`. You would log into the Solaris host as root and start the CIM extension by using the following command:

```
./start -users lesspriv
```

where `lesspriv` is a valid Solaris user name.

You would then logon to the management server, access the Discovery page (**Discovery > Setup**), and click the **Add Address** button. In the Add Address for Discovery page, provide the user name and password for `lesspriv`. Only the user name and password for `lesspriv` can be used to discover the Solaris host. This is because you used `lesspriv` in the `./start -users` command.

Another variation of the `start` command lets you provide multiple users in a colon-separated list, for example:

```
./start -users myname:jsmith
```

One of the names listed (`myname` or `jsmith`) must be used to discover the Solaris host (**Discovery > Setup** on the management server). Other user names and passwords, including root will not work.

## Changing the Port Number

The CIM Extension uses port 4673 by default. If the port is already used, use the `./start -port port_number` command to change the port the CIM Extension will access. For example, if you are running a J2EE server, such as BEA WebLogic or IBM WebSphere, the J2EE server might already be using the 4673 port.

---

**IMPORTANT:** The steps provided in the section provide information about temporarily changing the port of the CIM Extension. If you want to permanently change the port the CIM Extension uses, see [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159.

---

To change the port, enter the following:

```
./start -port 1234
```

where 1234 is the port the CIM Extension will listen on for all available network cards

You can tell the port is in use by entering the following at the command prompt:

```
netstat -a | grep 1234
```

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM Extension to listen on only on a specific network interface card (NIC) by using the “-on” command line option in the start command, for example:

```
./start -on 192.168.2.2
```

The CIM Extension listens only on the NIC that has the IP address 192.168.99.37.

The “-on” command line option may be repeated as often as desired to direct the CIM Extension to listen on multiple NICs, for example:

```
./start -on 192.168.2.2 -on 192.168.1.1
```

The CIM Extension listens only on the NICs that have the IP address 192.168.2.2 or 192.168.1.1.

The “-on” command line option may include a port specification. In that case, the CIM Extension listens on the indicated port of the indicated NIC, rather than the default port, for example:

```
./start -on 192.168.2.2:3456
```

The CIM Extension listens only on the NIC that has the IP address 192.168.2.2 on port 3456.

The “-port” command line option may be used in conjunction with the “-on” option. Any “-on” arguments that do not specify an explicit port number use the “-port” option argument as the port number, for example:

```
./start -on 192.168.1.1:3456 -on 192.168.2.2 -port 1170
```

This command tells the CIM Extension to listen on the following ports:

- Port 3456 on the NIC with the IP address 192.168.1.1
- Port 1170 on the NIC with the IP address 192.168.2.2

The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the NIC
- 1234 is the new port number

If you have already added the NIC to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the NIC with different ports.

## Finding the Version of a CIM Extension

You can find the version number of a CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Type the following at the command prompt:

```
./start -version
```

You are shown the version number of the CIM Extension and the date it was built, as shown in the following example:

```
CXWS for mof/cxws/cxws-solaris.mof
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

where

- x.x.x.x is the version for the CIM Extension
- xxxx is the year

## Combining Start Commands

You can also combine the `-users` and `-port` commands as follows:

```
./start -users myname -port 1234
```

or

```
./start -port 1234 -users myname
```

where

`myname` is the user name that must be used to discover this Solaris host

`1234` is the new port

## Finding the Status of the CIM Extension

You can always check the status of the CIM Extension by entering the following in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./status
```

The CIM Extension is running when the following message is displayed:

```
CIM Extension Running: Process ID: 93
```

where 93 is the process ID running the CIM Extension

## Modifying the Boot Time RC Start Script (Optional)

When you install the CIM Extension, its start scrip is put in the `/etc/rc3.d` directory with the file name `S99appqcime`. The CIM Extension uses this script to start at boot time. You can modify this script if you want to add parameters. Any parameter you can add when you manually start the CIM Extension, such as `-port`, can be added to the start script.

To modify the file:

1. Open `S99appqcime` in a text editor.
2. Find the following line of code:  

```
/${APPIQ_HOME}/tools/start
```
3. Add the parameter after `/start`. For example, assume you want to change the port for the CIM Extension to port 1234. You would add `-port 1234` after `/start`, as shown in the following example:

```
/${APPIQ_HOME}/tools/start -port 1234
```

4. Save the file.

The changes take effect the next time the script executed when the host reboots.

## Stopping the CIM Extension

To stop the CIM Extension, enter the following at the command prompt in the `/opt/APPQcime/tools` directory, where `/opt` is the directory into which you installed the CIM Extension:

```
./stop
```

Keep in mind the following:

- You must have root privileges to stop the CIM Extension.
- When you stop the CIM Extension, the management server is unable to gather information about this host.

## Rolling Over the Logs

The logging information for the CIM Extension is contained primarily in the `cxws.log` file. The `cxws.log` files roll over once the files become more than 30 MB. The information in `cxws.log` is moved to `cxws.log.1`. If `cxws.log.1`, already exists, `cxws.log.2` is created. The numbering for the files continues sequentially, for example, `cxws.log.3`, `cxws.log.4`, etc.

The cxws.out file contains some logging information, such as the CIM Extension starting, which is recorded in case something unexpected happens with the Java Virtual Machine. The cxws.out file is rewritten each time the CIM Extension restarts.

## Removing the CIM Extension from Solaris

To remove the CIM Extension for Solaris as root:

1. Login as root.
2. Stop the CIM Extension, as described in the topic, "[Stopping the CIM Extension](#)" on page 102.
3. Enter the following at the command prompt:  
`# pkgrm APPQcime`
4. Enter **y** when you are asked if you want to remove the CIM Extension.

When you see the following message, the CIM Extension has been removed:

```
Removal of <APPQcime> was successful.
```





---

# 11 Installing the CIM Extension for Microsoft Windows

This chapter describes the following:

- "About the CIM Extension for Windows" on page 105
- "Finding Applications Dependent on WMI" on page 106
- "How to Determine If WMI Is Running" on page 106
- "Verifying SNIA HBA API Support" on page 107
- "Installation Steps" on page 109
- "Installing the CIM Extension Using the Silent Installation" on page 110
- "Removing the CIM Extension from Windows" on page 110

Make sure you have reviewed [Table 2](#) on page 1 to ensure you are at the correct step.

## About the CIM Extension for Windows

The CIM Extension for Windows gathers information from the operating system and host bus adapters. It then makes the information available to the management server. It plugs into Windows Management Instrumentation (WMI), and thus, the CIM Extension is not a separate process. Microsoft created WMI as its implementation of Web-based Enterprise Management (WBEM). For more information about WMI, refer to the Microsoft Web site at <http://www.microsoft.com>.

Keep in mind the following:

- Install the CIM Extension on each host.
- The installation restarts WMI to make it aware of the CIM Extension. Services or applications using WMI are shut down. You will need to restart those applications manually. For example, Microsoft Exchange System Manager uses the Microsoft Exchange Management service, which depends on WMI. After the installation, you need to start the Microsoft Exchange Management service so that Microsoft Exchange System Manager becomes available. It is strongly recommended that before you install the CIM Extension, make note of services and applications using WMI. If you are not aware of the applications using WMI, see "[Finding Applications Dependent on WMI](#)" on page 106.
- The CIM Extension starts automatically whenever the system is restarted.
- If the Windows host has an Emulex LP9000-class host bus adapter (HBA), make sure you have the latest windows drivers for the HBA from the Emulex Web site at <http://www.emulex.com>. Follow the instructions that are provided on the Web site.

The CIM Extension communicates with an HBA by using the Host Bus Adapter Application Programming Interface (HBAAPI) created by the Storage Network Industry Association (SNIA). Some HBA vendors register their HBA drivers with the HBAAPI through the Windows registry. The management server only supports HBA communication with HBAs that are compliant with the HBAAPI. For more information about the HBAAPI, see the following Web page at the SNIA Web Site: [http://www.snia.org/tech\\_activities/hba\\_api/](http://www.snia.org/tech_activities/hba_api/)

## Finding Applications Dependent on WMI

The installation restarts WMI to make it aware of the CIM Extension. Services or applications using WMI are shut down. You need to restart those applications manually.

To find applications dependent on WMI:

1. Right-click **My Computer**.
2. Select **Manage** from the drop-down menu.
3. In the left pane of the **Computer Management** window, select **Services and Applications**.
4. In the right pane, double-click **Services**.
5. In the right pane, right-click **Windows Management Instrumentation**.
6. Select **Properties** from the drop-down menu.
7. Make note of the applications dependent on WMI.

## How to Determine If WMI Is Running

---

**NOTE:** The following steps are for Microsoft Windows 2000. For later versions of Microsoft Windows, refer to the documentation for your operating system.

---

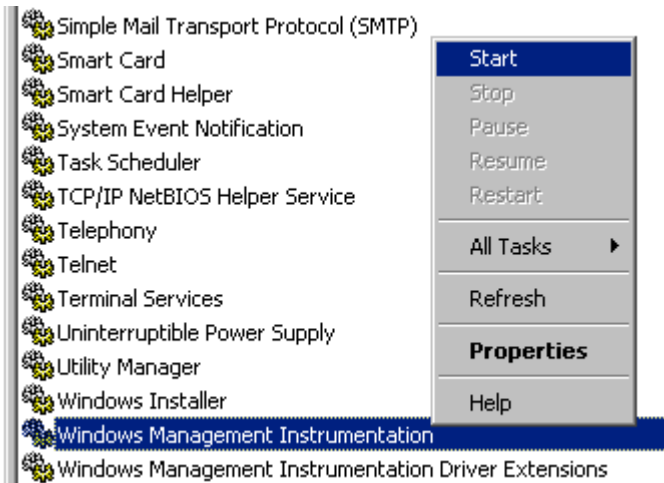
To determine if WMI is running:

1. Right-click **My Computer**.
2. Select **Manage** from the drop-down menu.
3. In the left pane of the **Computer Management** window, select **Services and Applications**.
4. In the right pane, double-click **Services**.
5. In the right pane, select **Windows Management Instrumentation**. Its status is displayed in the **Status** column.

---

**NOTE:** You can start the service by right-clicking **Windows Management Instrumentation** and selecting **Start** from the drop-down menu.

---



**Figure 1** Starting WMI (Microsoft Windows 2000)

## Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. You can run the `hbatest` program, which is accessible from the CIM Extension CD-ROM. The program, `hbatest`, lists the name and number for all HBA's that support the SNIA HBA API.

---

**IMPORTANT:** If you have an Emulex host bus adapter (HBA) on the host, you must install the full HBAnywhere package. If you do not install the full HBAnywhere package, `hbatest` will still detect the Emulex HBA but the installation for the CIM Extension will fail with the message that it cannot find any supported HBAs on the host. Contact Emulex at <http://www.emulex.com> for more information on how to obtain the full HBAnywhere package.

---

To run `hbatest`:

1. Open a command prompt window and go to the `Windows\tools` directory on the CIM Extension CD-ROM.
2. Enter the following at the command prompt: `hbatest.exe`  
The program runs its diagnostics.

## Driver Information for Verifying SNIA Emulex Adapters

This section lists the SNIA information for Emulex adapters.

**If you have SNIA HBA from HBAnywhere:**

When you install the SNIA HBA that comes from HBAAnyware, the SNIA registry setting is most likely in the following location:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SNIA\HBA\org.emulex.emulexhbaapi

The following lists the possible locations for the various drivers:

- Microsoft Windows 2003 Service Pack 1 drivers point to emulexhbaapi.dll. The emulexhbaapi.dll file can be found at C:\Program Files\HBAAnyware\emulexhbaapi.dll
- Windows 2003 drivers have registry point to emulexhbaapi.dll. The emulexhbaapi.dll file can be found at c:\winnt\system32\emulexhbaapi.dll and c:\winnt\system32\hbaapi.dll.
- Windows 2000 drivers have registry point to emulexhbaapi.dll. The emulexhbaapi.dll file can be found at c:\winnt\system32\emulexhbaapi.dll and c:\winnt\system32\hbaapi.dll.

#### **If you have SNIA HBA from lputil:**

When you install the SNIA HBA that comes from lputil only, the SNIA registry setting is most likely in the following location:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SNIA\HBA\org.emulex.emulexhbaapi

The following lists the possible locations for the various drivers:

- Registry points to emulexhbaapi.dll
- The dll can be found at c:\winnt\system32\hbaapi.dll
- The dll can be found at c:\winnt\system32\emulexhbaapi.dll

#### **If you have SNIA HBA from Elxcfg:**

When SNIA HBA comes from Elxcfg, the SNIA registry setting is most likely in the following location:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SNIA\HBA.

The driver can be found in the following location:

c:\winnt\system32\hbaapi.dll

## Driver Information for Verifying IBM Branded QLogic Adapters

This section provides information for verifying IBM branded QLogic adapters.

#### **If you have IBM Branded QLogic Adapters:**

The SNIA HBA comes from IBM MSJ (FastT Management Suite Java). The registry setting is most likely in the following location:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SNIA\HBA\QL2XXX

The driver can be found in the following location:

C:\Program Files\IBM FAST MSJ\ql2xhai2.dll

## Driver Information for Verifying QLogic Adapters

This section provides information for verifying QLogic adapters.

### If you have QLogic Adapters:

When you install the SNIA HBA, it either came with the driver or SANsurfer, the registry setting is most likely in the following location, which varies by release:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SNIA\HBA\QL2XXX

Newer drivers points to C:\WINNT\system32\ql2xhai2.dll, but they also have system32\qlsdm.dll available. Earlier drivers points to C:\WINNT\System32\qlsdm.dll

## Driver Information for Verifying AMCC/JNI Adapters

The SNIA HBA comes from JNI SNIA 2.0. The SNIA Library is in a separate package without the drivers. The registry setting is the following:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SNIA\HBA\JNI

The SNIA Library can be found in the following location:

C:\Program Files\JNI\JNISnia\Jni\JniHbaLib.dll

## Installation Steps

Keep in mind the following:

- If the installation fails with the message it cannot detect any supported HBAs and Emulex HBAs are installed on the host, install the full HBAAnywhere package. Contact Emulex at <http://www.emulex.com> for more information on how to obtain full HBAAnywhere package.
- You must have administrator privileges to install this software.
- Make sure other computers, including the management server, are not requesting the WMI service from the host during installation.
- Make sure no other programs are running when you install the CIM Extension.
- On Microsoft Windows 2003 servers “Explorer Enhanced Security Settings” is enabled by default. If this setting is enabled, the “Authenticode signature not found” message is displayed during installation. Ignore the message or disabled the “Explorer Enhanced Security Settings”.

Perform the following steps:

1. Insert the CD-ROM for the CIM Extensions, go to the Windows directory and then double-click **InstallCIMExtensions.exe**.
2. If you are asked if you want to install the product, click **Yes**.
3. When you see the introduction screen, click **Next**.
4. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, click the **Choose** button. You can always display the default directory by clicking the **Restore Default Folder** button. When you are done, click **Next**.

5. Read the important notes, such as installing the CIM Extension on your system will stop any service that depends on the Windows WMI service. An example is the Microsoft Exchange Management Service. You will need to restart those services or reboot your system when the installation is complete. Then, click **Next**.
6. Check the pre-installation summary. You are shown the following:
  - Product Name
  - Installation Folder
  - Disk Space Required
  - Disk Space Available
7. Do one of the following:
  - Click **Install** if you agree with the pre-installation summary.
  - Click **Previous** if you want to modify your selections.The CIM Extension is installed.
8. When you have been told the installation has been successful, click **Done** to quit the installation.

---

**IMPORTANT:** Keep in mind that the CIM Extension automatically starts when the system is restarted. The management server can only obtain information from this host when the CIM Extension is running.

---

## Installing the CIM Extension Using the Silent Installation

The CIM Extension for Windows provides a silent installation which installs the CIM Extension with no user interaction, all default settings are used.

Keep in mind the following:

- You must have administrator privileges to install this software.
- Make sure other computers, including the management server, are not requesting the WMI service from the host during installation.
- Make sure no other programs are running when you install the CIM Extension.
- Remove the previous version of the CIM Extension before you install the latest version.

To install the CIM Extension using the silent installation:

1. Insert the CD-ROM for the CIM Extensions.
2. Open a command prompt window and go to the Windows directory on the CD-ROM.
3. Enter the following at the command prompt:

```
E:\Windows>InstallCIMExtensions.exe -i silent
```

where E is the CD-ROM drive. The silent installation installs the CIM Extension in the default location.

## Removing the CIM Extension from Windows

To remove the CIM Extension for Windows:

1. Go to the Control Panel in Microsoft Windows.
2. Double-click **Add or Remove Programs**.
3. From the Currently installed programs list, select **Windows CIM Extension**.
4. Click the **Change/Remove** button.
5. When you are told the product is about to be uninstalled, click **Uninstall**.
6. When the program is done with removing the product, click **Done**.
7. It is highly recommended you reboot the host.





---

## 12 Discovering Applications and Hosts

This chapter describes the following:

- “[Step 1 - Discovering Your Hosts](#)” on page 113
- “[Step 2 - Setting Up Discovery for Applications](#)” on page 115
- “[Step 3 - Discovering Applications](#)” on page 128
- “[Changing the Oracle TNS Listener Port](#)” on page 129
- “[Adding/Modifying Microsoft Exchange Domain Controller Access](#)” on page 130
- “[Deleting a Microsoft Exchange Domain Controller](#)” on page 131
- “[Changing the Password for the Managed Database Account](#)” on page 131
- “[Obtaining Disk Drive Statistics from Engenio Storage Systems](#)” on page 132
- “[Assigning a File Extension in Netscape 7](#)” on page 132

### Step 1 - Discovering Your Hosts

Before you can discover your applications, you must discover their hosts. You discover hosts in the same way you discovered your switches and storage systems. You provide the host’s IP address, user name and password. The user name and password must have administrative privileges. Unlike switches and storage systems, you must have installed CIM Extension on the host if you want to obtain detailed information about the host.

Keep in mind the following:

- If you change the password of a host after you discover it, you must change the password for the host in the discovery list. Then, you must stop and restart the CIM Extension running on that host.
- Make sure you have reviewed the table, [Table 2](#) on page 1 to make sure you are at the correct step.
- If your license lets you discover UNIX and/or Linux hosts, the **Test** button for discovery reports SUCCESS from any UNIX and/or Linux hosts on which the management server can detect a CIM Extension. The CIM Extension must be running. The management server reports “SUCCESS” even if your license restricts you from discovering certain types of hosts. For example, assume your license lets you discover Solaris hosts but not AIX hosts. If you click the **Test** button, the management server reports “SUCCESS” for the AIX hosts. You will not be able to discover the AIX hosts. The IP address is not discoverable, because of the license limitation.
- You should have already installed a CIM Extension on the host you want to discover.
- If you want to receive status reports about Discovery Data Collection, see “[Configuring E-mail Notification for Discovery Data Collection](#)” on page 167 for information about how to configure this option.
- Depending on your license, you may not be able to access File System Viewer and/or monitor certain applications may not be available. See the List of Features to determine if you have access to File System Viewer and/or are able to monitor the other applications. The List of Features is accessible from the Documentation Center (**Help > Documentation Center** in

Storage Essentials). To learn more about File System Viewer, refer to the File Servers Guide, which is also available from the Documentation Center.

- If you are unable to discover a UNIX host because of DNS or routing issues, see [“Unable to Discover a UNIX Host Because of DNS or Routing Issues”](#) on page 176.

Discovery of hosts consists of two steps:

- Detecting the hosts by using HP Systems Insight Manager. See [“Step A - Set Up Discovery for Hosts”](#) on page 114.
- Obtaining details about those hosts by using the Discovery Data Collection feature in Storage Essentials. See [“Step B - Obtain Details”](#) on page 114.

## Step A - Set Up Discovery for Hosts

---

**IMPORTANT:** Dynamic disk support on Windows 2000 hosts is optional. If you want this feature enabled for Windows 2000 hosts, you can download LDMDump, as described in [“Enabling Dynamic Disk Detection for Windows 2000 Hosts”](#) on page 114.

---

Use HP Systems Insight Manager (SIM) to discover your hosts. Refer to your documentation for HP SIM for more information.

### Enabling Dynamic Disk Detection for Windows 2000 Hosts

Dynamic disk support for Windows 2000 hosts is optional. If you want this feature enabled for Windows 2000 hosts, perform the following steps for the management server to obtain information about dynamic disks on that host:

1. Download LDMDump from <http://www.sysinternals.com/Utilities/LdmDump.html> to the Windows 2000 host.
2. Unzip the LdmDump.zip file into the Windows\System32 folder on the Windows 2000 host.
3. Discover the Windows 2000 host.
4. If the management server detects LDMDump, the following is displayed in the Log Messages window.

```
Dynamic disk volumes supported via the utility 'ldmdump': Logical Disk
Manager Configuration Dump v1.03
```

---

**NOTE:** The version number displayed may vary from the version you downloaded.

---

## Step B - Obtain Details

Discovery Data Collection must be performed before you can do provisioning and/or obtain provisioning information, such as data about zone sets and LUN numbers.

Keep in mind the following:

- Obtaining details takes some time. You might want to perform this process when the network and the managed elements are not busy.
- If you want to enable File System Viewer for a host, make sure the File SRM option is selected.

- If Discovery Data Collection includes an AIX host, the system log displays three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port. You can ignore these errors.
- You can quarantine elements to exclude them from Discovery Data Collection. See [“Placing an Element in Quarantine”](#) on page 48 for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.
- When an element in a given discovery group is updated, its dependent elements are also updated. For example, assume Host\_A is the only element in Discovery Group 1. Host\_A is connected through a switch and storage system. When you Discovery Data Collection for Discovery Group 1, you also obtain details from the switch and storage system.
- If the management server unable to obtain information from a UNIX host during Discovery Data Collection as a result of a CIM Extension hanging, the management server places the access point where the CIM Extension is located in quarantine. The management server then moves onto getting details for the next element in the Discovery Data Collection table. These UNIX hosts appear as missing until they are removed from quarantine. See [“Removing an Element from Quarantine”](#) on page 49 for information on how to remove an element from quarantine.

To obtain details:

1. Select **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. Verify the **File SRM** option is selected. The File SRM option appears for hosts that have the CIM Extension and an operating system that supports File System Viewer.
3. Click the **Get Details** button.

For additional information, see [“Updating the Database with Element Changes”](#) on page 47 for information on how to automate the gathering of all element details. If you run into problems with discovery, see [“Troubleshooting”](#) on page 157.

## Step 2 - Setting Up Discovery for Applications

Keep in mind the following when discovering applications:

- Make a list of the applications you want to monitor. Configure your applications first as described in this section and then run discovery.
- You should have already installed a CIM Extension on the hosts that have the applications you want to discover. After you installed the CIM Extension, you should have already discovered the host. See [“Step 1 - Discovering Your Hosts”](#) on page 113.

You can configure the management server to monitor hosts and applications, such as Oracle, Microsoft Exchange server, and Sybase Adaptive Server Enterprise, in addition to Microsoft SQL servers and file servers. If you want to obtain detailed information about the host and its applications, you must install a CIM Extension on the host, as described in the previous chapters.

The following is an overview of what you need to do. It is assumed you have already discovered the hosts running your applications. See [“Step 1 - Discovering Your Hosts”](#) on page 113.

Then, set up the configurations for your applications on the management server. Some applications may require you to provide additional discovery information about the application. Finally,

perform discovery and then obtain Discovery Data Collection. Obtaining details takes some time. Perform this step when the network is not busy. More details about the steps mentioned above are provided later.

See the following topics for more information:

- ["Monitoring Oracle"](#) on page 116
- ["Monitoring Microsoft SQL Server"](#) on page 121
- ["Monitoring Sybase Adaptive Server Enterprise"](#) on page 123
- ["Monitoring Microsoft Exchange"](#) on page 126

## Monitoring Oracle

To monitor and manage Oracle, you must do the following:

- ["Step A - Create the APPIQ\\_USER Account for Oracle"](#) on page 116
- ["Step B - Provide the TNS Listener Port"](#) on page 118
- ["Step C - Set up Discovery for Oracle 10g"](#) on page 119

After you complete these steps, you must discover Oracle and obtain Discovery Data Collection. See ["Step 3 - Discovering Applications"](#) on page 128.

---

**IMPORTANT:** Before you begin these steps, make sure you purchased the module that lets you monitor Oracle. Contact your customer support if you are unsure if you purchased this module.

---

### Step A - Create the APPIQ\_USER Account for Oracle

The management server accesses Oracle through the APPIQ\_USER account. This account is created when you run the `CreateOracleAct.bat` script on Microsoft Windows or `CreateOracleAct.sh` on UNIX on the computer running the Oracle database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

Keep in mind the following:

- The `CreateOracleAct.bat` script must run under SYS user.
- Create APPIQ\_USER account on Oracle Database you want to monitor, not on the management server.
- You should have already installed the database for the management server.
- Verify that the instance TNS (Transparent Name Substrate) listener is running so that the management server can find the Oracle installation and its instances. For example on Microsoft Windows 2000, you can determine if the instance TNS listener is running by looking in the Services window for OracleOraHome92TNSListener. The name of the TNS listener might vary according to your version of Oracle. Refer to the Oracle documentation for information about verifying if the instance TNS listener is running. You can also verify the listener is running by entering the following at the command prompt: `lsnrctl status`. If the listener is not running you can start it by typing `lsnrctl start` on command line.

- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the Oracle user for management server:

1. Do one of the following:

- **To run the script on IBM AIX, SGI IRIX, or Sun Solaris**, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the `/DBIQ/Oracle/unix` directory by typing the following:

```
cd /cdrom/cdrom0/DBIQ/Oracle/unix
where /cdrom/cdrom0 is the name of the CD-ROM drive
```

- **To run the script on Microsoft Windows**, go to the `DBIQ\Oracle\win` directory on the CD-ROM.

---

**IMPORTANT:** You must complete the following steps.

---

2. Verify you have the password to the SYS user account.

You are prompted for the password for this user account when you run the script.

3. Run the `CreateOracleAct.bat` script on Microsoft Windows or `CreateOracleAct.sh` script on the UNIX operating system on the computer with the Oracle database.

The script creates a user with create session and select dictionary privilege on a managed Oracle instance.

---

**NOTE:** You can use a remote Oracle client to run this script.

---

4. Specify the Oracle instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the Oracle instance on which to create user for Oracle management packages and the password of the SYS account.

You are asked to specify the default and temporary tablespaces for APPIQ\_USER during the installation. You can enter users as default and temp as temporary if these tablespaces exist in the Oracle Instance.

5. Repeat the previous step for each Oracle instance you want to manage.

This script does the following in order:

- Creates the APPIQ\_USER account.
- Grant create session and select on dictionary tables privileges to APPIQ\_USER enabling management server to view statistics for the Oracle instances.

## Removing the APPIQ\_USER Account for Oracle

If you no longer want the management server to monitor an Oracle instance, you can remove the APPIQ\_USER account for that Oracle instance by running the `UninstallOracleAct.bat` script on Windows or `UninstallOracleAct.sh` script on the UNIX platform.

Keep in mind the following:

- Before you remove the APPIQ\_USER account for an Oracle instance, make sure no processes are running APPIQ\_USER for that Oracle instance. The management server uses APPIQ\_USER to obtain information about the Oracle database. For example, a process would be using APPIQ\_USER if someone was using Performance Manager to view monitoring statistics about that Oracle instance. After you removed the APPIQ\_USER account for Oracle, discover and perform Discovery Data Collection for the host if you want to continue monitoring it.
- If you receive a message about not being able to drop a user that is currently connected while you are removing the APPIQ\_USER account for Oracle, re-run the script for removing APPIQ\_USER.

To remove the APPIQ\_USER account for that Oracle instance:

1. If you plan to remove the management software for Oracle from the Solaris host, do the following:
  - a. Log into an account that has administrative privileges.
  - b. Mount the CD-ROM (if not auto-mounted)
  - c. Go to the `/DBIQ/Oracle/unix` directory by typing the following:
 

```
cd /cdrom/cdrom0/DBIQ/Oracle/unix
```

 where `/cdrom/cdrom0` is the name of the CD-ROM drive
2. If you plan to remove the management software for Oracle from a computer running Windows, go to the `\DBIQ\Oracle\win` directory on the CD-ROM.
3. Verify you have the password to the SYS user account.  
You are prompted for the password for this user account when you run the script.
4. Run the `UninstallOracleAct.bat` for Windows or `UninstallOracleAct.sh` script for UNIX platform on the computer with the Oracle database.
5. This script removes the management software for the specified Oracle instance.

---

**NOTE:** You can use a remote Oracle client to run this script.

---

6. When you are asked for the Oracle instance name, enter the name of the Oracle instance you do not want the management server to monitor. The name must be visible to the client.
7. Provide the password for the SYS user account.  
The APPIQ\_USER account for the specified Oracle instance is removed. The management server can no longer monitor that Oracle instance.

## Step B - Provide the TNS Listener Port

If your Oracle instances use a different TNS Listener Port than 1521, change the port as described in the following steps:

1. Select **Options > Protocol Settings > Storage Essentials > Global Application Discovery Settings**.  
The TNS Listener Port setting applies to all Oracle instances you monitor.
2. To assign a new port, click the **Create** button for the Oracle Information table.
3. Type the new port number and click **OK**.

4. If necessary, click the  button to remove the old port number.

---

**IMPORTANT:** Monitoring Oracle 10g and Oracle clusters require an additional step. If you are not monitoring Oracle 10g and Oracle clusters, see [“Step 3 - Discovering Applications”](#) on page 128.

---

## Step C - Set up Discovery for Oracle 10g

---

**NOTE:** If you are discovering an Oracle cluster, see [“Discovering Oracle Clusters”](#) on page 119.

---

To monitor Oracle 10g, provide additional information as described in the following steps:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, “No Targets Currently Selected,” change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

2. Select a target, and then, click **Run Now**.
3. Click the **Create** button for the Database Information table.
4. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Oracle. The **Management IP/DNS Name** field is optional.
5. In the **Server Name** field, type the Oracle System Identifier (SID) of the Oracle database you want to monitor.
6. In the **Port Number** field, type the monitored port.

If you are not sure of the monitored port, check the listener.ora file of the monitored database application. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

```
%ORA_HOME%\network\admin\listener.ora
```

The port can be found in the following code:

```
LISTENER =
 (DESCRIPTION_LIST =
 (DESCRIPTION =
 (ADDRESS_LIST =
 (ADDRESS = (PROTOCOL = TCP) (HOST = localhost) (PORT = 1521))
 (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC0))
)
)
)
```

7. Select **ORACLE** from the Database Type menu.
8. Click **OK**.

## Discovering Oracle Clusters

Perform the following steps for each node in the cluster:

1. Install the CIM Extension on each node in the cluster. See the Installation Guide for information on how to install the CIM Extensions. See ["Roadmap for Installation and Initial Configurations"](#) on page 1 for information about the CIM Extensions available.
2. Create the appiq\_user account on each node in the cluster. See ["Step A - Create the APPIQ\\_USER Account for Oracle"](#) on page 116.
3. Discover the host for the first node.
4. Discover first Oracle node as follows:

- a. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, "No Targets Currently Selected," change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

- b. Select a target, and then, click **Run Now**.
- c. Click the **Create** button for the Database Information table.
- d. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Oracle.

In the **Management IP/DNS Name** field, type the IP address the listener is listening on for the Oracle instance. The IP address can be a virtual IP or a host IP. You can find the IP address in the listener.ora file for the monitored database. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

```
%ORA_HOME%\network\admin\listener.ora
```

- e. In the **Server Name** field, type the Oracle System Identifier (SID) of the Oracle database you want to monitor.

- f. In the **Port Number** field, type the monitored port.

If you are not sure of the monitored port, check the listener.ora file of the monitored database application. You can find the listener.ora file in the following directory on the host of the monitored database. Do not look for the listener.ora file on the management server for this information.

```
%ORA_HOME%\network\admin\listener.ora
```



The port can be found in the following code:

```
LISTENER =
 (DESCRIPTION_LIST =
 (DESCRIPTION =
 (ADDRESS_LIST =
 (ADDRESS = (PROTOCOL = TCP) (HOST = localhost) (PORT = 1521))
 (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC0))
)
)
)
)
```

g. Select **ORACLE** from the Database Type menu.

h. Click **OK**.

5. Repeat Steps 4 and 5 for each node in the cluster.

## Monitoring Microsoft SQL Server

To manage and monitor Microsoft SQL Servers, you must do the following:

- “[Step A - Create the APPIQ\\_USER for the SQL Server](#)” on page 121
- “[Step B - Provide the Microsoft SQL Server Name and Port Number](#)” on page 122

---

**IMPORTANT:** Make sure the Microsoft SQL server database is in “Mixed Mode authentication.” To switch to mixed mode authentication, see “[Switching to Mixed Mode Authentication](#)” on page 121.

---

## Switching to Mixed Mode Authentication

Microsoft SQL Server must be running in Mixed Mode Authentication. You can switch to Mixed Mode Authentication as follows:

1. Open SQL Server Enterprise Manager (Start menu > **Programs** > **Microsoft SQL Server** > **Enterprise Manager**).
2. Expand the tree-control until you can see your server.
3. Right-click the server name.  
The SQL Server Properties (Configure) window appears.
4. Click the **Security** tab.
5. For “Authentication”, select **SQL Server and Windows**.

### Step A - Create the APPIQ\_USER for the SQL Server

The management server accesses SQL Server through the APPIQ\_USER account. This account is created when you run the `CreateSQLServerAct.bat` script on Microsoft Windows on the computer running the SQL Server database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

Keep in mind the following:

- The script must run under SA user.

- Obtain the SQL Server name before you run the script
- Create APPIQ\_USER account on SQL Server database you want to monitor.
- You should have already installed the database for the management server.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the APPIQ\_USER account for SQL Server:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CD-ROM.

---

**IMPORTANT:** You must complete the following steps.

---

2. Verify you have the password to the SA user account.  
You are prompted for the password for this user account when you run the script.
3. Run the `CreateSQLServerAct.bat` script on Microsoft Windows on the computer with the SQL Server database.  
The script creates a user with login to master and select privilege on data dictionary tables on a managed SQL Server instance.

---

**NOTE:** You can use a remote SQL Server `isql` to run this script.

---

4. Type the SQL Server instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the SQL Server on which to create user for SQL Server management packages and the password of the SA account.
5. Repeat the previous step for each SQL Server you want to manage.  
This script does the following in order:
  - Creates the APPIQ\_USER account.
  - Grant create session and select on dictionary tables privileges to APPIQ\_USER enabling management server to view statistics for the SQL Server.

## Removing the APPIQ\_USER Account for SQL Server

---

**IMPORTANT:** Before you remove the APPIQ\_USER account for the SQL Server databases on a host, make sure no processes are running APPIQ\_USER for that SQL Server database. The management server uses APPIQ\_USER to obtain information about a SQL Server database.

---

To remove the APPIQ\_USER account for the SQL Server databases on a host:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CD-ROM.

---

**IMPORTANT:** You must complete the following steps.

---

2. Verify you have the password to the SA user account.  
You are prompted for the password for this user account when you run the script.
3. Run the `UninstallSQLServerAct.bat` script on Microsoft Windows on the computer with the SQL Server database.
4. Type the name of the SQL Server server.
5. Type the password for the SA account.  
The account for APPIQ\_USER is removed. The management server can no longer monitor the SQL Server databases on this host.

## Step B - Provide the Microsoft SQL Server Name and Port Number

You must provide the server name for the Microsoft SQL server and port number for managing a SQL database in the following steps:

To add information for discovering a SQL server:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.  
To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, "No Targets Currently Selected," change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.
2. Select a target, and then, click **Run Now**.
3. Click the **Create** button for the Database Information table.
4. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Sybase.
5. You can leave the **Management IP/DNS Name** field blank. This field is for Oracle clusters. When you leave the **Management IP/DNS Name** field blank the management server automatically lists the DNS name or IP address of the host under the **Host IP/DNS Name** column and **Management IP/DNS Name** column.
6. In the **Server Name** field, type the SQL database you want to monitor.
7. In the **Port Number** field, type the port that SQL is using. If you do not enter a port number, the management server assumes you are using port 1433 (default).
8. Select **SQLSERVER** from the Database Type menu.
9. Click **OK**.

---

**IMPORTANT:** Perform Discovery Data Collection for your inputs to take effect. See "[Step 3 - Discovering Applications](#)" on page 128.


---

## Deleting SQL Server Information

If you do not want the management server to monitor a SQL Server instance, you can remove its information, as described in the following steps:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, "No Targets Currently Selected," change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

2. Select a target, and then, click **Run Now**.
3. In the Database Information table, click the  button, corresponding to the SQL Server instance you do not want the management server to monitor.
4. Perform Discovery Data Collection to make the management server aware of your changes.

## Monitoring Sybase Adaptive Server Enterprise

If you want to monitor Sybase Adaptive Server Enterprise you must:

- Create APPIQ\_USER account on the database for Sybase
- Provide the database server name and port number
- Discover the application.

The required drivers for Sybase Adapter Server Enterprise were automatically installed along with the management server.

---

**IMPORTANT:** Before you begin these steps, make sure you purchased the module that lets you monitor Sybase Adaptive Server Enterprise. Contact your customer support if you are unsure if you purchased this module.

---

### Step A - Create the APPIQ\_USER account for Sybase

The management server accesses Sybase through the APPIQ\_USER account. This account is created when you run the CreateSybaseAct.bat script on Microsoft Windows or CreateSybaseAct.sh on UNIX on the computer running the Sybase database you want to monitor. The account has create session and select dictionary privileges to be used with the management server.

Keep in mind the following:

- The script must run under SA user.
- Obtain the Sybase server name before you run the script
- Create APPIQ\_USER account on Sybase Database you want to monitor.
- You should have already installed the database for the management server.
- Make sure you have all the necessary information before you begin the installation. Read through the following steps before you begin.

To create the APPIQ\_USER account for the Sybase server:

1. Do one of the following:

- To run the script on IBM AIX, SGI IRIX, or Sun Solaris, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the /DBIQ/sybase/unix directory by typing the following:  

```
cd /cdrom/cdrom0/DBIQ/sybase/unix
```

where /cdrom/cdrom0 is the name of the CD-ROM drive
- To run the script on Microsoft Windows, go to the \DBIQ\sybase\win directory on the CD-ROM.

---

**IMPORTANT:** You must complete the following steps.

---

2. Verify you have the password to the SA user account.  
You are prompted for the password for this user account when you run the script.
3. Run the CreateSybaseAct.bat script on Microsoft Windows or CreateSybaseAct.sh script on the UNIX operating system on the computer with the Sybase database.  
The script creates a user with login to master and select privilege on data dictionary tables on a managed Sybase instance.

---

**NOTE:** You can use a remote Sybase isql to run this script.

---

4. Type the Sybase instance name, which must be visible to the client, as the first input when running the script. The script prompts you for the name of the sybase server on which to create user for Sybase management packages and the password of the SA account.
5. Repeat the previous step for each Sybase server you want to manage.  
This script does the following in order:
  - Creates the APPIQ\_USER account.
  - Grant create session and select on dictionary tables privileges to APPIQ\_USER enabling management server to view statistics for the Sybase server.

## Removing the APPIQ\_USER Account for Sybase

---

**IMPORTANT:** Before you remove the APPIQ\_USER account for the Sybase databases on a host, make sure no processes are running APPIQ\_USER for that Sybase database. The management server uses APPIQ\_USER to obtain information about a Sybase database.

---

To remove the APPIQ\_USER account for the Sybase databases on a host:

1. Do one of the following:
  - To run the script on IBM AIX, SGI IRIX, or Sun Solaris, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the /DBIQ/sybase/unix directory by typing the following:  

```
cd /cdrom/cdrom0/DBIQ/sybase/unix
```

where /cdrom/cdrom0 is the name of the CD-ROM drive

- To run the script on Microsoft Windows, go to the \DBIQ\sybase\win directory on the CD-ROM.

---

**IMPORTANT:** You must complete the following steps.

---

2. Verify you have the password to the SA user account.  
You are prompted for the password for this user account when you run the script.
3. Run the UninstallSybaseAct.bat script on Microsoft Windows or UninstallSybaseAct.sh script on the UNIX operating system on the computer with the Sybase database.
4. Type the name of the Sybase server.
5. Type the password for the SA account.  
The account for APPIQ\_USER is removed. The management server can no longer monitor the Sybase databases on this host.

## Step B - Provide the Sybase Server Name and Port Number

You must provide the Sybase server name and port number for managing the Sybase database in the following steps:

To add information for discovering Sybase Adaptive Server Enterprise:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.  
To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, "No Targets Currently Selected," change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.
2. Select a target, and then, click **Run Now**.
3. Click the **Create** button for the Database Information table.
4. In the **Host IP/DNS Name** field, type the IP address or DNS name of the host running Sybase.
5. You can leave the **Management IP/DNS Name** field blank. This field is for Oracle clusters. When you leave the **Management IP/DNS Name** field blank the management server automatically lists the DNS name or IP address of the host under the **Host IP/DNS Name** column and **Management IP/DNS Name** column.
6. In the **Server Name** field, type the Sybase database you want to monitor.
7. In the **Port Number** field, type the port that Sybase is using.
8. Select **SYBASE** from the Database Type menu.
9. Click **OK**.

---

**IMPORTANT:** Perform Discovery Data Collection for your inputs to take effect. See “[Step 3 - Discovering Applications](#)” on page 128.

---


## Deleting Sybase Information

If you do not want the management server to monitor a Sybase instance, you can remove its information, as described in the following steps:

**1. Select [Options](#) > [Protocol Settings](#) > [Storage Essentials](#) > [System Application Discovery Settings](#).**

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, “No Targets Currently Selected,” change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

**2. Select a target, and then, click [Run Now](#).**

**3. In the Database Information table, click the  button, corresponding to the Sybase instance you do not want the management server to monitor.**

**4. Perform Discovery Data Collection to make the management server aware of your changes.**

## Monitoring Microsoft Exchange

To monitor Microsoft Exchange, you must make the management server aware of domain controller access. After information for controller access has been added, discover Microsoft Exchange and perform Discovery Data Collection. To save time, delay these steps until you have added the configurations for your other applications and hosts.

To monitor Microsoft Exchange, you must:

- Add information for Microsoft Exchange Domain Controller Access
- Discover the application.

## Adding Microsoft Exchange Domain Controller Access

To obtain information about your Microsoft Exchange servers, you must provide the user name and password for at least a primary domain controller, in addition to a DNS name, as described in the following steps.

---

**IMPORTANT:** The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as Microsoft Exchange.

---

To provide information about the Microsoft Exchange servers:

**1. Select [Options](#) > [Protocol Settings](#) > [Storage Essentials](#) > [Global Application Discovery Settings](#).**

The information you provide for the primary domain controller and backup domain controller apply to all Microsoft Exchange servers you discover.

2. In the Microsoft Exchange Configuration section, click the **Edit** button.
3. Under the Primary Domain Controller section, perform the following steps:
  - a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
  - b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
  - c. In the **Domain Password** field, type the corresponding password for accessing the Microsoft Exchange server.
  - d. In the **Verify Password** field, re-type the password for verification.
4. Under the Backup Domain Controller section, perform the following steps:
  - a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
  - b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
  - c. In the **Domain Password** field, type the corresponding password for accessing the domain controller.
  - d. In the **Verify Password** field, re-type the password for verification.
5. Click the **OK** button.


---

**IMPORTANT:** You must discover the host running Microsoft Exchange. See “[Step 3 - Discovering Applications](#)” on page 128.

---

## Deleting a Microsoft Exchange Domain Controller

To delete a Microsoft Exchange domain controller:

1. Select **Options > Protocol Settings > Storage Essentials > Global Application Discovery Settings**.
2. Click the  button, corresponding to the domain controller you want to remove.
3. Perform Discovery Data Collection (**Discovery > Details**) for your changes to take effect.

## Step 3 - Discovering Applications

This step assumes you have already discovered your hosts and provided discovery information for your applications. To discover an application, do the following;

- Detect the application (“[Step A - Detect the Applications](#)” on page 128)
- Discovery Data Collection (“[Step B - Obtain Details](#)” on page 128)

Keep in mind the following:

- This section assumes you have already set up the discovery configurations for your applications as described in “[Step 2 - Setting Up Discovery for Applications](#)” on page 115.
- Make sure you have reviewed the table, [Table 2](#) on page 1 to make sure you are at the correct step.
- If DNS records for your Microsoft Exchange servers are outdated or missing, the discovery of Microsoft Exchange may fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory



replication and Active Directory lookups may fail or contain errors if DNS records are not accurate.

- The management server is unable to discover Oracle on a Windows host if the host is on a private network behind a Windows proxy. The management server can discover the Windows host through the Windows proxy, but the management server is not able to detect Oracle.

## Step A - Detect the Applications

Use HP Systems Insight Manager to discover the applications. Refer to the HP Systems Insight Manager documentation.

## Step B - Obtain Details

Obtain detailed information from the discovered applications as described in this section.

Keep in mind the following:

- Discovery Data Collection takes some time. You might want to perform this process when the network and the managed elements are not busy.
- If you want to enable File SRM for a host, make sure the File SRM option is selected.
- When you do Discovery Data Collection that includes an AIX host, the system log displays three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port. You can ignore these errors.
- You can quarantine elements to exclude them from Discovery Data Collection. See ["Placing an Element in Quarantine"](#) on page 48 for more information. Let us assume you want to discover all the elements in a discovery group, except for one. Perhaps the element you want to quarantine is being taken off the network for maintenance. You can use the quarantine feature to exclude one or more elements from discovery.
- If the management server unable to obtain information from an element during Discovery Data Collection as a result of a CIM Extension hanging, the management server places the access point where the CIM Extension is located in quarantine. The management server then moves onto getting details for the next element in the Discovery Data Collection table. These elements appear as missing until they are removed from quarantine. See ["Removing an Element from Quarantine"](#) on page 49 for information on how to remove an element from quarantine.

To obtain details:

1. Select **Options > Storage Essentials > Discovery > Run Discovery Data Collection**.
2. Verify the **File SRM** option is selected. The File SRM option appears for hosts that have the CIM Extension and an operating system that supports File SRM.

---

**NOTE:** If you plan to have File SRM scan a host, make sure you have 220 to 230 MB for each set of 1 million files.

---

3. Select the discovery group from which you want to Discovery Data Collection. If you are obtaining Discovery Data Collection for hosts for the first time, make sure **All Discovery Groups** is selected.

You can use discovery groups to break up getting Discovery Data Collection. For example, instead of Discovery Data Collection for all of the elements, you could specify that the

management server gets the element details for only the elements in Discovery Group 1, thus, saving you time. You add an element to a discovery group by modifying the properties used to discover the element. See [“Modifying the Properties of a Discovered Address”](#) on page 39.

4. Click the **Get Details** button.

---

**IMPORTANT:** If the management server cannot communicate with an application, it labels the application as “Discovered”. The management server could find the application, but it could not obtain additional information about it.

---

5. Refer to the topic, “Adding a Discovery Schedule” in the User Guide for information about automating the gathering of Discovery Data Collection. If you run into problems with discovery, see [“Troubleshooting”](#) on page 157.

## Changing the Oracle TNS Listener Port


The software uses port 1521 by default to communicate with the TNS Listener service on the Oracle server. If your port is different or you use multiple ports, you can assign a new port number.

---

**IMPORTANT:** The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as the Oracle Transparent Name Substrate (TNS).

---

To change this port number or to add ports:

1. Select **Options > Protocol Settings > Storage Essentials > Global Application Discovery Settings**.
2. To assign a new port, click the **Create** for the **Oracle Information** table.
3. Type the new port number and click **OK**.
4. If necessary, click the  button to remove the old port number.
5. Verify all elements have been discovered by clicking the **Start Discovery** button.

See [“Troubleshooting Discovery and Discovery Data Collection”](#) on page 167 for more information.

## Adding/Modifying Microsoft Exchange Domain Controller Access

To obtain information about your Microsoft Exchange servers, you must provide the user name and password for at least a primary domain controller, in addition to a DNS name, as described in the following steps.

---

**IMPORTANT:** The hosts should recognize the management server by name, as a reverse look-up is required by operating system security as well as Microsoft Exchange.

---

To provide information about the Microsoft Exchange servers:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, "No Targets Currently Selected," change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

2. Select a target, and then, click **Run Now**.
3. In the Microsoft Exchange Configuration section, click the **Edit** button.
4. Under the **Primary Domain Controller** section, perform the following steps:
  - a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
  - b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
  - c. In the **Domain Password** field, type the corresponding password for accessing the Microsoft Exchange server.
  - d. In the **Verify Password** field, re-type the password for verification.
5. Under the **Backup Domain Controller** section, perform the following steps:
  - a. In the **Host Name** field, type the fully qualified DNS name for the domain controller.
  - b. In the **User Name** field, type the user name for accessing the Microsoft Exchange server.
  - c. In the **Domain Password** field, type the corresponding password for accessing the Microsoft Exchange server.
  - d. In the **Verify Password** field, retype the password for verification.
6. Click the **OK** button.
7. Verify all elements have been discovered by clicking the **Start Discovery** button.
8. Update the database with element changes. See "[Updating the Database with Element Changes](#)" on page 47.


See "[Troubleshooting Discovery and Discovery Data Collection](#)" on page 167 for more information.

## Deleting a Microsoft Exchange Domain Controller

To delete a Microsoft Exchange domain controller:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, "No Targets Currently Selected," change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

2. Select a target, and then, click **Run Now**.
3. Click the  button, corresponding to the domain controller you want to remove.

## Changing the Password for the Managed Database Account

The management server connects to database applications through the use of the APPIQ\_USER account, an unprivileged account with read-only privileges. You can change the password the management server uses to connect to database applications, such as Oracle and Sybase. When you change the password of APPIQ\_USER, you must change the password of all database applications.

Keep in mind the following:

- Change the password in all database applications before you change the password through the user interface. The passwords must also match.
- You must enter a password in the **Password** and **Verify Password** fields.

To change the password:

1. Select **Options > Protocol Settings > Storage Essentials > System Application Discovery Settings**.

To select a target, you must have at least one element designated as a server, workstation or desktop. If you see the message, “No Targets Currently Selected,” change your element from unknown to either a server, workstation or desktop. Refer to the documentation for HP Systems Insight Manager.

2. Select a target, and then, click **Run Now**.
3. Click the **Change Password** button at the top of the page.
4. Verify you have already changed the password of the databases listed on this page.
5. Type a new password in the **Password** field.

The management server requires the password to have the following characteristics:

- a minimum of three characters
  - starts with a letter
  - contains only letters, numbers and underscores (\_)
  - does not start or end with an underscore (\_)
6. Retype the password in the **Verify Password** field.
  7. Click **OK**.

## Obtaining Disk Drive Statistics from Engenio Storage Systems

---

**IMPORTANT:** Depending on your license, the ability to obtain disk drives statistics from Engenio storage systems may not be available. See the “List of Features” to determine if you have access to the additional statistics. The “List of Features” is accessible from the Documentation Center (**Help > Documentation Center** in Storage Essentials).

---

To obtain information about disk drive statistics from Engenio storage systems, you must install a CIM Extension on a host that can access the Engenio storage system. Ensure the proxy host has at least one LUN rendered by each controller of the array. Then, you must make the management server aware of that host, as described in the following steps:

1. Install the CIM Extension on a host that has access to the Engenio storage system.
2. Discover that host.
3. Select **Optimize > Storage Essentials > Performance Data Collection**.
4. Verify the **Data Collection** tab is displayed.
5. Click the **Start** button corresponding with the disk drive statistics for an Engenio storage system.
6. Set the date and time.
7. Type a repeat interval and then select a unit of measurement from the drop-down menu.  
The repeat interval determines how often the collectors gather the data.
8. Select a proxy host by clicking the **Browse** button.
9. Select a proxy host from the drop-down menu and then click **OK**.  
The management server displays in the drop-down menu only hosts that are running a CIM Extension version 3.5 or later and have access to the corresponding Engenio storage system.

---

**NOTE:** You can always change the proxy host by returning to this page or by going to the **Properties** tab for an Engenio storage system. Double-click the Engenio storage system in System Manager. Click the **Properties** tab. Then, click the **Browse** button on the Properties tab.

---

10. Saving the proxy host may take time. When you are asked if you want to continue, click **OK**.
11. Click **OK** again to set the time for starting the collector.
12. If you do not see any hosts displayed verify you have the latest CIM Extension installed and running on a host that can access the Engenio storage system.

## Assigning a File Extension in Netscape 7

Netscape 7 automatically assigns unknown files an HTML extension. To make Netscape 7 recognize the type of file, you must assign a file extension.

To assign a MIME type:

1. Click the download file link or button in the software.
2. Click the **Advanced** button in the lower-left corner.
3. In the **Description of type** field, delete the existing text and type a description of the file.
4. In the **File extension** field, delete the existing text and type the file extension.
5. Click **OK**.

The next time Netscape 7 sees the associated MIME type, it will assign the extension you typed in the **File Extension** field.

For example, in the following figure, the zip extension was assigned to a MIME type of application/unknown. The next time Netscape sees that MIME type, it will automatically assign the zip extension to the file.

6. Click **OK**.



---

## 13 Managing Security

---

**IMPORTANT:** Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help > Documentation Center** in Storage Essentials).

---

This chapter describes the following:

- “[Managing User Accounts](#)” on page 141
- “[Changing the Password of System Accounts](#)” on page 154
- “[Managing Roles](#)” on page 147
- “[Managing Organizations](#)” on page 149

### About the Security for the Management Server

The management server offers security based on roles and organizations. Role-based security determines access to certain functionality depending on the user account assigned to a role. Organizations determine if you can modify an element type, such as hosts. The management server ships with the Everything organization, which lets you modify all element types.

See the following topics for more information:

- “[About Roles](#)” on page 135
- “[About Organizations](#)” on page 138
- “[Planning Your Hierarchy](#)” on page 141
- “[Naming Organizations](#)” on page 141

### About Roles

The management server ships with several predefined roles that are listed in the following table. These roles determine which components of the software a user can access.

For example, users assigned to the Help Desk role have access to Application Viewer and Event Monitoring for Storage Essentials, but not to System Manager, Provisioning Manager, Policy Manager, and Reporting. Likewise, users assigned to the domain administrator role have access to all of the features, as shown in the following table.

**IMPORTANT:** Roles only apply to features and elements in HP Storage Essentials. For example, assume you assigned a user to the Help Desk role in Storage Essentials. That user will have “view only” privileges only in Storage Essentials.

**Table 7** Default Role Privileges

| Feature                                    | CIO<br>(Chief<br>Informa-tion<br>Officer) | Domain<br>Admini-<br>strator | Storage<br>Admini-<br>strator | Server<br>Admin-<br>istrator | Applic-<br>ation<br>Admin-<br>istrator | Help<br>Desk |
|--------------------------------------------|-------------------------------------------|------------------------------|-------------------------------|------------------------------|----------------------------------------|--------------|
| Application Viewer                         | X                                         | X                            |                               |                              | X                                      | X            |
| System Manager                             | X                                         | X                            | X                             | X                            | X                                      |              |
| Event Monitoring for<br>Storage Essentials |                                           | X                            | X                             | X                            | X                                      | X            |
| Provisioning<br>Manager                    |                                           | X                            | X                             |                              |                                        |              |
| Capacity Manager                           | X                                         | X                            | X                             | X                            | X                                      |              |
| Policy Manager                             |                                           | X                            | X                             |                              |                                        |              |
| Chargeback<br>Manager                      | X                                         | X                            | X                             |                              |                                        |              |
| Business Tools                             | X                                         | X                            | X                             |                              |                                        |              |
| Reporting                                  | X                                         | X                            | X                             | X                            | X                                      |              |
| Global Reporter                            | X                                         | X                            | X                             |                              |                                        |              |
| File System Viewer                         |                                           | X                            |                               | X                            |                                        |              |
| Performance<br>Manager                     | X                                         | X                            | X                             | X                            | X                                      |              |
| Access CLI                                 |                                           | X                            | X                             |                              |                                        |              |
| Custom Commands                            |                                           | X                            | X                             |                              |                                        |              |
| System<br>Configuration                    |                                           | X                            |                               |                              |                                        |              |

Keep in mind the following:

- Users created in HP Systems Insight Manager are automatically placed in the SIMViewOnly role. This role does not allow users to access any of the features listed in [Table 7](#) on page 136. See “[Adding Users](#)” on page 142 for more information.



- Users with access to Global Reporter can view all the elements throughout the enterprise, including those on the server running Global Reporter. Grant access to Global Reporter only to those, who should be allowed to view all elements. You may want to disable this functionality for some users.
- If the System Configuration option is selected for a role, all users assigned to that role will have administration capabilities, as shown in the following list. If you do not want users belonging to that role to have those capabilities, do not assign the System Configuration option:
  - The ability to set organizations and roles
  - Schedule discovery
  - Find the CIM log level
  - Save log files, e-mail log files
  - Save the database, backup the database, and schedule a database backup
  - Configure Event Monitoring for Storage Essentials, File System Viewer and Performance Manager
  - Configure reports and traps
  - Set up the management server to send e-mail

Roles also restrict access to element properties, element records, and Provisioning Manager, as shown in the following table.

**Table 8** Default Role Privileges with Elements

| <b>Role</b>               | <b>Application</b> | <b>Host</b>  | <b>Switch</b> | <b>Storage System</b> | <b>Tape Library</b> | <b>Others</b> |
|---------------------------|--------------------|--------------|---------------|-----------------------|---------------------|---------------|
| CIO                       | View               | View         | View          | View                  | View                | View          |
| Domain Administrator      | Full Control       | Full Control | Full Control  | Full Control          | Full Control        | Full Control  |
| Storage Administrator     | View               | View         | Full Control  | Full Control          | Full Control        | Full Control  |
| Server Administrator      | View               | Full Control | View          | View                  | View                | View          |
| Application Administrator | Full Control       | View         | View          | View                  | View                | View          |
| Help Desk                 | View               | View         | View          | View                  | View                | View          |
| SIMViewOnly               | View               | View         | View          | View                  | View                | View          |

By selecting one of the following options, users belonging to that role are restricted access:

- **Full Control** - Lets you view and modify the record for the element (Asset Management tab) and perform provisioning if applicable.
- **Element Control** - Lets you view and modify the record for the element (Asset Management tab). Provisioning cannot be performed.
- **View** - Lets you only view element properties.

For example, if a user belongs to a role that only lets you view the element properties on storage systems, that user would not be allowed to perform provisioning on storage systems because their role does not have the **Full Control** option selected for storage systems. That same role could also have the **Full Control** option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but the user would be able to provision switches.

You can modify roles and/or create new ones. For example, you can modify the Help Desk role so that the users assigned to this role can also view Reporting and modify servers.

## About Organizations

---

**IMPORTANT:** Organizations only apply to elements in HP Storage Essentials. For example, assume you assigned a user to an organization containing only hosts. That user will be able to view only hosts in Storage Essentials; however, that user may be able to view all other elements in HP Systems Insight Manager.

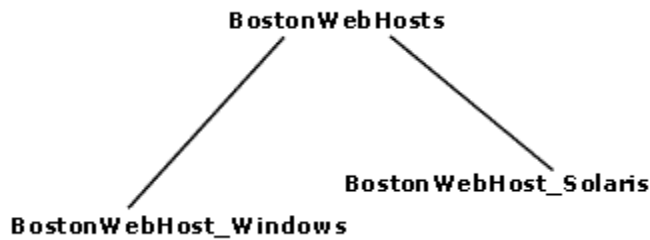
---

You can specify which elements users can access. For example, you can specify that some users have only access to certain switches and hosts. However, these users must already be assigned to roles that allow them to see switches and hosts.

Users only assigned to the organization can see just the elements that belong to the organization. If users are assigned to more than one organization, they see all elements that belong to the organizations to which they are assigned. For example, assume you created two organizations: One called OnlyHosts that allowed access to only hosts and another called OnlySwitches that allowed access to only switches. If you assigned a user to OnlyHosts and OnlySwitches, they would have access to hosts and switches because those elements are listed in at least one of the organizations.

Organizations can also contain other organizations. An organization contained within another is called a child. The organization containing a child organization is called a parent. In the following figure, the BostonWebHosts organization contains two child organizations,

BostonWebHost\_Windows and BostonWebHost\_Solaris. BostonWebHosts is a parent because it contains two organizations.



**Figure 2** Parent-Child Hierarchy for Organizations

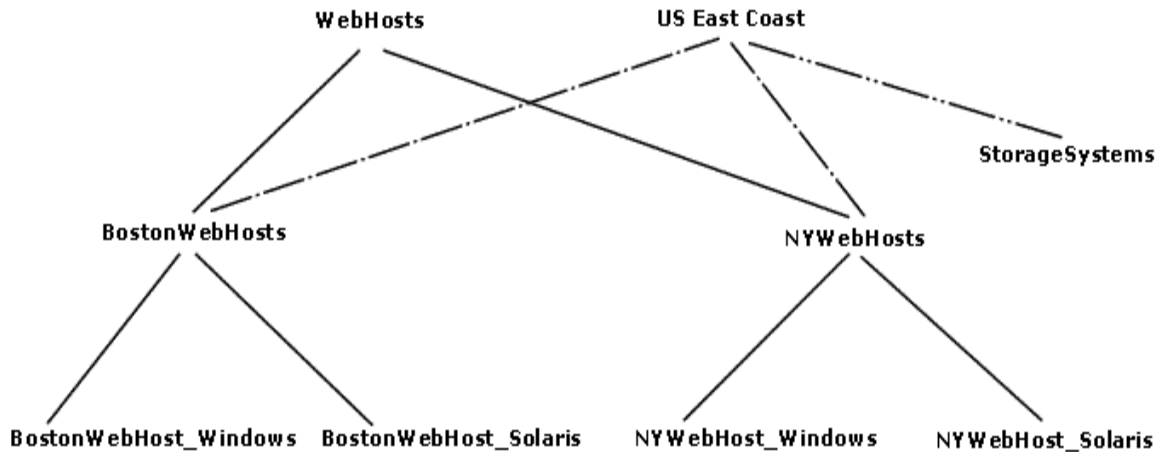
If a child contains organizations, it is also a parent. Let's assume you add two organizations called BostonWebMarketing and BostonWebProduction to BostonWebHost\_Windows. BostonWebHost\_Windows would become a parent because it now contains two organizations. It would also be a child because it is contained in BostonWebHosts.

Parent organizations allow access to all elements listed in their child organizations. For example, users assigned to the organization BostonWebHosts can access not only the elements in BostonWebHost\_Windows, but also those in BostonWebHost\_Solaris. This is because BostonWebHosts is a parent of the two child organizations.

The parent-child hierarchy for organizations saves you time when you add new elements. You need to add a new element only once. The change ripples through the hierarchy. For example, assume you add an element to BostonWebHost\_Windows. Users not only assigned to BostonWebHost\_Windows would see this addition, but also users assigned to any of the parent organizations containing BostonWebHost\_Windows. For example, users assigned to BostonWebHosts would also see the addition because it contains BostonWebHost\_Windows. Users, however, assigned to only BostonWebHost\_Solaris would not see the addition.

A child organization can be in multiple parent organizations. As shown in the following figure BostonWebHosts and NYWebHosts are not only children of the WebHosts organization, but they are also children of the US East Coast organization. Assume you have a user that oversees all Web hosts in the company, you could assign them to the WebHosts organization. Users managing hosts and storage systems on the east coast would be assigned to the US East Coast organization, which is a parent of BostonWebHosts, NYWebHosts, and StorageSystems organizations. Assume an element is added to NYWebHost\_Solaris, users assigned to one or more of the following organizations would see the addition:

- NYWebHost\_Solaris
- NYWebHosts
- WebHosts
- US East Coast



**Figure 3** Children in Multiple Organizations

When you remove an element from an organization, users belonging to that organization or to one of its parents can no longer access that element if it is not a member of any other organization. For example, assume an element named MyHost was not only a member of BostonWebHost\_Solaris, but also had mistakenly become a member of BostonWebHost\_Windows. If you remove MyHost from BostonWebHost\_Solaris, users belonging to BostonWebHost\_Solaris can no longer access the element. Users belonging to the following organizations would still see the element because the element is still a member of BostonWebHost\_Windows.

- BostonWebHosts
- WebHosts
- US East Coast

Keep in mind the following:

- You cannot edit the Everything organization.
- If you don't want users to have access to all elements, remove them from the Everything organization.
- Users can access information about all elements from security pages. For example, if a user is assigned to an organization that has access to only hosts, the user can still see information relating to storage systems on the security pages.
- Because generic elements cannot be placed into organizations, they do not appear unless the user belongs to the Everything organization. You can tell if an element is generic by double-clicking the element in System Manager and then clicking the Properties tab. Look for its description on this page. For example, if it is listed as "Generic Host" the element is a generic host.
- Discovery lists (**Discovery** tab) are not filtered. Users can see all elements in the discovery lists regardless of their affiliation with an organization.

- Reports only display elements assigned to the user's organization, including child organizations. For example, if you attempt to view a Host Summary report and you do not have permission to access hosts through your organization, you are not given information about the hosts in the report. This is also true for e-mailing reports. Let's assume again you do not have permission to access hosts. The reports you e-mail will not contain information about hosts, including the host specific reports. If the users receiving your reports want to be able to view information about hosts, one of the following must happen:
  - The hosts in question must be added to your organization.
  - Someone else, who has the hosts in question already in their organization, must send the reports.

---

**IMPORTANT:** When adding a child to an organization, do not add the organization's parent as a child. For example, assume you created an organization named Child1 that has a parent organization named Parent1. When you are adding child organizations to Child1, do not select Parent1, as this creates a loop.

---

## Planning Your Hierarchy

Before you begin creating organizations, plan your hierarchy. Do you want the hierarchy to be based on location, departments, hardware, software or tasks? Perhaps you want a combination of these options.

To help you with your task, create a table of users who manage elements on the network and the elements they must access to do their job. You might start seeing groups of users who oversee the same or similar elements. This table may help you in assigning users to the appropriate organizations.

Once you are done with planning your hierarchy, draw the hierarchy in an graphics illustration program, so you can keep track of which organizations are parents and children.

Create the child organizations first, then their parents. See the topic, "[Adding an Organization](#)" on page 149 for more information.

## Naming Organizations

When you create an organization, give it a name that reflects its members. For example, you might want to use one or more of the following as a guideline:

- Type of elements that are members of the organization, such as switches, Sun Solaris hosts
- Location of the elements, such as San Jose
- Task, such as backup machines

You may find that it is easy to forget which containers are parents and children. When you name an organization, you might want to include a portion of the name of the dominant parent organization. For example, assume you have two types of Web hosts in Boston: Microsoft Windows and Sun Solaris. You might name the two children organizations BostonWebHost\_Windows and BostonWebHost\_Solaris and their parent, BostonWebHosts.

# Managing User Accounts

This section discusses the following topics:

- “Adding Users” on page 142
- “Editing a User Account” on page 143
- “Deleting Users” on page 144
- “Modifying Your User Profile” on page 144
- “Modifying Your User Preferences” on page 144
- “Viewing the Properties of a Role” on page 146
- “Viewing the Properties of an Organization” on page 146

## Adding Users

To access the management server, users must enter a user name and password.

---

**NOTE:** The user name and password should be alpha-numeric. They cannot exceed more than 256 characters. The user name cannot begin with a number.

---

You must create your user account in HP Insight Manager SIM, as described in the following steps:

1. Select **Options > Security > Users and Authorizations**.
2. Click the User tab.
3. Click **New**.
4. Provide the following information:
  - **Login name** - Provide a user name.
  - **Domain** - Provide the domain name of the server running Storage Essentials.

You do not need to provide additional information. For more information about the other options mentioned on this page, access the documentation accompanying HP SIM.

5. Click **OK**.


The new user is created.

---

**IMPORTANT:** New users can view the toolbars for Storage Essentials and not have enough privileges to use its features. You must grant users privileges so they can use not only view the features in the toolbar, but use them as well.

---

6. To authorize a user to use the features in Storage Essentials:
  - a. Click **New**.
  - b. In the **New Authorizations** table, select the user.
  - c. Select **Manually assign toolbox and system/system group authorizations**.
  - d. In the **Selected Toolbox(es)** section, select **HP SE Tools**.


- e. In the **Select Systems** list box, select the systems you want the user to be able to manage. Select CMS (Central Management Server) if you want to access information about the server running HP Systems Insight Manager.
  - f. Click **OK**.
7. You must restart Storage Essentials.
- When Storage Essentials restarts, it contacts HP Systems Insight Manager for information about accounts that have been added or removed.
8. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
9. In the upper-right corner, select **Security > Users**.
- Notice that the users you created in HP Systems Insight Manager are put in the SIMViewOnly Role. This role does not allow them to access any of the features in Storage Essentials.
10. To enable users access to features in Storage Essentials, assign the user to a different role by doing the following:
- a. Click the **Edit** button () corresponding to the user account you want to modify.
  - b. To change the role assign the user account, select a new role from the **Role** drop-down menu.  
If you don't find any roles that fit your needs, you can create a new one, as described in "[Adding Roles](#)" on page 147.
  - c. Click **OK**.

## Editing a User Account

Keep in mind the following:

- The "admin" account acts differently than the other accounts. You cannot add or remove organizations from the "admin" account. You cannot remove the Everything organization from the "admin" account. New organizations are automatically added to the "admin" account when they are created.
- This change takes effect immediately, even if the user is logged into the management server.

To modify a user account:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Users**.
3. Click the **Edit** button () corresponding to the user account you want to modify.
4. To change the account name, type a new name for the user account in the **Name** field, for example: jsmith  
This name becomes the user name for the account.
5. To change the name assigned to the user account, type a new full name for the account in the **Full Name** field.  
This information is used to provide a correlation between an account name and a user.

6. To change the role assigned to the user account, select a new role from the **Role** drop-down menu.
7. To change the e-mail address listed, type a new e-mail address in the **E-mail** field.
8. To change the phone number listed, type the user's new phone number in the **Phone** field.
9. Change or remove information from the **Notes** field if necessary.
10. To change the organizations to which the user belongs, select or deselect the organizations from the table in the user interface.  
The Everything organization is the default organization that lets users access all current and future elements.
11. Click **OK**.

## Deleting Users

---

**IMPORTANT:** You cannot delete the admin account.

---

To delete a user account:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Users**.
3. Click the corresponding **Delete** button (🗑️).  
The user account is deleted.

## Modifying Your User Profile

While you are logged into the management server, you can change the following aspects of your user profile:

- Full Name
- E-mail address
- Phone number

However, you are not allowed to modify the following information:

- Login Name
- Role
- Organization affiliation

If you want this information modified, contact your domain administrator. Your domain administrator makes these changes in the **Configuration** menu.

To modify your user profile, do the following:

1. Click the name of your account in the upper-left corner.



**Figure 4** Changing Your User Profile



2. On the **User Profile** tab, modify one or more of the following:
  - **Full Name**
  - **E-mail address**
  - **Phone number**
3. When you are done with your modifications, click the **Save Changes** button.

## Modifying Your User Preferences

Use the **User Preference** tab to modify your user preferences for System Manager, Element Topology, and Event Monitoring for Storage Essentials. The **User Preference** tab controls what is displayed for your user account.

To access the **User Preferences** tab:

1. Click the name of your account in the upper-left corner of Storage Essentials.



**Figure 5** Accessing the User Preferences Tab

2. Click the **User Preferences** tab.

## System Manager and Element Topology Preferences

To change the severity icons you view in System Manager and in the element topology, select a severity level from the **Display Severity icons with this severity level or higher drop-down** menu.

If you want events refreshed within a time period, select the **Refresh events automatically** field. Then, enter in minutes how often you want the event information on the screen updated. If this option is set to every five minutes, the management server refreshes the severity icons displayed in System Manager and the element topology every five minutes.

## Event Monitoring for Storage Essentials Preferences

Use the following table as a guideline for changing your user preferences for Event Monitoring for Storage Essentials.

**Table 9** Changing User Preferences for Event Monitoring for Storage Essentials

| If you want...                              | Do the following...                                                                                                 |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| To be reminded whenever you change a filter | Select the option, <b>Always remind me to apply filters when I change them.</b>                                     |
| Events refreshed automatically              | Select the option, <b>Refresh events automatically.</b> Then, enter how often in minutes you want events refreshed. |

**Table 9** Changing User Preferences for Event Monitoring for Storage Essentials (continued)

| If you want...                                     | Do the following...                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change the number of events displayed on each page | Select the number of events to appear on a page from the <b>Number of Events</b> combo box.                                                                                                                                                                                                                 |
| Change the severities to be included               | <p>Select a severity level you want displayed in Event Monitoring for Storage Essentials from the <b>Severities to be Included</b> drop-down menu.</p> <p>If you want to customize the filter for the severity levels, click the <b>Custom</b> button.</p>                                                  |
| Change the element types to be included            | <p>Select the element types you want to be included from the <b>Element types to be included</b> drop-down menu. Events from these elements are displayed in Event Monitoring for Storage Essentials.</p> <p>If you want to customize the filter for the element types, click the <b>Custom</b> button.</p> |

## Warnings for Slow Systems Operations

By default, the management server warns you when it encounters issues with handling large amounts of data from storage systems, such as long load times.

If you do not want to be warned, clear the **Warn about slow storage system operations** option on the **User Preferences** tab. See ["Modifying Your User Preferences"](#) on page 144 for information on how to access the **User Preferences** tab.

## Viewing the Properties of a Role

You can quickly determine which components a user can access by viewing the properties of the user's role.

To view the properties of a role:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Users**.
  1. Click **Security > Users**.
  2. In the **Role** column, click the name of the role.

This page displays the following information:

- **Role Name** - The name of the role. This name appears in the users table (**Security > Users**)
- **Role Description** - A description of the role.
- **Access Level** - Determines how much access the user has to a type of element, such as hosts, storage systems, switches, and applications. See ["About the Security for the Management Server"](#) on page 135 for more information.

- **Access to the Storage Authority Components** - Determines which components in the management server the user can access.

To learn how to edit a role, see the topic, "[Editing Roles](#)" on page 148.

## Viewing the Properties of an Organization

You can quickly determine which elements a user can access by viewing the properties of the user's organization:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Users**.
3. In the **Organization** column, click the name of a organization.
4. To determine which elements are in a child organization, click the link of the child organization.
5. To learn more about an element, click the element's link.

This page displays the following information:

- **Name** - The name of the organization. This name appears in the users table (**Security > Users**)
- **Description** - A description of the organization
- **Organization Members** - Determines which elements the user can access. See "[About the Security for the Management Server](#)" on page 135 for more information.

To learn how to edit an organization, see the topic, "[Editing Organizations](#)" on page 151.

## Managing Roles

This section discusses the following topics:

- "[Adding Roles](#)" on page 147
- "[Editing Roles](#)" on page 148
- "[Deleting Roles](#)" on page 149

## Adding Roles

The management server ships with several roles. You can add roles to accommodate your organization. For example, you might want to add a role for quality assurance. See the topic, "[About the Security for the Management Server](#)" on page 135 for more information about roles and organizations.

---

**IMPORTANT:** The **Role Name** and **Description** fields do not accept special characters, except spaces and the following characters: \$, -, ^, ., and \_

---

To add a role:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Roles**.
3. Click the **New Role** button.
4. In the **Role Name** field, type a name for the role. For example: Quality Assurance.  
The name can contain spaces, but it cannot be longer than 256 characters.
5. In the **Description** field, type a description for the role. For example: Role for those in quality assurance.  
You cannot type more than 1024 characters in the **Description** field.
6. Select an access level for each element type:
  - **Full Control** - Lets you view and modify the record for the element (Asset Management tab) and perform provisioning.
  - **Element Control** - Lets you view and modify the record for the element (Asset Management tab).
  - **View** - Lets you view element properties.

For example, if a user belongs to a role that only lets you view the element properties on storage systems, that user would not be allowed to perform provisioning on storage systems because their role does not have the **Full Control** option selected for storage systems. That same role could also have the **Full Control** option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but the user would be able to provision switches.
7. Select the features you want a user to be able to access. For example, if you want a user to have access to System Manager, select System Manager from the list.  
See "[Management Server Components](#)" on page 7 for more information about these features.
8. Click **OK**.

## Editing Roles


The software lets you modify the default roles and/or the roles you have created. See the topic, "[About the Security for the Management Server](#)" on page 135 for more information about roles and organizations.

Keep in mind the following:

- You cannot edit the domain admin role.
- After you click the **OK** button in the Edit Role window, any users assigned to the role you edited are logged out of the management server. Users see the changes when they log back into the management server.
- The **Role Name** and **Description** fields do not accept special characters, except spaces and the following characters: \$, -, ^, ., and \_

To edit a role:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.

2. In the upper-right corner, select **Security > Roles**.
3. Click the **Edit** button ()
4. To edit the name of the role, change the name in the **Role Name** field.  
The name can contain spaces, but it cannot be longer than 256 characters.
5. To edit the description of the role, change the description in the **Description** field.  
You cannot type more than 1024 characters in the **Description** field.
6. To change the access level, change the options selected in the table.
  - **Full Control** - Lets you view and modify the record for the element (Asset Management tab) and perform provisioning.
  - **Element Control** - Lets you view and modify the record for the element (Asset Management tab).
  - **View** - Lets you view element properties.

For example, if a user belongs to a role that only lets you view the element properties on storage systems, that user would not be allowed to perform provisioning on storage systems because their role does not have the **Full Control** option selected for storage systems. That same role could also have the **Full Control** option selected for switches, allowing the user to perform provisioning for switches. Thus, the user would not be able to provision storage systems, but the user would be able to provision switches.
7. Select the features you want a user to be able to access. For example, if you want a user to have access to System Manager, select System Manager from the list.  
See "[Management Server Components](#)" on page 7 for more information about these features.
8. Click **OK**.


## Deleting Roles

---

**IMPORTANT:** A role cannot be deleted if it contains a user.

---

To delete a role:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Roles**.
3. Click **Roles** from the drop-down menu.
4. Click the corresponding **Delete** button ()  
The role is deleted.

## Managing Organizations

This section discusses the following topics:

- "[Adding an Organization](#)" on page 149
- "[Viewing Organizations](#)" on page 150

- ["Editing Organizations"](#) on page 151
- ["Deleting an Organization"](#) on page 152
- ["Removing Members from an Organization"](#) on page 152
- ["Filtering Organizations"](#) on page 153

## Adding an Organization

You can create new organizations to restrict access to certain elements. For example, assume you do not want the help desk to have access to elements belonging to a certain group. You could create an organization that does not allow access to those elements. Once you assign users to that organization, they would only be able to access the elements you specified.

See the topic, ["About the Security for the Management Server"](#) on page 135 for more information about roles and organizations.

Keep in mind the following:

- You cannot add organizations to any user with the Domain Administrator role, which has access to all organizations by default.
- Create child organizations first, then their parents.
- When adding a child to an organization, do not add the organization's parent as a child. For example, assume you created an organization named Child1, which is contained in a parent organization named Parent1. When you are adding child organizations to Child1, do not select Parent1, as this creates a loop.
- All discovered elements are accessible in Business Tools, regardless of a user's restrictions. For example, assume your account belongs to an organization that has only hosts as members. If you run the business tool Switch Risk Analysis, the management server still provides information about whether the switches are a risk in your environment.

To add an organization:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Roles**.
3. Click the **New Organizations** button.
4. In the **Name** field, type a name for the organization.  
The organization name can contain spaces, but it cannot be longer than 256 characters and it cannot contain the caret ( ^ ) symbol.
5. In the **Description** field, type a description for the organization.  
You cannot type more than 1024 characters in the **Description** field.
6. Click the **Add or Remove Members** button to determine which elements the user will see.
7. To add elements, expand the Elements node in the tree. Then, do at least one of the following:
  - **Select all elements of a certain type** - Just select the node for that element type. For example, you can select all the hosts by just clicking the Hosts node in the left pane. The elements in that category appear in the Organization Members pane.



- **Select individual elements** - Expand the Elements node. Then, expand the node for the element type, for example the Applications node. Select the elements you want to add to the organization. The selected elements appear in the Organization Members pane.
8. To add organizations, do one of the following:
    - **Select all organizations** - Select the Organizations (top-level node). The selected organizations appear in the Organization Members pane.
    - **Select individual organizations** - Expand the Organizations node. Then, select the organization. The selected organization appears in the Organization Members pane.

The organizations in the Organization Members pane are listed as child organizations because they are now contained within the organization you are creating. See the topic, "[About the Security for the Management Server](#)" on page 135 for more information.
  9. Once you are done adding elements, click **OK** in the Add or Remove Organization Members window.
  10. Once you are done adding the organization, click **OK** in the Add Organization window.

## Viewing Organizations

The Setup Organizations page lists the organizations and their descriptions, in addition to the number of elements, users and child organizations assigned to each organization.

The number of elements field provides the total number of elements assigned to an organization, not including those within the child organization. An organization containing only child organizations displays 0 under the No. of Elements column; however, users assigned to that organization would have access to the elements assigned to its child organizations.

| New Organization |                                                     |                 |                     |              |                                                                                       |                                                                                       |
|------------------|-----------------------------------------------------|-----------------|---------------------|--------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Name             | Description                                         | No. of Elements | Child Organizations | No. of Users | Edit                                                                                  | Delete                                                                                |
| Everything       | The default organization that includes all elements | 106             |                     | 2            |                                                                                       |                                                                                       |
| Boston_Hosts     |                                                     | 3               |                     | 0            |  |  |

**Figure 6** Viewing Organizations

Access the Setup Organizations page by clicking **Security > Organizations** in Storage Essentials. You can access information about child organizations by clicking their link under the Child Organization column.

## Editing Organizations


See the topic, "[About the Security for the Management Server](#)" on page 135 for more information about roles and organizations.

When elements are removed from an organization, users belonging only to that organization are no longer able to access the removed elements.

Keep in mind the following:

- Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help > Documentation Center** in Storage Essentials).
- The **Name** and **Description** fields in the Edit Organization window do not accept special characters, except spaces and the following characters: \$, -, ^, ., and \_
- The organization name can contain spaces, but it cannot be longer than 256 characters.
- You cannot edit the Everything organization.
- When adding a child to an organization, do not add the organization's parent as a child. For example, assume you created an organization named Child1, which is contained in a parent organization named Parent1. When you are adding child organizations to Child1, do not select Parent1, as this creates a loop.

To edit an organization:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Roles**.
3. Click the  button.
4. To change the name of the organization, type a new name in the **Name** field.  
The organization name can contain spaces, but it cannot be longer than 256 characters and it cannot contain the caret ( ^ ) symbol.
5. To change the description of the organization, type a new description in the **Description** field.  
You cannot type more than 1024 characters in the **Description** field.
6. Click the **Add or Remove Elements** button.
7. Add and remove elements as described in the topics, “[Adding an Organization](#)” on page 149 and “[Removing Members from an Organization](#)” on page 152.
8. Once you are done adding or removing elements, click **OK** in the Add Organization page.
9. In the Edit Organization page, click **OK**.

## Deleting an Organization

When an organization is removed, users assigned only to that organization are no longer able to access the elements in the removed organization. For example, assume you belong to two organizations, onlyHosts and onlySwitchesandHosts. The organization onlyHosts contains only hosts, and the organization onlySwitchesandHosts contains only switches and hosts. If you delete the onlySwitchesandHosts organization, you will still have access to hosts because you still belong to the onlyHosts organization.


Keep in mind the following:

- You cannot remove the Everything organization, which is the default organization.
- You can only remove organizations with no users.



Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help > Documentation Center** in Storage Essentials).

To delete an organization:

1. Click **Security > Organizations**.
2. Click the  button corresponding to the organization you want to remove.  
The software removes the organization.

## Removing Members from an Organization


When you remove an element from an organization, users belonging to that organization or to one of its parents can no longer access that element if it is not a member of any other organization. For example, assume an element named MyHost was not only a member of BostonWebHost\_Solaris, but also had mistakenly become a member of BostonWebHost\_Windows. If you remove MyHost from BostonWebHost\_Solaris, users belonging to BostonWebHost\_Solaris can no longer access the element. Users belonging to the BostonWebHost\_Windows organization or to its parent would still see the element.

---

**IMPORTANT:** Depending on your license, role-based security may not be available. See the “List of Features” to determine if you have access to role-based security. The “List of Features” is accessible from the Documentation Center (**Help > Documentation Center** in Storage Essentials).



---

Use one of the following methods to remove an element from an organization:

- In the Edit Organization window, click the  button corresponding to the element or child organization you want to remove from the organization.
- In the Add or Remove Organization Members window, select the element or child organization you want to remove in the right pane and then click the **Remove from Organization** button.  
Use this method if you want to add and remove elements from an organization.

## Accessing the Edit Organization Window

To access the Add Organization window

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Roles**.
3. Click the **Edit** () button corresponding with the organization you want to edit.
4. In the Edit Organization window, click the  button corresponding to the element or child organization you want to remove from the organization.

## Accessing the Add Elements to Organization Window

To access the Add Elements to Organization window:

1. Access Storage Essentials through one of the menu options, such as **Options > Storage Essentials > Email Settings**.
2. In the upper-right corner, select **Security > Roles**.
3. Click the **Edit** (✎) button corresponding with the organization you want to edit.
4. In the Edit Organization window, click the **Add or Remove Members** button.
5. Select the elements and/or organizations you want to remove in the right panel and then click the **Remove from Organization** button.
6. Click **OK**.



## Filtering Organizations

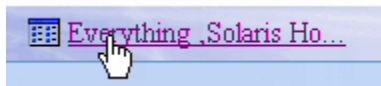
The management server provides a filtering feature that lets you designate which organizations are active in your view. For example, assume you belong to an organization name Hosts and this organization contains two organizations: "Windows Hosts" and "Solaris Hosts." If you want to view elements only in "Windows Hosts" and not in "Solaris Hosts" organizations, you could use the filtering feature to activate only the "Windows Hosts" organization.

Keep in mind the following:

- If you do not want to view an element, deselect all child organizations containing the element. You must also deselect all parent organizations containing the child organization that has that element. For example, assume you do not want to view all Solaris hosts and all Solaris hosts are in the "Solaris Hosts" organization. The "Solaris Hosts" organization is contained in the Hosts organization. You must deselect the "Solaris Hosts" organization and the Hosts organization if you do not want to see Solaris hosts.
- Users belonging to the Everything organization see all organizations on the management server in the Filtering Organizations window.
- If you do not select any organizations for filtering, you do not see any elements in the topology.

To filter organizations:

1. Access Storage Essentials through one of the menu options, such as **Tools > Storage Essentials > System Manager**.
2. In Storage Essentials, click the  button at the top of the screen, or click the link listing the organizations you can view.
1. Click the  button at the top of the screen, or click the link listing the organizations you can view.



**Figure 7** Clicking the Organization Link

2. Deselect the organizations containing the elements you do not want to obtain information about. Assume you want to view only the elements in the "Windows Hosts" organization, you would select only "Windows Hosts." Let's assume you have a parent organization named "Hosts" that contains "Solaris Hosts" and "Windows Hosts." You would need to deselect

“Solaris Hosts” and “Hosts.” “Hosts” would need to be deselected because it contains organizations other than “Windows Hosts.”

Links are displays for the organizations if you belong to a role that has System Configuration capability. To learn more about the contents of an organization, click its link.

3. Click **OK**.

You can now only obtain information about elements in the active organizations. The active organizations are listed in the link next to the filter button, as shown in the following figure.



**Figure 8** Active Organization

## Changing the Password of System Accounts

The management server uses the following accounts to access and manage the database for the management server. You should change the passwords to these accounts to prevent unauthorized access.

- **SYS** - Used for the management server database creation and upgrade. Default password: `change_on_install`
- **SYSTEM** - Used for management server database creation and upgrade, in addition to database import, export and re-initialization. Default password: `manager`
- **RMAN\_USER** - Used for RMAN backup and restore. This user has sys privilege. Default password: `backup`
- **DB\_SYSTEM\_USER** - Used for all the database activity, including establishing a connection to the management server database. Default password: `password`

You must change the passwords of the SYS, SYSTEM, RMAN\_USER, and DB\_SYSTEM\_USER accounts by using the `dbadmin.bat` tool, so the management server is aware of the changes. The passwords must also follow the following guidelines. Do not change the password for one of these accounts by using Oracle. Make sure you keep the new passwords in a safe location, as it is your responsibility to remember the Oracle passwords.

The management server requires the password to have the following characteristics:

- a minimum of three characters
- starts with a letter
- contains only letters, numbers and underscores (`_`)
- does not start or end with an underscore (`_`)

To make the management server aware of the new password:

1. Stop the AppStorManager service.
2. To access the database utility on Windows, go to the `[Install_Dir]\Tools` directory on the management server and double-click `dbAdmin.bat`, where `[Install_Dir]` is the directory into which you installed the management server.
3. Click **Change Passwords** in the left pane.
4. Select an account name from the **User Name** combo box.
5. Type the current password in the **Old Password** field.

6. Type the new password in the **New Password** field.
7. Retype the password in the **Confirm Password** field.
8. Click **Change**.  
The Database Admin Utility changes the password for the specified account.

---

## 14 Troubleshooting

This chapter describes the following:

- [“Data is late or an error occurred” Message](#) on page 157
- [“appiq.log Filled with Connection Exceptions”](#) on page 157
- [“Receiving “HTTP ERROR: 503” When Accessing the Management Server”](#) on page 158
- [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159
- [“Configuring UNIX CIM Extensions to Run Behind Firewalls”](#) on page 160
- [“Volume Names from Ambiguous Automounts Are Not Displayed”](#) on page 164
- [“Installing the Software Security Certificate”](#) on page 165
- [“Troubleshooting Discovery and Discovery Data Collection”](#) on page 167
- [“Troubleshooting Hardware”](#) on page 177

### “Data is late or an error occurred” Message

If you see the message “Data is late or an error occurred” when you tried to obtain information from a UNIX host, verify you were logged in as root when you started the CIM Extension (`./start`). You must be logged in as root if you want to use the `./start` command, even if you are using the

`./start -users username` command, where `username` is a valid UNIX account.

The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. This is why you must use root to start the CIM Extension. Only root has enough privileges to provide the information the management server needs.

If you continue to see the message, contact customer support.

### appiq.log Filled with Connection Exceptions

When an Oracle REDO log becomes corrupt, the management server is unable to connect to the database. Whenever the management server is unable to connect to the Oracle database, it writes to the `appiq.log` file. Many exceptions may cause the Application Log on Windows to become full.

To fix the problem, stop the management server and Oracle. Then, remove the corrupted REDO log, as described in the following steps:

1. Stop the AppStorManager service, which is the service the management server uses.

---

**NOTE:** While the service is stopped, the management server cannot monitor elements and users cannot access the management server.

---

2. To find the corrupt log file, look in the `alert_APPIQ.log` file, which can be found in `\oracle\admin\APPIQ\bdump`, where `ORACLE_BASE` is `c:\oracle`

You can verify if the REDO log listed in the alert\_APPIQ.log file is corrupt by looking for a “redo block corruption” error in the REDO log.

3. On the management server, enter the following at the command prompt:

```
Sqlplus /nolog
```

4. Enter the following:

```
Sql> connect sys/change_on_install as sysdba
```

5. Enter the following:

```
Sql> startup mount;
```

6. Enter the following:

```
Sql> ALTER DATABASE CLEAR UNARCHIVED LOGFILE
'C:\ORACLE\ORADATA\APPIQ\REDO02.LOG';
```

where C:\ORACLE\ORADATA\APPIQ\REDO02.LOG is the corrupted log file and its path.

7. Enter the following:

```
Sql> alter database open
```

8. Enter the following:

```
Sql> shutdown immediate;
```

9. Enter the following:

```
Sql> startup
```

## Receiving “HTTP ERROR: 503” When Accessing the Management Server

If you receive a message resembling the following when you try to access the management server, make sure your database for the management server is running. If it is not, start the database.

```
Receiving HTTP ERROR: 503 javax.ejb.EJBException: null;
```

Refer to the following sections for more information about how to start database for the management server.

Access the Services window to make sure the OracleOraHome92TNSListener service has started and is set to automatic. Refer to the Windows documentation for information on how to access the Services window.

If the OracleOraHome92TNSListener service has not started but the AppStorManager service has started, start the OracleOraHome92TNSListener service and then restart AppStorManager.

---

**IMPORTANT:** If you are starting the services manually, start the Oracle service before the service for the management server.

---

## Errors in the Logs

If you access the logs, you are shown messages resembling the following. The complete text has been shortened as a result of space constraints:

```
Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Creating
[Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Created
[Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Starting
[Aug 04 2004 11:59:07] INFO
[com.appiq.service.policyManager.policyService.PolicyService] Starting
Policy Factory
[Aug 04 2004 11:59:11] ERROR [com.appiq.security.DatabaseSecurityManager]
DatabaseSecurityManager Error:
org.jboss.util.NestedSQLException: Could not create connection; - nested
throwable: (java.sql.SQLException: ORA-01033: ORACLE initialization or
shutdown in progress
); - nested throwable: (org.jboss.resource.ResourceException: Could not
create connection; - nested throwable: (java.sql.SQLException: ORA-01033:
ORACLE initialization or shutdown in progress
))
```

## Permanently Changing the Port a CIM Extension Uses (UNIX Only)

CIM Extensions on UNIX use port 4673 by default. You can start a CIM Extension on another port by entering `./start -port 1234`, where 1234 is the new port. With this method, you must always remember to provide the nondefault port when starting the CIM Extension.

You can configure a CIM Extension to remember the nondefault port, so you only need to enter `./start` to start the CIM Extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. In this directory, create a file called `cxws.host.parameters`.
3. Open the newly created file in a text editor, and provide the following line:

```
-credentials username:password
-port 1234
```

---

**IMPORTANT:** The values for `-credentials` and `-port` must be on separate lines, as shown in the example.

---

where

- `username` is the user that is used to discover the CIM Extension. You will need to provide this user name and its password when you discover the host.

- password is the password of username.
  - 1234 the new port for the CIM Extension
4. Save the file.
  5. Restart the CIM Extension for your changes to take effect.

---

**NOTE:** The CIM Extension looks for parameters in the `cxws.host.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

---

6. The management server assumes the CIM Extension is running on port 4673. If you change the port number, you must make the management server aware of the new port number. In the IP Address/DNS Name field, type a colon and then the port number after the IP address or DNS name, as shown in the following example:

```
192.168.1.2:1234
```

where

- 192.168.1.2 is the IP address of the host
- 1234 is the new port number

If you have already added the host to the discovery list on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

## Configuring UNIX CIM Extensions to Run Behind Firewalls

In some instances you will need to discover a host behind a firewall. Use the following table as a guideline. Assume the management server wants to discover HostA, which has three network interface cards on three separate networks with three separate IPs: 10.250.250.10, 172.31.250.10, and 192.168.250.10. In the following table different configurations are presented:

- The “Manual Start Parameters for CIM Extensions” column provides what you would enter to start the CIM Extension manually on the host. See the Installation Guide for more information on how to start a CIM Extension manually.
- The “If Mentioned in `cxws.host.parameters`” column provides information on how you would modify the `cxws.host.parameters` file. See [“Permanently Changing the Port a CIM Extension Uses \(UNIX Only\)”](#) on page 159.
- The “Step 1 Discovery and RMI Registry Port” column - Provides information about what IP addresses are required for the discovery list. The RMI Registry port is the port the CIM Extension uses. Keep in mind that when a port other than 4673 is used for the CIM Extension, the port must be included in the discovery IP. For example, 192.168.1.1:1234, where 192.168.1.1 is the IP for the host and 1234 is the port the CIM Extension uses.



**Table 10** Troubleshooting Firewalls

| <b>Config-<br/>uration</b>                                                               | <b>Manual Start<br/>Parameters<br/>for CIM Extension</b> | <b>If Mentioned in<br/>cxws.host.parameters</b> | <b>Step 1<br/>Discovery<br/>and<br/>RMI Registry<br/>Port</b>                                         |
|------------------------------------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Firewall port 4673 opened between host and management server                             | start                                                    |                                                 | 10.250.250.10 OR<br>172.31.250.10 OR<br>192.168.250.10<br><br>Communication Port: 4673                |
| Firewall port 1234 opened between host and management server, but specific port          | start -port 1234                                         | -port 1234                                      | 10.250.250.10:1234 OR<br>172.31.250.10:1234 OR<br>192.168.250.10:1234<br><br>Communication Port: 1234 |
| Firewall port 4673 opened between host and management server on the 172.31.250.x subnet  | start -on 172.31.250.10                                  | -on 172.31.250.10                               | 172.31.250.10<br><br>Communication Port: 4673                                                         |
| Firewall port 1234 opened between host and management server on the 192.168.250.x subnet | start -on 192.168.250.10:1234                            | -on 172.31.250.10:1234                          | 172.31.250.10:1234<br><br>Communication Port: 1234                                                    |

**Table 10** Troubleshooting Firewalls (continued)

| Configuration                                                                                                                                                                                 | Manual Start Parameters for CIM Extension                                                    | If Mentioned in cxws.host.parameters                                                  | Step 1 Discovery and RMI Registry Port                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <p>With 3 firewall ports opened on different ports respectively 1234, 5678, 9012.</p>                                                                                                         | <p>start -on 10.250.250.10:1234<br/>-on 172.31.250.10: 5678<br/>-on 192.168.250.10: 9012</p> | <p>-on 10.250.250.10:1234<br/>-on 172.31.250.10:5678<br/>-on 192.168.250.10: 9012</p> | <p>10.250.250.10:1234 OR<br/>172.31.250.10:5678 OR<br/>192.168.250.10:9012</p> <p>Communication Port:<br/>1234, 5678, 9012</p> |
| <p>With firewall port 4673 opened between host and management server. NAT environment where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches other side of the firewall</p> | <p>start</p>                                                                                 |                                                                                       | <p>172.16.10.10</p> <p>Communication Port:<br/>17001</p>                                                                       |

**Table 10** Troubleshooting Firewalls (continued)

| Configuration                                                                                                                                                                            | Manual Start Parameters for CIM Extension                                         | If Mentioned in cxws.host.parameters                                                                                   | Step 1 Discovery and RMI Registry Port                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| With firewall port 1234 opened between a host and management server. NAT environment where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches other side of the firewall | start -port 1234                                                                  | -port 1234                                                                                                             | 172.16.10.10<br>Communication Port:<br>17001                                                                                    |
| With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. NAT environment where all 3 NICs are translated to different 172.16.x.x subnets                           | start -on 10.250.250.10:1234<br>-on 172.31.250.10:5678<br>-on 192.168.250.10:9012 | -on 10.250.250.10:1234<br>-on 172.31.250.10:5678<br>-on 192.168.250.10:9012                                            | 172.16.10.10:<br>1234 OR<br>172.16.20.20:<br>5678 OR<br>172.16.30.30:<br>9012<br><br>Communication Port:<br>1234, 5678,<br>9012 |
| False DNS or IP is slow to resolve                                                                                                                                                       |                                                                                   | jboss.properties, stop and restart service<br>cimom.Dcxws.agency.firstwait=200000<br>cimom.Dcxws.agency.timeout=200000 | Any IP that is reachable<br><br>Communication Port: 4673                                                                        |

**Table 10** Troubleshooting Firewalls (continued)

| Configuration                                                                                                                                                 | Manual Start Parameters for CIM Extension                                                                        | If Mentioned in cxws.host.parameters                                                                                   | Step 1 Discovery and RMI Registry Port                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No DNS, never resolve                                                                                                                                         |                                                                                                                  | jboss.properties, stop and restart service<br>cimom.Dcxws.agency.firstwait=200000<br>cimom.Dcxws.agency.timeout=200000 | Any IP that is reachable<br><br>Communication Port: 4673                                                                                                                             |
| No firewall. Don't want to use root credentials. Want to discover with a non-existent user.                                                                   | start -credentials abcuser:passwd                                                                                | -credentials abcuser:passwd                                                                                            | Specify abcuser and password in the discovery list.<br><br>Communication Port: 4673                                                                                                  |
| With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. Don't want to use root credentials. Want to discover with a non-existent user. | start<br>-on10.250.250.10:1234<br>-on172.31.250.10:5678<br>-on192.168.250.10:9012<br>-credentials abcuser:passwd | -on10.250.250.10:1234<br>-on172.31.250.10:5678<br>-on192.168.250.10:9012<br>-credentials abcuser:passwd                | 10.250.250.10:1234 OR<br>172.31.250.10:5678 OR<br>192.168.250.10:9012.<br>Then, specify abcuser and passwd in the discovery list.<br><br>Communication Port:<br><br>1234, 5678, 9012 |

## Volume Names from Ambiguous Automounts Are Not Displayed

Volume names from ambiguous automounts on Solaris hosts are not displayed on the Storage Volumes page and in Capacity Manager. Some Solaris hosts have autofs and NFS mounted through an automounter. The management server cannot display volume names from ambiguous

automounts because it cannot determine if the comma separate strings that are part of the mounted volume name are host names or part of the name of a remote volume.

The following example is a comma separate string that is part of a mounted volume name. The management server cannot tell whether `test` and `three` are host names or part of the name of a remote volume. As a result, the management server does not display the volume name.

```
VolumeName = two:/ntlocal2,two:/comma,test,three,one:/ntlocal
```

## Installing the Software Security Certificate

To stop receiving a Security Alert message each time you use the HTTPS logon, install the software security certificate, as described in the following steps.

---

**IMPORTANT:** Enter the DNS name of the computer in the URL instead of localhost. If you use `https://localhost` to access the management server, you are shown a “Hostname Mismatch” error.

---

## Installing the Certificate by Using Microsoft Explorer 6.0

1. Access the management server by typing the following:  
`https://machinename`  
where `machinename` is the name of the management server.
2. When the security alert message appears, click **OK**.  
If you do not want the Web browser to warn you about a secure connection at any Web site, select the **In the future, do not show this warning** option.
3. When you are told there is a problem with the site's security certificate, click the **View Certificate** button.
4. When you are shown the certificate information, click the **Install Certificate** button at the bottom of the screen.
5. When you are shown the Certificate Import Wizard, click **Next** to continue the installation process.
6. Select one of the following:
  - **Automatically select the certificate store based on the type of certificate** - This option places the certificate automatically in the appropriate location.
  - **Place all certificates in the following store** - This option lets you pick the store where the certificate will be stored.
7. Click **Finish**.
8. When you are asked if you want to install the certificate, click **Yes**.  
You are shown the following message when the certificate is installed.

## Installing the Certificate by Using Netscape Navigator 7

1. Access the management server by typing the following:  
`https://machinename`  
where `machinename` is the name of the management server.
2. When the security alert message appears, click the **Always** button.
3. When you are told you are requesting an encrypted page, click **OK**.
4. Click the **Always** button when you are asked if you want to accept the certificate.
5. When asked if you wanted to trust the signed applet, click the **Always** button.

## Changing the Security Certificate to Match the Name of the Server

If your users are shown a Security Alert window with the following message, you might want to modify the security certificate so users feel more comfortable with installing the certificate:

“The name of the security certificate is invalid or does not match the name of the site.”

You can change the security certificate so that users receive the following message instead:

“The security certificate has a valid name matching the name of the page you are trying to view.”

When you change the certificate, you must use the `generateAppiqKeystore.bat` program to delete the original certificate. Then, use the `generateAppiqKeystore.bat` program to create a new certificate and to copy the new certificate to the management server.

To change the certificate:

1. Go to the `[Install_Dir]\Tools` directory, where `[Install_Dir]` is the directory into which you installed the management server.
2. To delete the original certificate, enter the following at the command prompt:  
`C:\[Install_Dir]\Tools> generateAppiqKeystore.bat del`  
The original certificate is deleted.
3. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:  
`C:\[Install_Dir]\Tools> generateAppiqKeystore.bat`
4. If the program is unable to detect a DNS name, enter the following at the command prompt:  
`C:\[Install_Dir]\Tools> generateAppiqKeystore.bat mycomputername`  
where `mycomputername` is the DNS name of the computer
5. To copy the new certificate to the management server, enter the following at the command prompt:  
`C:\[Install_Dir]\Tools> generateAppiqKeystore.bat copy`  
The new certificate is copied to the correct location.

# Troubleshooting Discovery and Discovery Data Collection

This section describes the following:

- ["Configuring E-mail Notification for Discovery Data Collection"](#) on page 167
- ["Increasing the Time-out Period and Number of Retries for Switches"](#) on page 168
- [""Connection to the Database Server Failed" Error"](#) on page 170
- ["DCOM Unable to Communicate with Computer"](#) on page 170
- ["Duplicate Listings for Brocade Switches in Same Fabric"](#) on page 170
- ["Element Logs Authentication Errors During Discovery"](#) on page 171
- ["EMC Device Masking Database Does Not Appear in Topology \(AIX Only\)"](#) on page 171
- ["Microsoft Exchange Drive Shown as a Local Drive"](#) on page 171
- ["Unable to Discover Microsoft Exchange Servers"](#) on page 171
- ["Nonexistent Oracle Instance Is Displayed"](#) on page 171
- ["Requirements for Discovering Oracle"](#) on page 171
- ["Unable to Find Elements on the Network"](#) on page 172
- ["Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration"](#) on page 172
- ["A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly"](#) on page 172
- ["Unable to Monitor McDATA Switches"](#) on page 172
- ["Unable to Detect a Host Bus Adapter"](#) on page 173
- ["Navigation Tab Displays Removed Drives as Disk Drives"](#) on page 173
- ["Unable to Obtain Information from a CLARiiON Storage System"](#) on page 173
- ["Discovery Fails Too Slowly for a Nonexistent IP Address"](#) on page 173
- [""CIM\\_ERR\\_FAILED" Message"](#) on page 174
- ["Communicating with HiCommand Device Manager Over SSL"](#) on page 175
- ["Unable to Discover a UNIX Host Because of DNS or Routing Issues"](#) on page 176

## Configuring E-mail Notification for Discovery Data Collection

The management server lets you send status reports about Discovery Data Collection to users. The status reports that are sent to users can also be found in the `GAEDSummary.log` file in the `[Install_DIR]\logs` directory on the management server.

To configure the management server to send status reports on Discovery Data Collection to your e-mail account:

1. Enable e-mail notification for the management server. Refer to the User Guide for more information.
2. Add or edit the e-mail address for the Admin account.

The status reports for Discovery Data Collection automatically go the e-mail account provided for the Admin user. To add or edit an e-mail address for the Admin account, log in as Admin and then follow the steps in “[Modifying Your User Profile](#)” on page 144.

3. If you want additional users to receive the status reports for Discovery Data Collection, do the following:
  - a. Click **Options** > **Storage Essentials** > **Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
  - b. Click **Show Default Properties** at the bottom of the page.
  - c. Copy the `gaedemail` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
  - d. Return to the Advanced page (**Options** > **Storage Essentials** > **Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
  - e. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
  - f. Assign the e-mail accounts you want to receive the report to the `gaedemail` property. For example, if you want `user1@appiq.com` and `user2@appiq.com` to receive these status reports, modify the `gaedemail` property in the **Custom Properties** field as follows:  
`gaedemail=user1@appiq.com;user2@appiq.com`

---

**NOTE:** Make sure the hash (#) symbol is removed from the `gaedmail` property.

---

- g. When you are done, click **Save**.
- h. Restart the service for the management server for your changes to take effect.

## Increasing the Time-out Period and Number of Retries for Switches

If you are having difficulty obtaining information from your switches during Discovery Data Collection, you may need to increase the time-out period and the number of retries. By default, the management server gives a switches five seconds to respond to its requests for information during Discovery Data Collection. If the switch does not respond the first time, the management server tries again. The management server says it cannot contact the switch if it does not receive a response from the switch a second time.

To change the time-out period and number of retries for switches, modify the properties specified [Table 11](#) on page 169 and [Table 12](#) on page 169 as described in the following steps:

1. Access the management server.
2. Select **Options** > **Storage Essentials** > **Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.



4. Copy the commands specified in [Table 11](#) on page 169. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
5. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
6. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
7. Make sure the property is not commented out by removing the hash (#) symbol in front of the property. To modify the time-out period, set the corresponding property for your switch in the following table to the number of millisecond you want. The default is 5000 ms. For example, to change the time-out period to 30000 ms for a McDATA switch, you would set the `cimom.McData.Snmp.Timeout` property to 30000, as shown in the following example:

```
cimom.McData.Snmp.Timeout=30000
```

**Table 11** Time-out Properties

| Switch                                                                                                                                       | Property                               |
|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| McDATA/Connectrix<br>discovered through SNMP                                                                                                 | <code>cimom.McData.Snmp.Timeout</code> |
| Cisco                                                                                                                                        | <code>cimom.Cisco.Snmp.Timeout</code>  |
| Other switches discovered<br>through SNMP: <ul style="list-style-type: none"> <li>• CNT</li> <li>• Sun StorEdge</li> <li>• QLogic</li> </ul> | <code>cimom.snmp.switch.timeout</code> |

8. To modify the number of retries, repeat Steps 4 through 6 by copying and pasting the property specified in [Table 12](#) on page 169. Set the corresponding property for your switch in the following table to the number of retries you want. The default is two retries. For example, to change the number of retries to five for a McDATA switch, set the `cimom.McData.Snmp.Retries` properties as shown in the following example:

```
cimom.McData.Snmp.Retries=5
```

**Table 12** Retry Properties

| Switch                                       | Property                               |
|----------------------------------------------|----------------------------------------|
| McDATA/Connectrix<br>discovered through SNMP | <code>cimom.McData.Snmp.Retries</code> |
| Cisco                                        | <code>cimom.Cisco.Snmp.Retries</code>  |

**Table 12** Retry Properties (continued)

| Switch                                                                                                                                | Property                               |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Other switches discovered through SNMP: <ul style="list-style-type: none"><li>• CNT</li><li>• Sun StorEdge</li><li>• QLogic</li></ul> | <code>cimom.snmp.switch.retries</code> |

9. When you are done, click **Save**.

10. Restart the service for the management server for your changes to take effect.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

## “Connection to the Database Server Failed” Error

If you received an error message resembling the following after getting all element details, verify that the database instance is running:

```
The connection to the database server failed. Check that the Oracle instance 'OIQ3 on host '192.168.1.162:1521 is running correctly and has the management software for Oracle installed correctly.
```

Assume you received the error message listed above. You would want to verify the following:

- Oracle instance OIQ3 on host 192.168.1.162 port 1521 is running.
- The management software for Oracle is installed on the server running the Oracle instance. One of the installation's tasks is to create an APPIQ\_USER user account with enough privileges for the software to view statistics from the database.

Once you have verified the items listed above, run “Discovery Data Collection” again. If you continue to see the error message, contact customer support.

## DCOM Unable to Communicate with Computer

Sometimes the following error message appears in the event log of the management server when the software is monitoring a Brocade switch:

```
DCOM was unable to communicate with the computer 192.168.10.21 using any of the configured protocols
```

where 192.168.10.21 is the IP address of the Brocade switch.

Ignore this error message.

## Duplicate Listings for Brocade Switches in Same Fabric

If you discover more than one Brocade switch in the same fabric, the **Targets** tab displays duplicate listings for the Brocade switches. Each Brocade switch is listed multiple times with the IP address of the other switches and its own.

For example, assume you discovered Brocade switches QBrocade2 and QBrocade5 in the same fabric, the switches are listed twice on the **Targets** tab. QBrocade2 is listed twice, once with its own IP address, the other time with the IP address of QBrocade5, as shown below:

```
192.168.10.22 Switch QBrocade2, QBrocade5 admin
192.168.10.25 Switch QBrocade2, QBrocade5 admin
```

## Element Logs Authentication Errors During Discovery

During discovery, you may see SNMP authentication errors on the element you are trying to discover. The management server is probing the element with an SNMP request. If the element does not know the management server, it logs authentication errors.

## EMC Device Masking Database Does Not Appear in Topology (AIX Only)

An EMC device masking database attached to an AIX host does not appear in the Topology tree under the **Application Path - Unmounted** node on the **Topology** tab in System Manager.

If the EMC device masking database is attached to a host running Microsoft Windows or Sun Solaris, the masking database appears under the **Application Path - Unmounted** node.

## Microsoft Exchange Drive Shown as a Local Drive

Microsoft Exchange Servers have a drive M. The software displays this drive as a local fixed disk, instead of a Microsoft Exchange Server special drive.

## Unable to Discover Microsoft Exchange Servers

If DNS records for your Microsoft Exchange servers are outdated or missing, the discovery of Microsoft Exchange may fail because Microsoft Exchange is dependant on Active Directory, which is dependant on DNS. Since Active Directory is dependant on DNS, Active Directory replication and Active Directory lookups may fail or contain errors if DNS records are not accurate.

## Nonexistent Oracle Instance Is Displayed

The software uses the Oracle Transparent Name Substrate (TNS) listener port to detect Oracle instances on a server. Sometimes an Oracle instance is removed from the server, but not from the TNS listener port. This results in the software detecting the nonexistent Oracle instance and displaying it in the topology. Refer to Oracle documentation for information on how to remove the deleted Oracle instance from the TNS listener port.

## Requirements for Discovering Oracle

To discover Oracle:

- The management software for Oracle must be installed. For information about installing the management software for Oracle, refer to the *Installation Guide*.
- By default, the software sets the TNS Listener Port to 1521. If you use another port, you can change the port number on the Discovery Targets tab.
- Oracle discovery relies on the TNS networking substrate on which Oracle is built (TNS is Oracle's proprietary protocol). The software does not use TNS listener password. If you have

set a TNS Listener password, the software is not able to discover the Oracle instances serviced by the listener.

## Unable to Find Elements on the Network

The management server uses ping to find the devices on the network enabled for IP. Ping is a program that lets you verify that a particular IP address exists. Ping is not guaranteed to return a response from all devices. If Discovery is not able to find a device automatically, enter the IP address for the device on the Discovery Targets tab, which can be accessed by clicking the Discovery button at the top of the screen in the management server. Sometimes ping cannot find the device if one of the following conditions occur:

- Network configuration does not support ping, including data center security (firewalls).
- Device has the ping responder turned off.
- Device does not support ping.

## Device Locking Mechanism for Brocade Element Manager Query/Reconfiguration

Please keep in mind that the configuration for Brocade switches is locked while getting all details for elements in a zones. The software ensures that each CIM query locks out any reconfiguration. For example, if you are getting details for elements in all zones, you cannot add a new Brocade switch while your doing it (the discovery or configuration process waits until the collection of details is finished before proceeding). However, simultaneous CIM queries do not lock each other out.

## A Discovered Sun StorEdge A5000 JBOD Does Not Display Its WWN Properly

Although full monitoring and management support is available only to those devices for which there is a provider, the software's topology displays other devices found on your storage area network (SAN) to give you a more complete view. However, because these devices do not have a provider, only basic information is returned. In some cases, as with the Sun StorEdge A5000 JBOD (Just a Bunch of Disks), the Worldwide Name (WWN) presented and reported to the management server may be different from the official WWN of the device, as the management server reports the WWN of the port connected to the fabric.

## Unable to Monitor McDATA Switches

McDATA switches use the Fibre Channel Switch Application Programming Interface (SWAPI) to communicate with devices on the network. The McDATA switches allow only one SWAPI connection at a time. For example, if the management server discovers the IP address of the McDATA switch, other management servers and third-party software are not able to communicate with the switch using SWAPI.

Use Enterprise Fabric Connectivity (EFC) Manager to communicate with the McDATA switch. EFC Manager versions 7.0 and later can communicate with the management server and the switch. This configuration lets multiple instances of the management server or other clients contact EFC Manager, which in turn provides information about the switch. To communicate with the EFC Manager, first install the Bridge Agent. Then, enter the IP address of the server running EFC Manager in the Discovery pane. The user name and password must be for EFC Manager, and the

user name and password are case sensitive. Refer to your McDATA representative for more information about the Bridge Agent and EFC Manager.

---

**IMPORTANT:** EFC Manager uses the SWAPI connection, preventing other third-party software from contacting the switch.

---

## Unable to Detect a Host Bus Adapter

The software is unable to detect a host bus adapter if you install its driver before you have completed installing the Solaris operating system for the first time. For example, you installed the HBA drives too early when you used JumpStart to install Solaris. The best way to install the HBA driver is to install it after Solaris has been installed and is running.

## Navigation Tab Displays Removed Drives as Disk Drives

If you remove an internal disk from a Solaris host and do not enter the `cfgadm` command, the Navigation tab displays the empty slot as `DiskDrives_XXXXX` after getting element details. The `cfgadmn` command makes the software realize the drive has been removed. Refer to the documentation that shipped with the Solaris operating system for more information about the `cfgadm` command.

## Unable to Obtain Information from a CLARiiON Storage System

If you are having difficulty obtaining topology information or element details from a CLARiiON storage system, the NaviCLI might have timed out as a result of the service processor being under a heavy load. The management server uses the NaviCLI to communicate with the CLARiiON storage system. This situation has been seen in the field when the service processor is running more than 35,000 IOPS (IOs/Sec).

Try obtaining Discovery Data Collection from a CLARiiON storage system when the service processor is not under such a heavy load.

## Discovery Fails Too Slowly for a Nonexistent IP Address

If you enter a nonexistent IP address, the management server times out by default after 20 seconds on Windows and after three minutes. If you want to shorten the time-out period, modify the `cimom.CimXmlClientHttpConnectTimeout` property as described in this section.

---

**NOTE:** The management server does not accept a period longer than its default setting. If you set `cimom.CimXmlClientHttpConnectTimeout` property to more than 20 seconds on Windows, the management server ignores the values of this property and reverts back to the default settings.

---

To modify the default time-out:

1. Access the management server.
2. Click **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.

4. Copy the `cimom.CimXmlClientHttpConnectTimeout` property you want to modify. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
5. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
6. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
7. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
8. To modify the time-out period, set the `cimom.CimXmlClientHttpConnectTimeout` property to the number of millisecond you want. For example, to change the time-out period to 200 ms, set the `cimom.CimXmlClientHttpConnectTimeout` property, as shown in the following example:

```
cimom.CimXmlClientHttpConnectTimeout=200
```
9. When you are done, click **Save**.
10. Restart the service for the management server for your changes to take effect.  
While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

## “CIM\_ERR\_FAILED” Message

If you are in a McDATA environment where the EFC Manager Service Processor is managing multiple switches, it is possible that the management server will send SWAPI requests faster than the EFC Manager Service Processor can handle them. The management server may detect this as a failed connection and take corrective action. When this happens, you are shown a “CIM\_ERR\_FAILED” message whenever the management server tried to access the McDATA switches and directors.

The management server then attempts to reconnect to the EFCM by creating a new SWAPI connection. EFCM versions 8.x and later have five SWAPI connections available. EFCM versions 7.1.3 and later but before version 8.x have three SWAPI connections available. If the management server reconnects successfully, a reconnect event is generated and no further action is necessary.

If the management server cannot reconnect to the EFCM, another event is generated with a severity of major. If this happens, any operation the management server is performing (Discovery Data Collection) involving switches on that EFCM fails.

To prevent the “CIM\_ERR\_FAILED” messages, increase the delay between the management server’s SWAPI calls to EFCM, as described in the following steps:

1. Click **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.

3. Copy `cimom.mcData.swapIThrottle=200`. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field by changing the value of `cimom.mcData.swapIThrottle`. For example, the default is 200 milliseconds. To change the value to 800 milliseconds, change the xxx value to 800, as shown in the following example:

```
cimom.mcData.swapIThrottle=800
```

---

**NOTE:** If you want no delay, change the value to 0 for 0 milliseconds. The maximum delay you can have is 1,000 milliseconds (`cimom.mcData.swapIThrottle=1000`),

---

7. When you are done, click **Save**.
8. Restart the service for the management server for your changes to take effect. While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

## Communicating with HiCommand Device Manager Over SSL

By default the management server communicates with HiCommand Device Manager through a nonsecure connection. You can configure the management server so that it communicates with HiCommand Device Manager over a secure socket layer (SSL) connection by doing one of the following:

- **Use HTTPS in the discovery address** - Prepend `https://` to the discovery address to force the connection to HTTPS mode, for example, `https://192.168.1.1`, where 192.168.1.1 is the IP address of the host running HiCommand Device Manager. Use this option if you have one HiCommand Device Manager you want to communicate through a secure connection (SSL) and another you want to communicate through a nonsecure connection.
- **Modify an internal property** - Change the value of the `cimom.provider.hds.useSecureConnection` to `true`, as described in the steps in this section. Use this option if you want all connections to HiCommand Device Manager to be secure (SSL).

To set all connections with HiCommand Device Manager to SSL:

1. Click **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.

3. Copy the `cimom.provider.hds.useSecureConnection` property. How you copy the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, select the text and then right-click the selected text. Then, select **Copy**.
4. Return to the Advanced page (**Options > Storage Essentials > Manage Product Health**). Then, click **Advanced** in the Disk Space tree).
5. Paste the copied text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.
6. Make your changes in the **Custom Properties** field. Make sure the property is not commented out by removing the hash (#) symbol in front of the property.
7. Change the value assigned to the `cimom.provider.hds.useSecureConnection` property to true, as shown in the following example:
 

```
cimom.provider.hds.useSecureConnection=true
```
8. When you are done, click **Save**.
 

If you want to connect to another instance of HiCommand Device Manager by using a nonsecure connection, prepend `http://` to the discovery address to force the connection to nonsecure mode, for example, `http://192.168.1.1`, where 192.168.1.1 is the IP address of the host running HiCommand Device Manager.
9. Restart the service for the management server for your changes to take effect.
 

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

**Important:** While the AppStorManager service is stopped, the following occurs:

- Users are not be able to access the management server.
- The management server is unable to monitor elements at this time.

## Unable to Discover a UNIX Host Because of DNS or Routing Issues

If the management server is unable to discover a UNIX host because of a DNS or routing issues, you will need increase the amount of time that passes before the management server times out for that CIM Extension. By default, the management server waits 1,000 ms before it times out. It is recommended you increasing the time before the management server times out to 200000 ms (3.33 minutes), as described in the following steps. If you continue to see time out issues, you can still increase the time before the management server times out, but keep in mind that it will lengthen discovery.

To increase the time out period:

1. Select **Options > Storage Essentials > Manage Product Health**. Then, click **Advanced** in the Disk Space tree in the management server.
2. Paste the following text into the **Custom Properties** field. How you paste the text depends on your Web browser. If you are using Microsoft Explorer or Netscape Navigator, right-click the field and select **Paste**.

```
cimom.cxws.agency.firstwait=200000
cimom.cxws.agency.timeout=200000
where
```



- `cimom.cxws.agency.firstwait` - The `firstwait` property controls the amount of time required for the management server to wait after it first contacts the CIM Extension on the host before the management server attempts to proceed with a username and password. The default value is 1,000 ms. You are modifying it to wait 20,000 ms or 3.33 minutes.
- `cimom.cxws.agency.timeout` - The `timeout` property controls the allowable interval of silence before either the CIM Extension or the management server start to question whether its partner is still alive. If an entity (management server or extension) has not received a message from the other during the interval set by the `timeout` property, it will send an “are you there” message. If that message is not acknowledged during the interval set by the `timeout` property, the entity will conclude that the connection is no longer functioning. The CIM Extension will stop attempting to make a connection. When this occurs on the side of the management server, the management server will attempt to re-connect (and it will keep re-attempting until the host becomes available). The default value is 1,000 ms. You are modifying it to wait 20,000 ms or 3.33 minutes.

3. Click **Save**.

4. Restart the service for the management server for your changes to take effect.

While AppStorManager is restarting, users are not able to access the management server. The AppStorManager service must be running for the management server to monitor elements.

## Troubleshooting Hardware

This section describes the following:

- [“About Swapping Host Bus Adapters”](#) on page 177
- [““Fork Function Failed” Message on AIX Hosts”](#) on page 177
- [“Known Driver Issues”](#) on page 177
- [“Known Device Issues”](#) on page 178
- [““mailbox command 17 failure status FFF7” Message”](#) on page 181
- [““Process Has an Exclusive Lock” Message”](#) on page 181

### About Swapping Host Bus Adapters

Swapping brands of host bus adapters (HBA) on a Microsoft Windows 2000 host may have undesirable side effects. For example, after swapping out one brand of an HBA for another (including driver installation), `WinMgmt.exe` might crash repeatedly and appear to be associated with an error in the Windows Event Log about being unable to retrieve data from the `PerfLib` subkey in the Registry. To solve this problem, reinstall the operating system.

### “Fork Function Failed” Message on AIX Hosts

If a CIM Extension running on AIX detects low physical or virtual memory while starting, a “Fork Function Failed” message appears. A CIM Extension on AIX uses additional memory and CPU resources at start time. If the resources on the AIX machine is already low, you may see the “Fork Function Failed” message. Depending on the AIX operating system or hardware, the host may crash after you see this message.

## Known Driver Issues

If you are having problems with a driver, keep in mind the following:

- The software requires the driver to have a compliant SNIA HBA API. Emulex driver version 4.21e does not support the SNIA HBA API.
- If the driver has a compliant SNIA HBA API, make sure the driver is installed correctly.

## Known Device Issues

The following table provides a description of the known device issues. You can find the latest information about device issues in the release notes.

**Table 13** Known Device Issues

| Device                               | Software | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIX host                             | NA       | <p>If you are receiving replication errors for an AIX host, the provider may be trying to connect to the host using the 0.0.0.0 IP address instead of the real host IP address. If this situation is occurring, you would see a message containing the following when you start the CIM Extension:</p> <pre>CXWS 3.1.0.144 on 0.0.0.0/0.0.0.0 now accepting connections</pre> <p>To fix this situation, add the following line to the <code>/opt/APPQcime/tools/start</code> file on the AIX host:</p> <pre>export NSORDER=local,bind</pre> |
| AIX host using an IBM Storage System | NA       | <p>If you have an AIX host using an IBM storage system, not all bindings may be displayed on the bindings page on the Navigation tab. For example, assume diskA on host123 has six paths. All six bindings may not be displayed.</p>                                                                                                                                                                                                                                                                                                        |

**Table 13** Known Device Issues (continued)

| Device                                          | Software                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosts running SGI IRIX version 6.5.22 or 6.5.24 | NA                                                 | If a host running SGI IRIX version 6.5.22 or 6.5.24, the HBA port page on the Navigation tab in System Manager displays 0 GB/s for HBA ports.                                                                                                                                                                                                                                                                                                      |
| SGI IRIX host                                   | CXFS file systems                                  | The management server can only monitor CXFS file systems from the host generating the input/output. For example, assume the elements are part of a CXFS file system. When you generate input/out into the metadata server into /folder, only the metadata server is able to monitor the file system. For example, assume the metadata server generates 100 KB write, the management server displays 0 KB write for /folder on the metadata client. |
| Solaris host                                    | Sun SAN Foundation Suite driver (Leadville driver) | The bindings page reports a SCSI number that comes from the HBA API. This number cannot be seen by the user. For example SCSI target 267008 does not correlate to anything.                                                                                                                                                                                                                                                                        |
| Solaris host                                    | HDLM                                               | If you sync the Solaris host by itself without the switches and storage, the storage volume page reports all drive types as local.<br><br>Once you discover the host with the switches and storage, it reports its drives as being external. It was the same result with Active-Active and Active-Standby.                                                                                                                                         |
| Solaris host                                    | HDLM                                               | Solaris HDLM disks cannot be monitored. If you try monitoring them, the management server displays a message saying "data is late or an error occurred."                                                                                                                                                                                                                                                                                           |

**Table 13** Known Device Issues (continued)

| Device       | Software | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Solaris host | HDLM     | <p>Do a Discovery Data Collection for the host by itself. In the bindings page, the controller number are displayed as c-1. For example c-1t0d58.</p> <p>Perform Discovery Data Collection on the host with storage and switches. The controller numbers are displayed correctly.</p>                                                                                                                                                                                                                                                                                                              |
| Solaris host | VxVM     | <p>If you discover a host with any typical SAN disk groups off line, the storage volume page shows SAN mount points as local instead of external. These disks, however, are not accessible.</p> <p>When you perform Discovery Data Collection with all disk groups online, disks on the SAN are shown as external. Hosts connected directly to a storage system are shown as local, except for hosts connected by fibre. Hosts connected directly to a storage system through fibre are shown as external.</p>                                                                                     |
| Windows host | VxVM     | <p>When a Windows host with VxVM is used, the SCSI bus number is always reported to be one in the SCSI bus column of the Disk Drives page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Any host     | NA       | <p>The Unmounted Volume field under Capacity Summary automatically displays 0 MB if you discovered the host but not the storage system connected to it. This may occur if you did not enter the IP address of the storage system when performing discovery and/or your license does not allow you to discover a particular storage system. See the Supported Elements section in the "List of Features" to determine which storage systems you can discover. The "List of Features" is accessible from the Documentation Center (<b>Help &gt; Documentation Center</b> in Storage Essentials).</p> |

**Table 13** Known Device Issues (continued)

| Device              | Software                                                 | Description                                                                                                                                                                                                   |
|---------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IBM Storage Systems | Subsystem Device Driver (SDD) or MPIO (Multi Pathing IO) | If you discover an IBM storage system without SDD, incorrect stitching is displayed in System Manager for the storage system. You are shown only one path if the storage system is using MPIO instead of SDD. |

### “mailbox command 17 failure status FFF7” Message

If one or more of your Microsoft Windows hosts are using an Emulex HBA driver, you may see the following message in Windows Event Viewer:

“mailbox command 17 failure status FFF7”

This message can be safely ignored. The HBA API is being used to access data in the FLASH memory of the adapter that does not exist and this is causing the event to be logged. This issue has been seen with version 5.2.2 of the driver.

### “Process Has an Exclusive Lock” Message

You will receive a message resembling the one shown below if a process has already locked the EMC Symmetrix storage system and you attempt a process that requires a lock on the Symmetrix storage system. The Symmetrix storage system can become locked for many reasons. For example, the storage system becomes locked when it performs LUN mapping, LUN masking or Discovery Data Collection. The Symmetrix storage system may also remain locked after a provisioning operation has failed.

“SYMAPI routine SymDevMaskSessionStart failed with error code 188: The operation failed because another process has an exclusive lock on the local Symmetrix.”

After the management server has detected the lock on the Symmetrix storage system, it tries to access the storage system for 15 minutes and logs the errors.

If you receive the error message, determine if someone is performing an operation that requires a lock, such as LUN mapping, LUN masking or Discovery Data Collection. This also applies even if one of the processes is being used by a third-party product, such as for LUN masking. If so, wait until the process is complete. Only manually remove the lock if you are certain that no other processes are occurring on the storage system. To learn how to remove the lock, refer to the documentation for the Symmetrix storage system.

If a provisioning failure has caused the Symmetrix storage system to remain locked, you are alerted to this situation in Event Monitoring for Storage Essentials and on the Properties tab. You may receive a message resembling the following:

```
Unable to end device masking session. Symmetrix '000001835005700' may be
locked.
```

# Index

## A

### about

- AIX CIM Extension 51
- Altix CIM Extension 61
- HP-UX CIM Extension 69
- IRIX CIM Extension 79
- management server 1
- security 135
- Solaris CIM Extension 95
- Windows CIM Extension 105

### accessing

- domain controller 115

### account

- password 143

### accounts

- users 142

### Active Directory 171

### adding

- domain controller 115, 130
- elements 150, 151
- IP range 17
- organizations 150
- roles 147
- switches 46
- TNS Listener Port 130
- user accounts 142

### AIX 171

### AIX CIM Extension

- installing 51
- prerequisites 51
- removing 51
- starting 51
- stopping 51

### Altix CIM Extension

- installing 61
- prerequisites 61
- removing 61
- starting 61
- stopping 61

### APPIQ\_OWNER account 115

### APPIQ\_USER 132

### Application Administrator role 135

### applications

- discovering 115

### assigning

- MIME types 46, 133

### audience xi

### authentication errors

- SNMP 171

### authorized reseller, HP xiii

## B

### benefits 1

### Bridge Agent 20

### Brocade Rapid program 39

### Brocade switches 39

- discovering 17

## C

### changing

- database 47
- domain controller 115, 130
- e-mail address 144
- full name 144
- login name 144
- number of retries 28, 168
- organizations 151
- password 39, 132, 144
- phone number 144
- roles 148
- SNMP trap listener 20
- time-out period 28, 168
- TNS Listener Port 130
- user account 143
- user name 39
- user preferences 145
- user profile 144

### child organizations 135

### CIM xi, 1

### CIM Extension

- installing 69, 95, 105
- port 159

- Solaris 69, 95
- Windows 105
- CIM Extensions
  - about 51, 61, 69, 79, 95, 105
  - AIX 51
  - Altix 61
  - HP-UX 69
  - IRIX 79
  - Solaris 95
  - Windows 105
- cimom.CimXmlClientHttpConnectTimeout 173
- cimom.emc.skipRefresh 43
- cimom.hds.exclude 34
- cimom.symmetrix.exclude 32
- CIO role 135
- clearing
  - elements 28
- CNT
  - switches 19
- configuring
  - e-mail notification 167
- controller
  - removing 115, 131
- conventions
  - document xii
  - text symbols xii
- cookies
  - JavaScript 1
- creating
  - new password 144
  - organizations 150
  - roles 147
  - user accounts 142

## D

- Data Discovery Collection
  - e-mail notification 167
- database
  - AIX 171
  - management server 7
  - updating 47
- database connection failed
  - error 170
- DCOM
  - unable to communicate 170
- deleting
  - domain controller 115, 131

- elements 28, 40
- organizations 152
- roles 149
- switches 46
- TNS Listener Port 130
- user accounts 144
- details
  - obtaining 41
- detecting
  - IP range 17
  - McDATA switches 46
  - switches 46
- device issues 178
- devices
  - deleting 40
- discovered address
  - modifying 39
- discovered elements
  - deleting elements 40
- discovering
  - applications 115
  - Brocade switches 17, 39
  - CNT switches 19
  - EMC Solutions Enabler 31
  - HDS storage systems 33
  - HDS systems 34
  - HP XP storage systems 35
  - IP address 17
  - McDATA switches 20
  - Microsoft Exchange 115, 127, 171
  - NetApp filers 36
  - Oracle 115, 116
  - Oracle clusters 116
  - SQL servers 121
  - storage system 15
  - storage systems 33, 36
  - Sun StorEdge storage systems 37, 38
  - Sun StorEdge switches 19
  - switches 15, 17
  - Sybase 115, 124
  - Symmetrix systems 32
  - troubleshooting 171, 181
- discovery
  - authentication errors 171
  - quarantine 48, 49
  - time-out 173
  - troubleshooting 170



- discovery groups 39
- discovery requirements
  - Oracle 171
- discovery settings
  - importing 47
- discovering
  - IBM storage systems 38
- disk drive 132, 173
- displaying
  - deleted Oracle instances 171
- DNS 171
- document
  - conventions xii
  - prerequisites xi
  - related documentation xi
- documentation, HP web site xi
- Domain Administrator role 135
- domain controller
  - access 130
  - accessing 115, 130
  - removing 115, 131
- domain controller access 115, 130
- drivers
  - fixing 178
- drives
  - Microsoft Exchange 171
  - uninitialized 173

## E

- editing
  - e-mail address 144
  - full name 144
  - login name 144
  - organizations 151, 153
  - password 144
  - phone number 144
  - roles 148
  - user account 143
  - user preferences 145
  - user profile 144
- EFC Manager 20
- element details
  - obtaining 41
- elements
  - adding 150, 151
  - deleting 28, 40
  - getting details 47

- managing 151
- modifying 39
- organization 151
- removing 153
- unable to find 172
- e-mail address
  - changing 144
- e-mail notification
  - Get Details 167
- EMC CLARiiON 33
- EMC Solutions Enabler 31
- error
  - database connection failed 170
- Error 503 158
- error message
  - exclusive lock 181
- errors
  - authentication 171
- excluding
  - HDS systems 34
  - switches 27
  - Symmetrix systems 32
- exclusive lock
  - error message 181
- Extension
  - CIM 69, 95

## F

- features
  - key 1
- file extension
  - assigning 46, 133
- filtering
  - organizations 154
- finding
  - applications 115
  - hosts 115
  - IP address 17
  - IP range 17
  - storage systems 15
  - switches 15
- fixing
  - drivers 178
- full name
  - changing 144

## G

- ganizations 151
- getting
  - element details 41
- getting details 41, 47
  - applications 115
  - hosts 115

## H

- HBAs
  - swapping 177
- HDS storage systems
  - discovering 33
- HdsSkipRefresh 45
- Help Desk role 135
- help, obtaining xiii
- hierarchy
  - organizations 135
- host
  - not in topology 172
- host bus adapter
  - unable to detect 173
- hosts
  - discovering 115
  - removing 28
- hot-swapped
  - drives 173
- HP
  - authorized reseller xiii
  - storage web site xiii
  - Subscriber's choice web site xiii
  - technical support xiii
- HP XP storage systems 35
- HP-UX CIM Extension
  - installing 69
  - prerequisites 69
  - removing 69
  - starting 69
  - stopping 69
- HTTP Error 503 158
- HTTPS 7

## I

- IBM storage systems
  - discovering 38
- importing

- discovery settings 47
- information
  - obtaining element 41
- installing
  - AIX CIM Extension 51
  - Altix CIM Extension 61
  - CIM Extension 69, 95, 105
  - HP-UX CIM Extension 69
  - IRIX CIM Extension 79
  - Java plug-in 12
  - management server 7
  - security certificate 7
  - Solaris CIM Extension 95
  - Windows CIM Extension 105
- internal
  - drives 173
- IP range 17
- IRIX CIM Extension
  - installing 79
  - prerequisites 79
  - removing 79
  - starting 79
  - stopping 79
- issues
  - devices 178

## J

- Java 1
- Java plug-in
  - installing 12

## K

- key benefits 1
- key features 1

## L

- local drives 171
- locating
  - storage systems 15
  - switches 15
- log messages
  - viewing 28
- login name
  - modifying 144

## M

- management server
  - about 1
  - database 7
  - installing 7
  - security 135
- managing
  - elements 150, 151, 153
  - switches 46
- McDATA switches 172
  - adding 46
  - discovering 20
- messages
  - data is late 157
- Microsoft Exchange
  - discovering 115, 127, 171
  - drive M 171
- MIME types 46, 133
- mixed mode authentication 121
- modifying
  - database 47
  - discovered address 39
  - domain controller 115, 130
  - elements 39
  - e-mail address 144
  - full name 144
  - login name 144
  - organizations 151
  - password 39, 132, 144
  - phone number 144
  - roles 148
  - SNMP trap listener 20
  - TNS Listener Port 130
  - user account 143
  - user name 39
  - user preferences 145
  - user profile 144

## N

- naming organizations 135
- NetApp filers
  - discovering 36
- netcfg 31
- nethost 31
- Networking xi
- new password 144

- nonexistant IP addresses 173
- nonexistent Oracle instances 171
- number of retries
  - changing 28, 168

## O

- Oracle
  - deleted instances 171
  - discovering 115, 116
  - discovery requirements 171
- Oracle TNS Listener Port 130
- organizations
  - about 135
  - adding 150
  - deleting 152
  - editing 151, 153
  - elements 150, 151, 153
  - filtering 154
  - properties 147
  - users 147
  - viewing 151

## P

- parent organizations 135
- password
  - changing 39, 132, 143, 144
- phone number
  - editing 144
- planning organizations 135
- port
  - CIM Extension 159
- prerequisites xi
  - AIX CIM Extension 51
  - Altix CIM Extension 61
  - HP-UX CIM Extension 69
  - IRIX CIM Extension 79
  - Solaris CIM Extension 95
  - Windows CIM Extension 105
- privileges
  - roles 135
- problems
  - drivers 178
- process
  - exclusive lock 181
- profile
  - user 144

- properties
  - organizations 147
  - roles 146
- provisioning
  - troubleshooting 181

## Q

- quarantine
  - adding elements 48
  - clearing elements 49

## R

- Rapid program 39
- refreshing
  - Symmetrix systems 43
- related documentation xi
- remote drives 171
- removing
  - AIX CIM Extension 51
  - Altix CIM Extension 61
  - domain controller 115, 131
  - elements 28, 40, 151, 153
  - HP-UX CIM Extension 69
  - IRIX CIM Extension 79
  - organizations 152
  - roles 149
  - Solaris CIM Extension 95
  - switches 46
  - TNS Listener Port 130
  - user accounts 144
  - Windows CIM Extension 105
- replacing
  - switches 46
- replication 47
- requirements 1
  - software 1
- roles
  - about 135
  - adding 147
  - Application Administrator 135
  - CIO 135
  - deleting 149
  - Domain Administrator 135
  - editing 148
  - Element Control privilege 135
  - Full Control privilege 135

- Help Desk 135
- privileges 135
- properties 146
- Server Administrator 135
- Storage Administrator 135
- users 146
- View privilege 135

## S

- SAN xi
- saving
  - settings to a file 47
- scanning
  - IP range 17
- security
  - Management server 135
  - roles 147, 148
- security certificate
  - installing 7
- Server Administrator role 135
- silent installation
  - Windows 110
- SNMP
  - authentication errors 171
- SNMP trap listener
  - changing 20
- software requirements 1
- Solaris CIM Extension
  - installing 95
  - prerequisites 95
  - removing 95
  - starting 95
  - stopping 95
- SQL Server
  - authentication modes 121
- SQL servers
  - discovering 121
- starting
  - AIX CIM Extension 51
  - Altix CIM Extension 61
  - HP-UX CIM Extension 69
  - Solaris CIM Extension 95
  - Windows CIM Extension 105
- statistics 132
- stopping
  - AIX CIM Extension 51
  - Altix CIM Extension 61

- HP-UX CIM Extension 69
- IRIX CIM Extension 79
- SAN details 43
- Solaris CIM Extension 95
- Windows CIM Extension 105
- Storage Administrator role 135
- storage systems 36, 132
  - discovering 15, 36
  - removing 28
- storage terms 1
- Subscriber's choice, HP xiii
- Sun StorEdge
  - SNMP trap listener 20
- Sun StorEdge storage systems 37, 38
- Sun StorEdge switches 19
- swapped
  - drives 173
- swapping
  - switches 46
- swapping HBAs 177
- switches
  - adding 46
  - discovering 15, 17
  - excluding 27
  - managing 46
  - McDATA 20, 46, 172
  - number of retries 28, 168
  - removing 28, 46
  - replacing 46
  - time-out period 28, 168
  - unable to monitor 172
- Sybase
  - discovering 115, 124
- symbols in text xii
- System Manager
  - can't access 177
  - deleting elements 40

## T

- technical support, HP xiii
- terms
  - storage 1
- text symbols xii
- time-out period
  - changing 28
- TNS Listener Port
  - changing 130

- topology
  - AIX 171
  - host not appearing 172
- troubleshooting
  - discovery 170
  - discovery and getting element details 170, 171, 172, 181
  - Microsoft Exchange 171
  - provisioning 181

## U

- unable to
  - discover 170
  - detect
    - host bus adapter 173
  - find elements 172
  - retrieve data 177
- uninitialized
  - drives 173
- updating
  - database 47
- user accounts
  - creating 142
  - deleting 144
- user name
  - changing 39
- user preferences
  - changing 145
- user profile
  - modifying 144
- users
  - about 135
  - adding 142
  - organizations 147
  - roles 146, 147, 148

## V

- viewing
  - log messages 28
  - organization properties 147
  - organizations 151

## W

- Web browsers 1
- web sites

- HP documentation [xi](#)
- HP storage [xiii](#)
- HP Subscriber's choice [xiii](#)
- WEBEM [1](#)
- Windows
  - silent installation [110](#)
- Windows CIM Extension
  - installing [105](#)
  - removing [105](#)
  - starting [105](#)
  - stopping [105](#)

## Figures

|   |                                               |     |
|---|-----------------------------------------------|-----|
| 1 | Starting WMI (Microsoft Windows 2000).....    | 107 |
| 2 | Parent-Child Hierarchy for Organizations..... | 139 |
| 3 | Children in Multiple Organizations.....       | 140 |
| 4 | Changing Your User Profile.....               | 144 |
| 5 | Accessing the User Preferences Tab.....       | 145 |
| 6 | Viewing Organizations.....                    | 151 |
| 7 | Clicking the Organization Link.....           | 154 |
| 8 | Active Organization.....                      | 155 |





## Tables

|    |                                                                                 |     |
|----|---------------------------------------------------------------------------------|-----|
| 1  | Document conventions . . . . .                                                  | xii |
| 2  | Roadmap for Installation and Initial Configurations . . . . .                   | 1   |
| 3  | Discovery Requirements for Switches . . . . .                                   | 16  |
| 4  | Required Switch Models and InVsn<br>Versions for Discovery18                    |     |
| 5  | Discovery Settings for McDATA and Connectrix Switches . . . . .                 | 21  |
| 6  | Discovery Requirements for Storage Systems and NAS Filers . . . . .             | 29  |
| 7  | Default Role Privileges . . . . .                                               | 136 |
| 8  | Default Role Privileges with Elements . . . . .                                 | 137 |
| 9  | Changing User Preferences for Event Monitoring for Storage Essentials . . . . . | 145 |
| 10 | Troubleshooting Firewalls . . . . .                                             | 161 |
| 11 | Time-out Properties . . . . .                                                   | 169 |
| 12 | Retry Properties . . . . .                                                      | 169 |
| 13 | Known Device Issues . . . . .                                                   | 178 |

