HP Storage Essentials SRM 6.0 Installation Guide

for Enterprise Edition and Standard Edition SRM Software

Second edition: April 2008

invent

Legal and notice information

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

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 shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and 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, HP-UX, and OpenVMS, Tru64 UNIX are registered trademark of Hewlett-Packard Development Company. QLogic is a trademark of QLogic Corporation. Emulex is a registered trademark of Emulex Corporation. HBAnyware is a trademark of Emulex Corporation.

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.

HP Storage Essentials SRM 6.0 Installation Guide

Contents

Figures

Tables

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 SRM
- HP Storage Essentials SRM User Guide
- HP Storage Essentials SRM Application Guide
- HP Storage Essentials SRM CLI Guide
- HP Storage Essentials SRM 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	• 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
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• 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 contains the following topics:

Supported Platforms for Installing HP Storage Essentials

This chapter provides a general overview of the installation steps for the various operating systems on which HP Storage Essentials is supported:

- Linux
- Microsoft Windows

NOTE: The Linux management server is not available with Storage Essentials Standard Edition.

Roadmap for Installation and Initial Configurations

Storage Essentials integrates tightly with HP Systems Insight Manager. The installation steps for Storage Essentials require you to install Storage Essentials, HP System Insight Manager, and the HP SIM Connector. HP highly recommends that you follow the steps outlined in Table 2 on page 2.

Be sure to see the support matrix for your edition. The support matrix can be found on the top level of the management server CD-ROM.

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.	• **Microsoft Windows** - See "Installing the Management Server on Microsoft Windows" on page 7. • **Linux** - See "Installing the Management Server on Linux" on page 59.
2	Perform discovery for switches, NAS devices, and storage systems. This step requires the management server to be connected to the network containing the switches, NAS devices, and storage systems you want to manage.	See "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" on page 105.

Table 2 Roadmap for Installation and Initial Configurations (continued)

Step	Description	Where to Find
3	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. It is possible to install, upgrade, and manage CIM Extensions remotely across any number of hosts. See "Deploying and Managing CIM Extensions" on page 181. HP Storage Essentials Standard Edition supports a subset of the devices supported by Enterprise Edition. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials). **IMPORTANT:** Do not install CIM extensions on the management server.[1]	• **IBM AIX** - See "Installing the CIM Extension for IBM AIX" on page 191. • **SGI ProPack for Linux** - See "Installing the CIM Extension for SGI ProPack for Linux" on page 201. • **HP-UX** - See "Installing the CIM Extension for HP-UX" on page 209. • **SGI IRIX** - See "Installing the CIM Extension for SGI IRIX" on page 219. • **SUSE and Red Hat Linux** - See "Installing the CIM Extension for SUSE and Red Hat Linux" on page 227. • **HP OpenVMS (Alpha)** - See "Installing the CIM Extension for OpenVMS" on page 249. • **HP Tru64 UNIX** - See "Installing the CIM Extension for HP Tru64 UNIX" on page 261. • **Sun Solaris** - See "Installing the CIM Extension for Sun Solaris" on page 271. • **Microsoft Windows** - See "Installing the CIM Extension for Microsoft Windows" on page 281. • **NonStop** - See "Installing the CIM Extension for NonStop" on page 237
4	The Windows Proxy is required when the management server is on Linux and you want to obtain information from Microsoft Windows hosts that do not have a CIM extension installed.	See "Installing and Discovering the Windows Proxy" on page 291.
4	Configure the applications and hosts for monitoring. This step includes discovering applications, master backup servers, and hosts.	See "Discovering Applications, Backup Hosts and Hosts" on page 297.
5	Change the password of the system accounts.	See "Changing the Password of System Accounts" on page 368.

[1] If you install CIM extensions on the management server, the Database Admin Utility returns the following error and does not run correctly: `[isAppIQCIMOMAlive] - false`

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 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 for the management server and for the elements you plan to discover, refer to the support matrix for your edition.

Web Browser Configuration Requirements

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

- cookies
- JavaScript
- Java

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

Follow the steps in this chapter to install the management server on the Windows operating system. See the following topic if you are installing the management server on another supported operating system:

- "Installing the Management Server on Linux" on page 59

Important Information About Upgrading

Please contact your Account Representative for upgrades. Upgrading requires assistance from HP Services.

Be sure to read "Installation/Upgrade Process is Now Automated" on page 8 and the requirements in the "Pre-installation Checklist (Installations and Upgrades)" on page 8 for important installation and upgrade information.

NOTE: The Linux management server is not available with Storage Essentials Standard Edition.

This chapter contains the following topics:

Keep in Mind the Following

- **All steps must be completed for the management server to work properly.**
- Before beginning any installation or upgrade steps, refer to the support matrix for your edition to determine the minimum software and hardware requirements. The support matrix can be found on the top level of the management server CD-ROM.
- During the management server for Windows installation, double-byte characters are not allowed in the installation path. The installation wizard displays the following error message if the path does not meet the requirements:

  ```
  The installation path for $PRODUCT_NAME$ may NOT contain embedded
  spaces, non-English characters, or punctuation. The path is limited
  to basic ASCII alphanumeric characters.
  ```
- Install the management server on a dedicated computer.
- Installation using Virtual Network Computing (VNC) software is not supported.
- If the installation software is accessed over a network, the software must be accessed using a mapped network drive (drive letter). Installation using an UNC path (\\host\sharename) will not work.
- All communication with regard to managed elements is out-of-band via IP, and no SAN connectivity is required or recommended for the management server.

Installation/Upgrade Process is Now Automated

The installation and upgrade process is now automated by the installation/upgrade wizard. Manual installations are no longer recommended. Be sure to read and follow the new installation and/or upgrade instructions in this document.

IMPORTANT: Please contact your Account Representative for upgrades. Upgrading requires assistance from HP Services.
Do not manually install the Oracle database. You must begin the installation starting with the Storage Essentials installation wizard CD or setup.exe file.

Pre-installation Checklist (Installations and Upgrades)

The following basic requirements must be met before beginning an installation or upgrade. If the management server installation wizard detects missing requirements during system verification you will need to make changes to your system. The basic system requirements are explained in this section along with additional information on how to meet these requirements:

- Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met), page 9
- How to Install Microsoft SNMP and SNMP Trap Services, page 12
- How to Verify that Microsoft Access Data Components (MDAC) 2.7 Service Pack 1 or Later is Installed, page 13

- How to Verify Networking, page 14
- Be Sure to Install a Supported Browser, page 14

Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)

The requirements listed in Table 3 on page 10 must be met or the installation or upgrade will stop. See "Overview of the Verify System Requirements Screen" on page 11 for additional information about the requirements listed on the Verify System Requirements screen (one of the screens displayed during an installation or an upgrade by the installation/upgrade wizard).

IMPORTANT: Contact Customer Support if you are upgrading. Upgrades require assistance from Customer Support.

Table 3 Pre-installation Requirements to Install or Upgrade

Requirement:	**Must Meet or Exceed or the Installation or Upgrade Will Stop:**
NTFS File System:	**Installations:** The NTFS file system is required to install the product. **Upgrades:** If Oracle 9i is installed on a volume using the FAT32 file system, you must convert the volume to NTFS before you can upgrade. Contact customer support for information about converting the volume to NTFS.
Screen Resolution:	Minimum resolution is 800x600.
Windows Account:	You must be logged in as an Administrator.
Operating System:	Microsoft Windows Server 2003 SP1 or higher. Windows 2000 is no longer supported. See the support matrix for more information.
MS Internet Explorer:	Internet Explorer 6 SP 1 or higher.
TCP/IP:	TCP/IP must be enabled.
Minimum disk space for temp and installation files:	The drive that the TEMP environment variable points to must have at least 2 GB of free space. If your TEMP directory is not on your system drive, make sure your system drive has at least 65 MB free as well.
%perl5lib% environment variable:	The `%perl5lib%` environment variable cannot be set to any value. See "Troubleshooting Installation/Upgrade" on page 379 for more information.
Installation Locations specified in the Installation Options screen for the following share these requirements: • HP Systems Insight Manager • Storage Essentials • Oracle Database • Oracle Database Backup	• Valid locations must be entered on the Installation Options screen. • Path information can only contain the following characters: A-z, 0-9, hyphen, underscore, period, back slash. • Storage Essentials, Oracle database, and Oracle database backup paths cannot contain spaces. • Drive letter must be a fixed drive.

Table 3 Pre-installation Requirements to Install or Upgrade

Requirement:	**Must Meet or Exceed or the Installation or Upgrade Will Stop:**
HP Systems Insight Manager Credentials:	Valid HP Systems Insight Manager credentials must be entered on the Storage Essentials HP Systems Insight Manager Service Account Credentials screen or the Storage Essentials installation wizard will stop during a single-server installation (HP SIM and Storage Essentials installed on the same server).
SNMP and SNMP Trap Services:	SNMP and SNMP Trap Services must be installed and running or the Storage Essentials installation wizard will stop during a single-server installation (HP SIM and Storage Essentials installed on the same server). See "How to Install Microsoft SNMP and SNMP Trap Services" on page 12 for details on installing and starting these services.

Overview of the Verify System Requirements Screen

The Verify System Requirements screen displays the current status for the following based on the results of the system scan performed by the installation wizard after starting the installation or upgrade. Requirements that must be met to proceed with the installation/upgrade and requirements that do not stop the installation/upgrade are described here:

- **Current User Account —** The account you use to install/upgrade must have Windows Administrator privileges or the installation or upgrade will stop.
  - **Memory** — The minimum RAM requirement varies depending on your installation option:
    - When HP SIM and Storage Essentials are installed on separate servers the minimum RAM requirement for the Storage Essentials server is 4 GB with 6 GB recommended.
    - When HP SIM and Storage Essentials are installed on the same server together the minimum RAM requirement for the Storage Essentials server is 6 GB with 8 GB recommended.

  NOTE: If the minimum amount of RAM is close to the requirement, the installation wizard continues.

- **Physical Address Extension (PAE)** — PAE is a Windows setting to utilize amounts of RAM greater than 4 GB on certain versions of Windows. See your Windows documentation for more information about PAE settings. The installation or upgrade continues regardless of PAE.
- Disk Storage (typical installation) — Depends on the following:

    - With ARCHIVING and RMAN backup off: minimum disk space: 100 GB, recommended disk space: 200 GB.
    - With ARCHIVING and RMAN backup on: minimum disk space: 200 GB, recommended disk space: 350 GB.

  The installation or upgrade will not continue if the disk space requirements are not met.

  Operating System — Windows 2003 Server SP1, SP2, R2, R2 SP2. The installation or upgrade will not continue if the operating system requirement is not met.

- **Processor —** A dual Intel XEON (or AMD equivalent) 3.4 GHz or higher CPU is required. If the CPU is close to the requirement, the installation wizard continues.
- DNS Resolution — The installation wizard verifies the IP address and DNS name of the server using nslookup. If nslookup is not successful, the installation will continue.

> **IMPORTANT:** DNS Resolution failure will prevent the product from running successfully. See the following topic in the troubleshooting chapter if the DNS Resolution requirement fails: “Reverse Lookup Failed” Message (Windows only), page 382.

- **Port Availability —** The management server requires the following ports to be available:
    - 80
    - 162
    - 443
    - 1098–1120
    - 4444
    - 4445
    - 4763
    - 5962–5988
    - 8009
    - 8083
    - 8093

  If you see a warning in the Ports Availability requirement you need to check to be sure that the ports listed are not currently in use and make any changes that are necessary. Be aware that the installation will continue even if a required port is not available.

> **NOTE:** During upgrades, the Port Availability check may falsely indicate that the port for the management server is currently in use. When you check the port, you see that it is reserved by the management server and you can therefore safely ignore the warning.

How to Install Microsoft SNMP and SNMP Trap Services

To install Microsoft SNMP and SNMP Trap Services:

1. Check Windows Services (**Start > Administrative Tools > Services**) to see if the SNMP Service is installed and running. If it is not installed, continue with step 2.

NOTE: These instructions may vary depending on the version of Windows you are running.

2. Go to **Control Panel > Add or Remove Programs > Add/Remove Windows Components**.
3. Select the **Management and Monitoring Tools** line and click **Details**.
4. Unselect everything except **Simple Network Management Protocol**. Click **OK**.
5. Select **Next**, then select **Next** again. Keep Remote administration mode selected.
6. Ensure that you deselect **Internet Information Services (IIS)** – it is enabled by default when installing SNMP. Click **OK** if you get a warning box to remove Connection Manager Components.
7. Insert the Windows CD when prompted.
8. Follow the wizard to complete the installation of the SNMP Services.
9. Verify in Services that the SNMP Service is now running as a service.

IMPORTANT: If SNMP is not running, the HP SIM login page will not be displayed.

How to turn off Internet Information Services (IIS) and Third–Party Web servers

To turn off Internet Information Services (IIS) and third–party Web servers, verify that Internet Information Services (IIS) is either not installed or the service is set to manual and stopped.

Other third–party Web servers also conflict with Storage Essentials, which uses port: 80 and/or port: 443 for its services. If IIS is running, port: 80 and/or port: 443 is already used and Storage Essentials pages will not be displayed. HP SIM pages will continue to render properly. If IIS is running, you will not be able to access a Storage Essentials page from HP SIM and you will see the following error in the log located at `<Storage Essentials Installation Directory>\logs\appstorm.<timestamp>.log`:

```
java.net.BindException: Address already in use: JVM_Bind:
```

How to Verify that Microsoft Access Data Components (MDAC) 2.7 Service Pack 1 or Later is Installed

To verify that Microsoft Access Data Components (MDAC) 2.7 Service Pack 1 or later is installed:

1. Navigate to `<installDrive>\Program Files\Common Files\System\Ado`
2. Right-click the icon for the msado15.dll file.
3. In the pop-up menu, select **Properties**, and click the **Version** tab to display the version number. The version must be 2.7 or later.
4. If the file is not found in this path, use the Windows search engine to find the file.
5. If you must download MDAC, refer to http://www.microsoft.com/downloads/ and search for MDAC Service Pack. Download and install 2.7 SP1 or later.
6. Reboot when prompted.

How to Verify Networking

The management server must have static or dynamic host name resolution. To verify that the server's name can be resolved through DNS:

1. Right click **My Computer** in the Start menu.
2. Select **Properties**.
3. Click on the **Computer Name** tab to see the fully qualified name of the computer under the label Full Computer Name. The server must be in the domain in which it is going to be used.
4. From a command prompt, type `nslookup <FQDN>`.

   FQDN (fully qualified domain name) is the fully qualified computer name obtained in the previous step.
5. In the command prompt, type `nslookup <IP address>`.

   IP address is the IP address of the server.

   Both results from nslookup should have the same fully qualified computer name and IP address.
6. In the command prompt, type `nslookup <Short name of computer>`. Results should resolve to the computer's fully qualified computer name and IP address.

HP SIM uses nslookup to resolve the names and IP addresses of managed systems. If the DNS suffix `com` is listed in the TCP/IP properties as one to append, problems such as inaccurate system status and incorrect IP addresses for systems HP SIM manages may occur. To correct this, remove `com` from the TCP/IP DNS suffix list:

1. Open **Control Panel** > **Network Connections** > **Local Area Connection > Properties**. Choose the **Internet Protocol** > **Properties** > **Advanced** > **DNS** tab.
2. If `com` is in the **Append these suffixes (in order)** box, remove it.

NOTE: If you will be browsing to HP SIM from a server in a different domain, assure that the DNS suffix of the management server is added to the suffix list of the web client. Failure to set this will prevent Storage Essentials pages from rendering. HP SIM pages will work correctly.

Be Sure to Install a Supported Browser

Install a supported browser on any machine from which you intend to view HP SIM and HP Storage Essentials pages. See the support matrix for a list of supported browsers.

About the New Storage Essentials for Windows Installation Options

If you are familiar with installing earlier builds of Storage Essentials, earlier than Build 6.0, be aware that the installation steps have changed. See "Installation/Upgrade Process is Now Automated" on page 8 for important information.

Storage Essentials can be installed as a plug-in to HP Systems Insight Manager (HP SIM) in an integrated configuration or you can choose to install the standalone version of Storage Essentials. The integrated version of Storage Essentials and HP SIM can be installed on separate servers or on a single server depending on your requirements. An additional software component—included in the Storage Essentials installation files—(the HP SIM Connector) provides the integration between Storage Essentials and HP SIM.

The Storage Essentials installation wizard automatically installs the HP SIM Connector on the Storage Essentials server (along with the other software components described later). When Storage Essentials is installed in the separate server configuration, the Storage Essentials installation wizard additionally installs the HP SIM Connector on the separate HP SIM server via a network connection to provide communication between HP SIM and Storage Essentials on separate servers.

As a best practice, HP recommends installing HP Storage Essentials as a plug-in for HP Systems Insight Manager (the integrated version of Storage Essentials). The integrated version of HP SIM and Storage Essentials provides the following feature sets:

- Hardware and software health status polling, monitoring, and event management for:
    - Storage
    - Servers
    - Switches
    - Infrastructure
    - And other elements on your network such as enclosures, racks, clients and printers
- HP SIM provides standards-based support for HP and third-party devices and management frameworks.
- When Storage Essentials is integrated with HP SIM, you access the Storage Essentials features and menu options via Storage Essentials menu items on the HP SIM menus and within various HP SIM screens.

The integrated version of HP Storage Essentials and HP Systems Insight Manager includes the following software components:

- HP Systems Insight Manager 5.1 SP1
  (HP SIM 5.2 is also supported. Contact your Sales Engineer to determine which version of HP SIM is best for your environment. This installation guide provides instructions for installing HP SIM 5.1, the version included with your Storage Essentials 6.0 product kit.)
- Storage Essentials 6.0
- HP SIM Connector 6.0
  (included in the Storage Essentials installation files and automatically installed by the Storage Essentials installation wizard)
- Oracle 10g Standard Edition for Storage Essentials 6.0
  (automatically installed by the Storage Essentials installation wizard)
- CIM Extension files (6.0)—Common Information Module files that you install on the hosts and other network elements you want to manage and for which you want to automate discovery.
- CIM Extension Management tool for installing some of the supported CIM extensions in batch mode, remotely, onto multiple hosts.

Storage Essentials Installation Wizard Options

This release of the HP Storage Essentials management server for Windows provides the following options for installing the Storage Essentials management server:

IMPORTANT: The server must meet or exceed the minimum requirements listed in the support matrix for your edition.

- **Integrated with Storage Essentials and HP Systems Insight Manager (HP SIM) on separate servers (recommended)**
  As a best practice HP recommends installing the integrated product on separate servers. This installation option provides hardware and software health status polling, monitoring, and event management for storage, servers, switches, infrastructure, and other elements on your network such as enclosures, racks, clients and printers. In addition, HP SIM provides standards-based support for HP and other third-party management frameworks.

  See Installing Storage Essentials and HP Systems Insight Manager for Windows on Separate Servers, page 17 for steps on installing with this option.

- **Integrated with HP Storage Essentials and HP Systems Insight Manager on the same server**
  Installing Storage Essentials and HP SIM on the same server provides the same benefits provided with the recommended installation option, except that all of the components are installed on one server. This option has greater minimum system requirements. See the support matrix for details.

  See Installing Storage Essentials and HP SIM for Windows on the Same Server, page 27 for steps on installing with this option.

- **Standalone Option: HP Storage Essentials only installation**
  HP Storage Essentials is installed on a single server without the HP SIM and other integrated components. (This option is supported, but not recommended because it does not provide the full feature set provided by the integrated installation options.)

  See "Installing the Standalone Version of Storage Essentials for Windows" on page 34 for steps on installing with this option.

The Storage Essentials installation wizard checks your system to verify that it meets the basic system requirements and it automatically installs the required Oracle database instance and the following software: HP Storage Essentials, the HP SIM Connector, and HP Systems Insight Manager (note that the separate server installation option requires the manual installation of HP SIM on the designated HP SIM server).

IMPORTANT: Do not install the Oracle database separately. With this release of the product, you must first install the management server for Windows CD. The installation wizard automatically installs the Oracle database and prompts you for the Oracle CD during the installation at the appropriate time. Installing the Oracle database used by the management server manually is no longer recommended. Be sure to see "Installation/Upgrade Process is Now Automated" on page 8.

Installing Storage Essentials and HP Systems Insight Manager for Windows on Separate Servers

This is the recommended installation option. Complete the following steps to install HP SIM and the Storage Essentials management server for Windows on separate servers.

IMPORTANT: HP SIM and Storage Essentials must be installed on the same domain.

Step 1 – Read the Support Matrix and Release Notes

Read the support matrix and make sure the server (or servers) on which you are installing the Storage Essentials management server meets or exceeds the requirements. The installation wizard provides a link to the support matrix and release notes on each screen (**Documentation** > **Support Matrix** or **Release Notes**).
See "Troubleshooting Installation/Upgrade" on page 379 for additional help if needed.

Step 2 – (Required for Separate Server Installations Only) Manually Install HP Systems Insight Manager

IMPORTANT: As of the publication of this Second edition of the *HP Storage Essentials SRM 6.0 Installation Guide*, HP SIM 5.2 is also supported. Contact your Sales Engineer for help with determining which version of HP SIM best meets your network management requirements.

Storage Essentials 6.0 is only compatible with HP SIM 5.1 SP1 or 5.2. Earlier versions of HP SIM are not supported with this release of Storage Essentials. Note that the instructions in this section describe how to install HP SIM 5.1 — the version of HP SIM included in your Storage Essentials 6.0 product software kit. HP SIM 5.1 Service Pack 1 is additionally required.

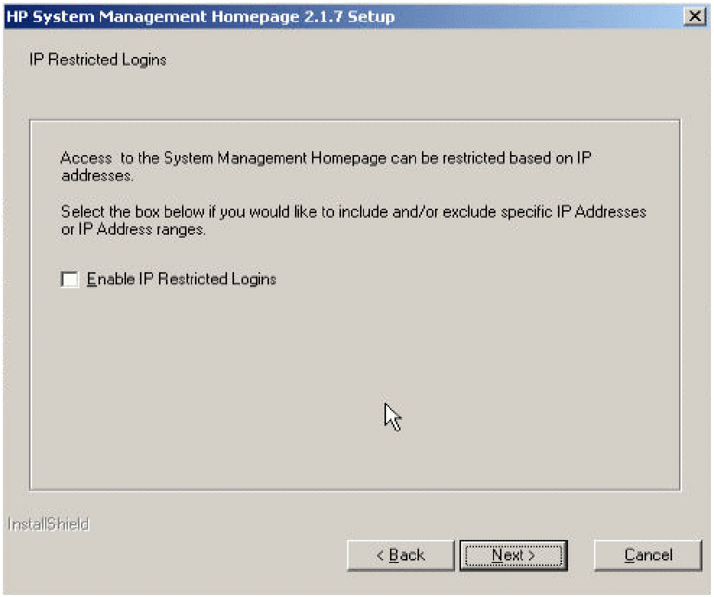
Install HP SIM 5.1 on the designated HP SIM server following the steps in this section.

By default, the Custom installation option is enabled during the HP SIM installation. You can set system security options based on your site requirements when prompted during the HP SIM installation.

1. Log on to the designated HP SIM Windows server and create a Windows user account with administrative privileges with which to install and manage HP SIM. As a best practice, consider naming the account HP SIM to make it easier to delineate from other user accounts.

2. Put the HP SIM 5.1 CD in the CD drive of the designated HP SIM server. The HP SIM installation wizard program starts automatically. If the HP SIM installation does not start, double-click **setup.exe** found in the `hpsim` directory.
3. Follow the instructions on the HP SIM 5.1 installation screens. As a best practice, install only the HP SIM components that are required to install and set up Storage Essentials:
   - System Management Homepage
   - HP Systems Insight Manager
4. Accept the default options on each HP SIM screen except for the options noted below.

   - Do not enable IP Restricted Logins.



HP System Management Homepage 2.1.7 Setup

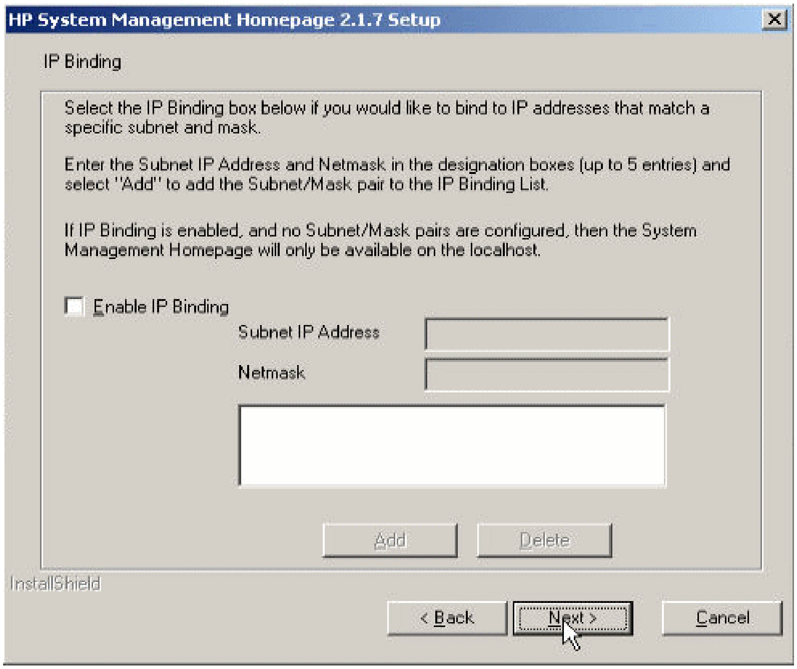
IP Restricted Logins

Access to the System Management Homepage can be restricted based on IP addresses.

Select the box below if you would like to include and/or exclude specific IP Addresses or IP Address ranges.

□ Enable IP Restricted Logins

- Do not enable IP Binding.



HP System Management Homepage 2.1.7 Setup

IP Binding

Select the IP Binding box below if you would like to bind to IP addresses that match a specific subnet and mask.

Enter the Subnet IP Address and Netmask in the designation boxes (up to 5 entries) and select "Add" to add the Subnet/Mask pair to the IP Binding List.

If IP Binding is enabled, and no Subnet/Mask pairs are configured, then the System Management Homepage will only be available on the localhost.

☐ Enable IP Binding

Subnet IP Address

Netmask

You can optionally install other HP SIM components at a later time by running the HP SIM CD again on the HP SIM server and following the instructions in the HP SIM documentation once the Storage Essentials installation is complete.

5. Reboot the HP SIM server when prompted at the end of the HP SIM installation.
6. Do not set up discovery when prompted by the HP SIM First Time User wizard. For the integrated version of Storage Essentials and HP SIM you will set up discovery after the Storage Essentials components are installed and you have imported your Storage Essentials license.

Step 3 – Install Storage Essentials on the Storage Essentials Server

Install Storage Essentials from the Storage Essentials CD (or a network or local drive) following the steps in this section.

NOTE: The drive on which you install Storage Essentials must be NTFS format or the installation will fail.

The directory in which you install the Storage Essentials management server must have write access for the local Administrators group. Be aware that installing the management server in a directory created by another program (for example: the Proliant Support Pack) is not recommended.

Follow these steps to install Storage Essentials (for the HP SIM-integrated separate server installation option):

1. Verify the following:
   - The designated Storage Essentials server meets or exceeds the requirements listed in the Pre-installation Checklist (Installations and Upgrades), page 8 and in the support matrix for your edition.
   - The file system format on the Storage Essentials server is NTFS. The Storage Essentials installation wizard will display an error message if the file system is not NTFS.
   - The Storage Essentials server must reside on the same domain with the HP SIM server.
2. Start the Storage Essentials installation wizard using one of the following options:

   To install from the CDs do the following:

   a. Put the Storage Essentials CD in the CD drive of the designated Storage Essentials server. The Storage Essentials installation wizard program should start automatically.

   b. If it does not start, double-click **setup.exe** found in the `root` directory on the Storage Essentials CD.

   To install from a network or local hard drive, do the following:

   a. Create the following directory structure on the designated drive from which you will install Storage Essentials:

   IMPORTANT: The directory names, as shown below, cannot contain any spaces.

   `\<ManagementServerCDs>\oracle`
   (Copy the Oracle 10g installation files found on the Oracle DVD to this directory.)

   `\<ManagementServerCDs>\srm`
   (Copy the Storage Essentials for Windows installation files found on the Storage Essentials CD to this directory.)

   `\<ManagementServerCDs>\cimext1`
   (Copy the CIM Extensions CD 1 installation files to this directory.)

`\<ManagementServerCDs>\cimext2`
(Copy the CIM Extensions CD 2 installation files to this directory. Note that the CIM Extensions CD 2 is not required as part of this Storage Essentials management server installation.)

b. Double-click **setup.exe** in the `srm` directory to which you copied the Storage Essentials installation files.

The Storage Essentials for Windows installation wizard starts and the Welcome screen is displayed.

3. Click **Next** to continue. The Getting Started screen is displayed. Click the hyperlinks to review the requirements for getting started with the installation.
4. Click **Next** to continue.

   The Storage Essentials for Windows installation wizard scans the server to determine if this is a new installation or an upgrade and the Installation Options screen is displayed.
5. By default the **HP Storage Essentials and HP Systems Insight Manager (HP SIM) on Separate Servers** option is selected. If the option is not selected, then click this option.

   IMPORTANT: Valid locations must be entered on the Installation Options screen. Path information can only contain the following characters: A-z, 0-9, hyphen, underscore, period, back slash. Storage Essentials, HP SIM, and the Oracle database paths cannot contain spaces. Drive letters must be fixed drives.

6. Enter the fully qualified domain name or the IP Address for the HP SIM server (the server on which you previously installed HP SIM in Step 2) in the **HP SIM server name <FQDN> or IP Address** box.
7. Enter the path or browse to the directory in which you want to install Storage Essentials in the **HP Storage Essentials installation location** box. The installation path must be basic ASCII alphanumeric characters, no spaces, no international characters, and no double-byte characters.
8. Enter or browse to the directory in which you want to install the Oracle database and click **Next**. A dialog box is displayed and the Storage Essentials installation wizard prompts you to verify that HP SIM is installed and running on the remote server that you specified on this Installation Options screen before you can proceed to the next Storage Essentials installation wizard screen.
9. You must manually verify that you can access the remote HP Systems Insight Manager on the remote server you specified and click **OK** to continue. The Verify System Requirements screen is displayed.
10. Scroll through the list of requirements on the Verify System Requirements screen and make any system changes necessary. If you see a warning in the Ports Availability requirement you need to check the port assignments to be sure that the ports listed are not currently in use and make any changes that are necessary. See the support matrix to verify the requirements listed below:
    - **Current User Account** — The account you use to install must have Windows Administrator privileges or the installation will stop.

- **Memory** — The minimum RAM requirement varies depending on your installation option:
  - When HP SIM and Storage Essentials are installed on separate servers the minimum RAM requirement for the Storage Essentials server is 4 GB with 6 GB recommended.
  - When HP SIM and Storage Essentials are installed on the same server together the minimum RAM requirement for the Storage Essentials server is 6 GB with 8 GB recommended.

  NOTE: If the minimum amount of RAM is close to the requirement, the installation wizard continues.

- **Physical Address Extension (PAE)** — PAE is a Windows setting to utilize amounts of RAM greater than 4 GB on certain versions of Windows. See your Windows documentation for more information about PAE settings. The installation or upgrade continues regardless of PAE.
- Disk Storage (typical installation) — Depends on the following:
  - With ARCHIVING and RMAN backup off: minimum disk space: 100 GB, recommended disk space: 200 GB.
  - With ARCHIVING and RMAN backup on: minimum disk space: 200 GB, recommended disk space: 350 GB.

    The installation or upgrade will not continue if the disk space requirements are not met.
- **Operating System** — Windows 2003 Server SP1, SP2, R2, R2 SP2. The Storage Essentials installation or upgrade will not continue if the operating system requirement is not met.
- **Processor —** A dual Intel XEON (or AMD equivalent) 3.4 GHz or higher CPU is required. If the CPU is close to the requirement, the installation wizard continues.
- DNS Resolution — The installation wizard verifies the IP address and DNS name of the server using nslookup. If nslookup is not successful, the installation will still continue.

  IMPORTANT: DNS Resolution failure will prevent the product from running successfully. See the following topic in the troubleshooting chapter if the DNS Resolution requirement fails: "Reverse Lookup Failed" Message (Windows only), page 382.

- **Port Availability —** The management server requires the following ports to be available:
  - 80
  - 162
  - 443
  - 1098–1120
  - 4444
  - 4445
  - 4763
  - 5962–5988

- 8009
- 8083
- 8093

If you see a warning in the Ports Availability requirement you need to check to be sure that the ports listed are not currently in use and make any changes that are necessary. Be aware that the installation will continue even if a required port is not available.

NOTE: During upgrades, the Port Availability check may falsely indicate that the port for the management server is currently in use. When you check the port, you see that it is reserved by the management server and you can therefore safely ignore the warning.

11. Click **Next** and the Storage Essentials installation wizard proceeds to its HP Systems Insight Manager Service Account Credentials screen. The fully qualified domain name or the IP Address that you entered in the Installation Options screen for the designated server on which HP SIM is installed is automatically displayed in the HP SIM Server box.
12. Enter the following on the HP Systems Insight Manager Service Account Credentials screen and click **Next**:
    - The user account name of the HP SIM server that you installed in "Step 2 – (Required for Separate Server Installations Only) Manually Install HP Systems Insight Manager" on page 17.
    - The password for the HP SIM server and also verify the password.
    - The Domain name of the domain on which the HP SIM server resides.

    The Installation Summary screen is displayed.
13. Verify the components that will be installed, use the Previous button to make any changes and click **Install** when you are ready to install Storage Essentials and the other required software components listed on the screen. The Storage Essentials installation wizard automatically installs the components on the Storage Essentials server starting with the Oracle 10g Standard Edition database.

    IMPORTANT: If you decide to cancel the Storage Essentials installation before it has finished, the installation wizard must first complete the installation of the current component and will prompt you to click **Yes** to cancel the installation or **No** to continue the installation after the current component installation is finished. If you cancel and then resume the installation at a later time, the installation wizard will continue the installation from where it stopped when you cancelled.
14. The Storage Essentials installation wizard prompts you to verify that the remote HP SIM server you installed previously in Step – 2 is running when the Storage Essentials installation wizard finishes installing the Oracle component. Do not click **OK** until you have verified that the remote HP SIM server is running.

Step 4 – Verify that HP SIM is Running on the Remote Server

Before the Storage Essentials installation wizard installs the HP SIM Connector component, you must verify that HP SIM is currently running on the remote HP SIM server you specified in the Installation Options screen. The Storage Essentials installation wizard automatically installs the HP SIM Connector on the Storage Essentials server and the HP SIM Connector must be able to connect to the remote HP SIM server in order for the integrated Storage Essentials and HP SIM installation to be successful. Follow these steps:

1. Manually access the remote HP SIM server over the network.
2. Verify that you can log in to HP SIM on that server.

Step 5 – Complete the Storage Essentials Installation

Continue the Storage Essentials installation after verifying that the HP SIM server is running and is accessible on the network.

1. Go back to the Storage Essentials server and click **OK** to dismiss the dialog box that prompts you to verify your HP SIM server is running.

   The Storage Essentials installation wizard will then install the HP SIM Connector component on the Storage Essentials server.

   There is a two minute delay after you click OK on the Storage Essentials server while the HP SIM Connector is installed on the Storage Essentials server and the Storage Essentials installation wizard then connects to the specified HP SIM server and automatically installs the HP SIM Connector component on the HP SIM server.

   The Storage Essentials menu items are added to the HP SIM menus and screens when the Storage Essentials installation wizard automatically installs the HP SIM Connector component on the HP SIM server.
2. Click **Next** on the Status screen. The Storage Essentials Installation Complete screen is displayed.

NOTE: If the HP SIM Connector fails, re-start the Storage Essentials installation wizard. The Storage Essentials installation wizard will detect the Storage Essentials and Oracle components and will automatically display the HP SIM Connector screen allowing you to re-install the HP SIM Connector. If the issue continues, contact Customer Support.

3. Copy the Unique Client ID (UID) number displayed on the Installation Complete screen and paste it into a text document or make a note of it. You need the UID number to obtain a License Key.

IMPORTANT: You must have your license ready to import before you can set up discovery using the HP Systems Insight Manager's First Time wizard. If you do not import your Storage Essentials license before setting up discovery using the HP SIM First Time User wizard, Storage Essentials cannot run its discovery and the Storage Essentials discovery will fail.

4. Click **Finish** accepting the default setting: **Yes, reboot the system now**. The Storage Essentials server must be rebooted.

Step 6 – Configure Browser Settings

Configure your browser settings for HP SIM and Storage Essentials to function properly. See the support matrix for your edition for a list of supported browsers. Refer to your browser's documentation for details.

1. Verify that Java and JavaScript are installed and enabled.
2. Configure the browser to accept all cookies.
3. Turn off popup blocking.
4. Verify that SSL 3.0 or TLS 1.0 is enabled.
   - For Internet Explorer: **Tools** > **Internet Options** > **Advanced** > **Security**
   - For Firefox: **Tools** > **Options** > **Advanced**

Step 7 – Browse to the HP SIM Home Page

1. Browse to HP Systems Insight Manager Home Page and wait until HP SIM is fully started. HP SIM has fully started when you can bring up the Systems Insight Manager Home page. See the HP SIM documentation for help with starting SP SIM.
2. Start the HP Storage Essentials (AppStorManager) service and change to Automatic.
3. You should now be able to access HP SIM and Storage Essentials from a web browser using the URL https://<FQDN of localhost>:50000
   (for example https://example.domain.com:50000). The host name must be fully qualified. HP SIM is displayed in the browser window and you are prompted to enter the user name and password for HP SIM.

NOTE: Do not use the Systems Insight Manager Homepage icon placed on the desktop after installation. This icon will use localhost to browse to HP SIM. A best practice is to save a bookmark for https://<FQDN>:50000 to the desktop, edit the properties, change icon, and browse to <install dir>:\HP\Systems Insight Manager\HPSIM.ico.

4. Supply the login credentials for the user that was used to install HP SIM. HP SIM launches and the Storage Essentials menus are included on the HP SIM menus.
5. Disregard the HP SIM First Time User wizard until you have imported your Storage Essentials license following the instructions in the next step.

IMPORTANT: Be sure to apply your Storage Essentials license before setting up discovery with the HP SIM First Time User wizard. See Step 8 – Obtain and Apply a Storage Essentials License Key Before Setting Up Discovery on HP SIM, page 26.

Step 8 – Obtain and Apply a Storage Essentials License Key Before Setting Up Discovery on HP SIM

If you see the HP Systems Insight Manager First Time User wizard, do not click the **Do not automatically display this dialog again** check box. You must first import your Storage Essentials license. Without the license, Storage Essentials cannot start and the HP SIM discovery will fail. After you import the Storage Essentials license, restart the HP SIM First Time wizard (**Options** > **First Time Wizard** from HP SIM) to set up discovery. Follow these steps to obtain and import your Storage Essentials license:

1. Go to http://webware.hp.com and use the generate password option with the UID (copied from the Installation Complete screen) and the HP Order ID (found on the entitlement certificate) to create a permanent license key.
2. Import the license key:
   a. Log in to HP SIM on the remote HP SIM server.
   b. Click the **Security** menu. Click **Deploy** > **License Manager** > **Storage Essentials** > **Manage Storage Essentials Keys** in HP Systems Insight Manager.
   c. Click **Licenses** from the menu.
   d. Click the **Import License File** button.
   e. Click the **Browse** button.

      You are shown the file system of the computer being used to access the management server.
   f. Select the license file.
   g. Click **OK**.

Step 9 – Copy Your CIM Extensions to the HP SIM Server

As a best practice HP recommends copying the CIM extensions included on the CIM extensions CD to the HP SIM server. The HP SIM software component includes a tool called the CIM Extension Management tool which can be used to install your CIM extensions on multiple hosts in batch mode.

See "Deploying and Managing CIM Extensions" on page 181.

Step 10 – Check for and Install any Required Service Packs and Hot Fix Files

1. Contact your Sales Engineer to obtain the latest service packs and hot fix files for Storage Essentials and HP SIM.
2. Install the latest required service packs and hot fix files for Storage Essentials and HP Systems Insight Manager. See the Service Pack release notes for installation instructions.

Step 11 – Install Your CIM Extensions and Set Up Discovery

Before you can discover all of the elements (systems) on your network, you must install the CIM extensions that were copied to the management server during the installation as mentioned in the previous step. For more information about CIM extensions and setting up discovery, see the following chapters:

See "Deploying and Managing CIM Extensions" on page 181.

See "Discovery Steps" on page 109.

Installing Storage Essentials and HP SIM for Windows on the Same Server

Complete the following steps to install the Storage Essentials management server and HP SIM for Windows on the same server.

Step 1 – Read the Support Matrix and Release Notes

Read the support matrix and the release notes to make sure the server on which you are installing the Storage Essentials management server meets or exceeds the requirements. The installation wizard provides a link to these documents accessible on each screen (**Documentation** > **Support Matrix** or **Release Notes**). Additionally, be sure to read the important information in "Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)" on page 9.

Step 2 – Log On to the Windows Server

Create a new account or log in to an existing account on the Windows system on which you are installing HP Storage Essentials and HP Systems Insight Manager that has Administrator privileges providing the following permissions:

- Ability to log on as a service
- Ability to create a token object
- Ability to replace a process level token

Step 3 – Start the Storage Essentials for Windows Installation Wizard

Do not install the Oracle database separately. See "Installation/Upgrade Process is Now Automated" on page 8 for important information about installing the Oracle database.

IMPORTANT: The drive on which you install the management server must be NTFS format or the installation wizard will fail.

1. Verify the following:
   - The designated Storage Essentials server meets or exceeds the requirements listed in the Pre-installation Checklist (Installations and Upgrades), page 8 and in the support matrix for your edition.
   - The file system format on the Storage Essentials server is NTFS. The Storage Essentials installation wizard will display an error message if the file system is not NTFS.
2. Start the Storage Essentials installation wizard using one of the following options:

To install from the CDs do the following:

a. Put the Storage Essentials CD in the CD drive of the designated Storage Essentials server. The Storage Essentials installation wizard program should start automatically.

b. If it does not start, double-click **setup.exe** found in the `root` directory on the Storage Essentials CD.

To install from a network or local hard drive, do the following:

a. Create the following directory structure on the designated drive from which you will install Storage Essentials:

IMPORTANT: The directory names, as shown below, cannot contain any spaces.

`\<ManagementServerCDs>\oracle`
(Copy the Oracle 10g installation files found on the Oracle DVD to the Oracle directory you created.)

`\<ManagementServerCDs>\srm`
(Copy the Storage Essentials for Windows installation files found on the Storage Essentials CD to the srm directory you created.)

`\<ManagementServerCDs>\hpsim`
(Copy the HP Systems Insight Manager installation files found on the HP SIM CD to the hpsim directory you created.)

`\<ManagementServerCDs>\cimext1`
(Copy the CIM Extensions CD 1 installation files to the cimext1 directory you created.)

`\<ManagementServerCDs>\cimext2`
(Copy the CIM Extensions CD 2 installation files to the cimext2 directory you created. Note that the CIM Extensions CD 2 is not required as part of the Storage Essentials installation.)

b. Double-click **setup.exe** in the `srm` directory to which you copied the Storage Essentials installation files.

IMPORTANT: The directory in which you install the management server must have write access for the local Administrators group. Be aware that installing the management server in a directory created by another program (for example: the Proliant Support Pack) is not recommended.

3. Read the information on the Welcome screen. Click the hypertext links on the screen to learn about service packs and other important requirements and click **Next** when you are ready to continue.

   The System Inspection screen is displayed briefly while the installation wizard checks the system and the Getting Started screen is displayed giving you an overview of the installation process.
4. Click **Next** to continue. The Installation Options screen is displayed.
5. Click the **Storage Essentials and HP SIM on the same server** option.

   Choose the installation locations. Installing HP Storage Essentials and HP Systems Insight Manager on the same server allows you to install all of the software components on one designated system. The software components include:
   – HP Storage Essentials
   – HP Systems Insight Manager
   – Oracle 10g Standard Edition database
   – HP SIM Connector
   – CIM Extension Management tool

   IMPORTANT: Valid locations must be entered on the Installation Options screen. Path information can only contain the following characters: A-z, 0-9, hyphen, underscore, period, back slash. Storage Essentials, HP SIM, and the Oracle database paths cannot contain spaces. Drive letters must be fixed drives.

   Choose the installation directory where you want to install the Oracle database for the Storage Essentials management server. Choose a drive with enough dedicated disk space for the Oracle database and its backup files. The disk space requirements are dependent on the size of the SAN you are managing.

   If the system does not meet the disk space requirements for the Oracle database used to store the management server data, the installation stops and prompts you to allocate the required disk space.
6. Click **Next**. The Service Account Credentials screen is displayed. Enter the user name and password for the HP SIM service account and the Domain name of the domain on which you are installing Storage Essentials and click **Next**. Click the Help button for more information about the service account credentials if needed.

NOTE: In Storage Essentials, the HP SIM Administrator will be assigned the HP Storage Essentials Administrator role (Domain Admin). See "About Security for the Management Server" on page 349 for more information.

The installation wizard scans the system to verify that it meets the requirements specified in the support matrix and the Verify System Requirements screen is displayed showing the current status of the system.

7. Scroll through the list of system requirements to see if you need to make any changes to your system and click **Next**. Once you click Next, the Summary screen is displayed.

NOTE: See "Pre-installation Checklist (Installations and Upgrades)" on page 8 if you need help making changes to meet basic system requirements. See "Troubleshooting Installation/Upgrade" on page 379 for additional information.

8. Scroll through the list of requirements on the Verify System Requirements screen and make any system changes necessary. If you see a warning in the Ports Availability requirement you need to check the port assignments to be sure that the ports listed are not currently in use and make any changes that are necessary. See the support matrix to verify the requirements listed below:
   - **Current User Account —** The account you use to install must have Windows Administrator privileges or the installation will stop.
   - **Memory** — The minimum RAM requirement varies depending on your installation option:
     - When HP SIM and Storage Essentials are installed on separate servers the minimum RAM requirement for the Storage Essentials server is 4 GB with 6 GB recommended.
     - When HP SIM and Storage Essentials are installed on the same server together the minimum RAM requirement for the Storage Essentials server is 6 GB with 8 GB recommended.

   NOTE: If the minimum amount of RAM is close to the requirement, the installation wizard continues.

   - **Physical Address Extension (PAE)** — PAE is a Windows setting to utilize amounts of RAM greater than 4 GB on certain versions of Windows. See your Windows documentation for more information about PAE settings. The installation or upgrade continues regardless of PAE.
   - Disk Storage (typical installation) — Depends on the following:
     - With ARCHIVING and RMAN backup off: minimum disk space: 100 GB, recommended disk space: 200 GB.
     - With ARCHIVING and RMAN backup on: minimum disk space: 200 GB, recommended disk space: 350 GB.

       The installation or upgrade will not continue if the disk space requirements are not met.

    - **Operating System** — Windows 2003 Server SP1, SP2, R2, R2 SP2. The Storage Essentials installation or upgrade will not continue if the operating system requirement is not met.
    - **Processor —** A dual Intel XEON (or AMD equivalent) 3.4 GHz or higher CPU is required. If the CPU is close to the requirement, the installation wizard continues.
    - DNS Resolution — The installation wizard verifies the IP Address and DNS name of the server using nslookup. If nslookup is not successful, the installation will still continue.

    IMPORTANT: DNS Resolution failure will prevent the product from running successfully. See the following topic in the troubleshooting chapter if the DNS Resolution requirement fails: "Reverse Lookup Failed" Message (Windows only), page 382.

- **Port Availability —** The management server requires the following ports to be available:
    - 80
    - 162
    - 443
    - 1098–1120
    - 4444
    - 4445
    - 4763
    - 5962–5988
    - 8009
    - 8083
    - 8093

  If you see a warning in the Ports Availability requirement you need to check to be sure that the ports listed are not currently in use and make any changes that are necessary. Be aware that the installation will continue even if a required port is not available.

    NOTE: During upgrades, the Port Availability check may falsely indicate that the port for the management server is currently in use. When you check the port, you see that it is reserved by the management server and you can therefore safely ignore the warning.

9. Click **Install** after reviewing the components that will be installed. Click **Previous** if you need to make any changes before installing the management server files. Once you click the Install button, the Oracle installation for the management server begins and the Command Prompt window is displayed showing the status of the Oracle installation. The management server installation wizard Status screen is displayed in the background.

NOTE: Because you are installing Storage Essentials and HP Systems Insight Manager on the same server, the CIM extension files are copied to the management server so that you can install the extensions on the hosts in your network at a later time. The CIM extensions are not installed, only copied to the management server during this installation.

If you click **Cancel** during the installation, the installation wizard completes the installation of the current component before stopping. Once the component installation is complete, the installation wizard prompts you to confirm that you want to cancel. Click **Yes** to cancel or **No** to continue with the installation.

If you are installing the management server from the CD set, you are prompted to insert the CDs in the required order of installation indicated by the installation wizard screens.

10. Click **Next** when all components are installed. The Installation Complete screen is displayed.
11. If you see a Unique Client ID number on the Installation Complete screen, copy the number and complete "Step 4 – Obtain a License Key (Required to Start the Management Server for the First Time)" on page 32.

    If your product allows honorary licensing, you will not see the Unique Client ID in which case, you must select the restart the management server option and click **Done**.

Step 4 – Obtain a License Key (Required to Start the Management Server for the First Time)

See your product invoice for important information about licensing. If you are required to import a license, copy your Unique Client ID number and follow the instructions in your product invoice documentation to obtain and apply your license key.

IMPORTANT: You must have your license ready to import before you can set up discovery using the HP Systems Insight Manager's First Time wizard. If you do not import your Storage Essentials license before setting up discovery using the HP SIM First Time wizard, Storage Essentials cannot run its discovery and the Storage Essentials discovery fails.

If you are installing Storage Essentials the management server for the first time and your product requires a license, you must obtain a license key to start and run the product. If you see the HP Systems Insight Manager First Time wizard, do not click the **Do not automatically display this dialog again** check box. After you import the Storage Essentials license, restart the HP SIM First Time wizard (**Options** > **First Time Wizard** from HP SIM). Follow these steps to obtain and import your Storage Essentials license:

1. Copy (Ctrl + C) the Unique Client ID (UID) displayed on the Installation Complete screen.
2. Follow the instructions for obtaining your license key in your product invoice documentation. Go to http://webware.hp.com and use the generate password option with the UID and HP Order ID (found on the entitlement certificate) to create a permanent license key.
3. Import the license key:
    a. Click **Deploy** > **License Manager** > **Storage Essentials** > **Manage Storage Essentials Keys** in HP Systems Insight Manager.

b. Click the **Import License File** button.

c. Click the **Browse** button.

   You are shown the file system of the computer being used to access the management server.

d. Select the license file.

e. Click **OK**.

IMPORTANT: See "Checking Installation Log Files" on page 380 for more information about installations and upgrades.

Step 5 – Configure Browser Settings

Configure your browser settings for HP SIM and Storage Essentials to function properly. See the support matrix for your edition for a list of supported browsers. Refer to your browser's documentation for details.

1. Verify that Java and JavaScript are installed and enabled.
2. Configure the browser to accept all cookies.
3. Turn off popup blocking.
4. Verify that SSL 3.0 or TLS 1.0 is enabled.
   - For Internet Explorer: **Tools** > **Internet Options** > **Advanced** > **Security**
   - For Firefox: **Tools** > **Options** > **Advanced**

Step 6 – Browse to the HP SIM Home Page

1. Browse to HP Systems Insight Manager Home Page and wait until HP SIM is fully started. HP SIM has fully started when you can bring up the Systems Insight Manager Home page.
2. Start the HP Storage Essentials (AppStorManager) service and change to Automatic.
3. You should now be able to access HP SIM and Storage Essentials from a web browser using the URL https://<FQDN of localhost>:50000
   (for example https://example.domain.com:50000). The host name must be fully qualified.

   NOTE: Do not use the Systems Insight Manager Homepage icon placed on the desktop after installation. This icon will use localhost to browse to HP SIM. A best practice is to save a bookmark for https://<FQDN>:50000 to the desktop, edit the properties, Change icon, and browse to <install dir>:\HP\Systems Insight Manager\HPSIM.ico.

4. Supply the login for the user that was used to install HP SIM.

IMPORTANT: Be sure to apply your Storage Essentials license key before setting up discovery with the HP SIM First Time User wizard. See "Step 4 – Obtain a License Key (Required to Start the Management Server for the First Time)" on page 32.

Step 7 – Check for Required Service Packs and Hot Fix Files

Check with your Sales Engineer to obtain and install the latest required service packs and hot fix files for Storage Essentials and HP Systems Insight Manager.

Step 8 – Install Your CIM Extensions and Set Up Discovery

Before you can discover all of the elements (systems) on your network, you must install the CIM extensions that were copied to the management server during the installation. See the following chapters:

See "Deploying and Managing CIM Extensions" on page 181.

See "Discovery Steps" on page 109.

If Storage Essentials Fails to Start

If the credentials for the HP SIM server are entered incorrectly, you might not see the Storage Essentials options on the HP SIM menus and/or Storage Essentials might fail to start when you access Storage Essentials options from the HP SIM menus. Re-install the SIM Connector if you see either of these issues following these steps:

1. Put the Storage Essentials CD in the CD drive of the Storage Essentials server. The installation wizard starts automatically, determines that all components are installed, and automatically displays the HP Systems Insight Manager Service Account Credentials screen.
2. Verify that HP SIM is running and accessible if Storage Essentials and HP SIM are installed on separate servers (log in to HP SIM on the separate HP SIM server).
3. Return to Storage Essentials and enter the correct credentials for the HP SIM server and click **OK**. The SIM Connector is installed and the connection between HP SIM and Storage Essentials is successful as long as the HP SIM credentials you enter in the Re-install Connector screen are correct.

Installing the Standalone Version of Storage Essentials for Windows

Follow the steps in this section to install Storage Essentials for Windows using the standalone installation option. The standalone version of Storage Essentials consists of the following software components:

- Storage Essentials (Build 6.0)
- Oracle 10g for Storage Essentials (Build 6.0)

- CIM Extension files (Build 6.0—Common Information Module files that you install on the hosts and other network elements you want to manage and for which you want to automate discovery)
- CIM Extension Management tool for installing some of the supported CIM extensions in batch mode, remotely, onto multiple hosts.

Step 1 – Read the Support Matrix and Release Notes

Read the support matrix and the release notes to make sure the server on which you are installing the Storage Essentials management server meets or exceeds the requirements. The installation wizard provides a link to these documents accessible on each screen (**Documentation** > **Support Matrix** or **Release Notes**). Additionally, be sure to read the important information in "Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)" on page 9.

Step 2 – Log On to the Windows Server

Create a new account or log in to an existing account on the Windows system on which you are installing HP Storage Essentials that has Administrator privileges providing the following permissions:

- Ability to log on as a service
- Ability to create a token object
- Ability to replace a process level token

Step 3 – Start the Storage Essentials for Windows Installation Wizard

Do not install the Oracle database separately. See "About the New Storage Essentials for Windows Installation Options" on page 14 for important information about installing the Oracle database.

IMPORTANT: The drive on which you install the management server must be NTFS format or the installation wizard will fail.

1. Verify the following:
   - The designated Storage Essentials server meets or exceeds the requirements listed in the Pre-installation Checklist (Installations and Upgrades), page 8 and in the support matrix for your edition.
   - The file system format on the Storage Essentials server is NTFS. The Storage Essentials installation wizard will display an error message if the file system is not NTFS.

IMPORTANT: The directory in which you install the management server must have write access for the local Administrators group. Be aware that installing the management server in a directory created by another program (for example: the Proliant Support Pack) is not recommended.

2. Start the Storage Essentials installation wizard using one of the following options:

   To install from the CDs do the following:

a. Put the Storage Essentials CD in the CD drive of the designated Storage Essentials server. The Storage Essentials installation wizard program should start automatically.

b. If it does not start, double-click **setup.exe** found in the `root` directory on the Storage Essentials CD.

To install from a network or local hard drive, do the following:

a. Create the following directory structure on the designated drive from which you will install Storage Essentials:

IMPORTANT: The directory names, as shown below, cannot contain any spaces.

`\<ManagementServerCDs>\oracle`
(Copy the Oracle 10g installation files found on the Oracle DVD to the Oracle directory you created.)

`\<ManagementServerCDs>\srm`
(Copy the Storage Essentials for Windows installation files found on the Storage Essentials CD to the `srm` directory you created.)

`\<ManagementServerCDs>\cimext1`
(Copy the CIM Extensions CD 1 installation files to the cimext1 directory you created.)

`\<ManagementServerCDs>\cimext2`
(Copy the CIM Extensions CD 2 installation files to the cimext2 directory you created. Note that the CIM Extensions CD 2 is not required as part of the Storage Essentials installation.)

b. Double-click **setup.exe** in the `srm` directory to which you copied the Storage Essentials installation files.

IMPORTANT: The directory in which you install the management server must have write access for the local Administrators group. Be aware that installing the management server in a directory created by another program (for example: the Proliant Support Pack) is not recommended.

3. Read the information on the Welcome screen. Click the hypertext links on the screen to learn about service packs and other important requirements and click **Next** when you are ready to continue.

   The System Inspection screen is displayed briefly while the installation wizard checks the system and the Getting Started screen is displayed giving you an overview of the installation process.
4. Click **Next** to continue. The Installation Options screen is displayed.
5. Click **Standalone Option: HP Storage Essentials only installation**.

6. Choose the installation location. You can change the installation location of the management server and the Oracle database if you prefer.

   IMPORTANT: Valid locations must be entered on the Installation Options screen. Path information can only contain the following characters: A-z, 0-9, hyphen, underscore, period, back slash. Storage Essentials and the Oracle database paths cannot contain spaces. Drive letters must be fixed drives.

   Choose the installation directory where you want to install the Oracle database for the Storage Essentials management server. Choose a drive with enough dedicated disk space for the Oracle database and its backup files. The disk space requirements are dependent on the size of the SAN you are managing.

7. Click **Next**. The installation wizard scans the system to verify that it meets the requirements specified in the support matrix and the Verify System Requirements screen is displayed showing the current status of the system.

   If the system does not meet the disk space requirements for the Oracle database used to store the Storage Essentials management server data, the installation stops and prompts you to allocate the required disk space.

8. Scroll through the list of system requirements to see if you need to make any changes to your system and click **Next**. Once you click Next, the Summary screen is displayed.

   NOTE: See "Pre-installation Checklist (Installations and Upgrades)" on page 8 if you need help making changes to meet basic system requirements. See "Troubleshooting Installation/Upgrade" on page 379 for additional information.

   If you see a warning in the Ports Availability requirement you need to check the port assignments to be sure that the ports listed are not currently in use and make any changes that are necessary. See the support matrix to verify the requirements listed below:

   - **Current User Account —** The account you use to install must have Windows Administrator privileges or the installation will stop.
   - **Memory** — The minimum RAM requirement is 4 GB with 6 GB recommended.

     NOTE: If the minimum amount of RAM is close to the requirement, the installation wizard continues.

   - **Physical Address Extension (PAE)** — PAE is a Windows setting to utilize amounts of RAM greater than 4 GB on certain versions of Windows. See your Windows documentation for more information about PAE settings. The installation or upgrade continues regardless of PAE.
   - Disk Storage (typical installation) — Depends on the following:
     - With ARCHIVING and RMAN backup off: minimum disk space: 100 GB, recommended disk space: 200 GB.

    - With ARCHIVING and RMAN backup on: minimum disk space: 200 GB, recommended disk space: 350 GB.

      The installation or upgrade will not continue if the disk space requirements are not met. See the *HP Storage Essentials 6.0 SRM User Guide* for information about the archiving and RMAN backup features.
  - **Operating System** — Windows 2003 Server SP1, SP2, R2, R2 SP2. The Storage Essentials installation or upgrade will not continue if the operating system requirement is not met.
  - **Processor —** A dual Intel XEON (or AMD equivalent) 3.4 GHz or higher CPU is required. If the CPU is close to the requirement, the installation wizard continues.
  - DNS Resolution — The installation wizard verifies the IP address and DNS name of the server using nslookup. If nslookup is not successful, the installation will still continue.

  IMPORTANT: DNS Resolution failure will prevent the product from running successfully. See the following topic in the troubleshooting chapter if the DNS Resolution requirement fails: "Reverse Lookup Failed" Message (Windows only), page 382.

- **Port Availability —** The management server requires the following ports to be available:
  - 80
  - 162
  - 443
  - 1098–1120
  - 4444
  - 4445
  - 4763
  - 5962–5988
  - 8009
  - 8083
  - 8093

  If you see a warning in the Ports Availability requirement you need to check to be sure that the ports listed are not currently in use and make any changes that are necessary if there are any port conflicts. Be aware that the installation will continue even if a required port is not available.

  NOTE: During upgrades, the Port Availability check may falsely indicate that the port for the management server is currently in use. When you check the port, you see that it is reserved by the management server and you can therefore safely ignore the warning.

9. Click **Install**. Click **Previous** if you need to make any changes before installing the management server files. Once you click the Install button, the Oracle installation for the management server begins and the Command Prompt window is displayed showing the status of the Oracle

installation. The Storage Essentials installation wizard Status screen is displayed in the background.

If you click **Cancel** during the installation, the installation wizard completes the installation of the current component before stopping. Once the component installation is complete, the installation wizard prompts you to confirm that you want to cancel. Click **Yes** to cancel or **No** to continue with the installation. If you cancel, you can resume the installation by starting the Storage Essentials installation wizard `setup.exe` file at a later time. The installation wizard will resume its installation from where you cancelled.

IMPORTANT: The CIM extension files are copied to the management server so that you can install the extensions on the hosts in your network at a later time. The CIM extensions are not installed, only copied to the management server during this installation.

If you are installing the management server from the CD set, you are prompted to insert the CDs in the required order of installation indicated by the installation wizard screens.

10. Click **Next** when all components are installed. The Installation Complete screen is displayed.
11. Copy the Unique Client ID number on the Installation Complete screen and complete "Step 4 – Obtain a License Key (Required to Start the Management Server for the First Time)" on page 32.

IMPORTANT: See "Checking Installation Log Files" on page 380 for details about accessing the Storage Essentials installation log files.

Step 4 – Obtain a License Key (Required to Start the Management Server for the First Time)

See your product invoice for important information about licensing. If you are required to import a license, copy your Unique Client ID number and follow the instructions in your product invoice documentation to obtain and apply your license key.

If you are installing Storage Essentials for the first time you must obtain a license key to start and run the product. Follow these steps to obtain and import your Storage Essentials license:

1. Copy (Ctrl + C) the Unique Client ID (UID) displayed on the Installation Complete screen.
2. Follow the instructions for obtaining your license key in your product invoice documentation. Go to http://webware.hp.com and use the generate password option with the UID and HP Order ID (found on the entitlement certificate) to create a permanent license key.
3. Import the license key:
   - **a.** Click the **Security** menu.
   - **b.** Click **Licenses** from the menu.
   - **c.** Click the **Import License File** button.
   - **d.** Click the **Browse** button.

     You are shown the file system of the computer being used to access the management server.

e. Select the license file.

f. Click **OK**.

Step 5 – Check for Required Service Packs and Hot Fix Files

Check with your Sales Engineer to obtain and install the latest required service packs and hot fix files for Storage Essentials.

Step 6 – Install Your CIM Extensions and Set Up Discovery

Before you can discover elements (systems) on your network, you must install the CIM extensions that were copied to the management server during the installation. See the following chapters:

See "Deploying and Managing CIM Extensions" on page 181.

See the Discovery Steps section in the Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries chapter for details on setting up disocvery.

Upgrading the Storage Essentials for Windows Management Server (Contact Your Account Representative Before Upgrading)

This section provides details about upgrading the Storage Essentials for Windows management server.

IMPORTANT: Please contact your Account Representative for upgrades. Upgrading requires assistance from HP Services.

Keep in Mind the Following

- Before upgrading, verify that the server meets the requirements listed in the "Pre-installation Checklist (Installations and Upgrades)" on page 8.
- Refer to the release notes for upgrade path and late breaking information about upgrading the management server. See the Upgrade section in the release notes.
- Complete the upgrade and its subsequent steps in one session, which may take several hours depending on your network configuration. Completing the steps over several sessions will result in incomplete data until all steps have been completed.

Considerations Before Upgrading

Before you upgrade, consider the following:

- **Brocade SMI-S Switches**
  The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and with this release of the management server, the Brocade Fabric Access API provider is no longer supported. After upgrading, any Brocade switches that are managed by the Brocade API provider will be quarantined. Historical data will be retained by the API-managed Brocade switches, but you will not be able to run Discovery Data Collection on these switches until they

are migrated to the Brocade SMI-S provider (note that the Brocade SMI-S provider is called the SMI-Agent in the Brocade documentation). Data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or to gather port performance statistics through the Brocade switch.

Before the Brocade API-managed switches can be migrated to SMI-S, you must first download, install, and configure the Brocade SMI-S provider on the management server. For details on downloading, installing, and configuring the Brocade SMI-A agent provider, see "Migrate Your Brocade Switches to SMI-A" on page 50.

- **CIM Extensions**
  The latest build of the management server requires you to upgrade some of your CIM extensions. See "About Upgrading Your CIM Extensions" on page 189 for details.
- After you upgrade the management server, you are required to run Discovery Data Collection on all new and existing managed elements. This allows the software to gather any new data that is associated with the new features available in the latest release.
- **Windows hosts using SecurePath**
  SecurePath information is not retrieved from legacy CIM extensions.
- **Backup Manager Hosts**
  After you upgrade, you need to rediscover backup details. Make note of your Backup Manager hosts. Refer to Managing Backups in the user guide for help with viewing a list of Backup hosts.
- The following elements are not supported even though they were supported in Service Pack 4, Build 5.1 of the management server:
  - Cisco switches with firmware versions earlier than 3.1.x for switches discovered through SMI-S. You need to upgrade to version 3.2.(2c) if you want to discover the Cisco switches through SMI-S.
  - Brocade SMI-A versions prior to 120.6.0a. You need to upgrade to at least version 120.6.0a.
- **Oracle Upgrade**

  This release of the management server is only compatible with Oracle 10g Standard Edition. During the upgrade process, Oracle 9i is automatically removed from the management server and Oracle 10g is automatically installed. Because Oracle 9i is removed during the upgrade to Oracle 10g, any customized Oracle passwords must be reset to the defaults. After the upgrade is successful it is strongly recommended that you change the Oracle passwords from the defaults using the Database Admin utility. See Database Passwords in the user guide for more information.

  IMPORTANT: Oracle passwords will be reset to their default values.

- **Determine What Kind of Data HP SIM Passes Storage Essentials**

  When devices are discovered in HP SIM, the information for the device that is passed from HP SIM to Storage Essentials is the IP address and any user credential information that has been entered within HP SIM. It is possible to have the DNS name instead of the IP Address passed from HP SIM to Storage Essentials by changing the **StorageEssentialsSendIPAddress** flag in the

HP SIM **globalsettings.props** file from `True` to `false`. This file can be found in the following directory on the HP SIM server:

```
[SIM_Installation_Directory]\config\globalsettings.props
```

- Windows 2000 is no longer supported. See the support matrix for your edition for complete information on supported Windows versions.
- After upgrading, hosts are managed directly from the application server, and will no longer be managed by our internal CIMOMs. Each host will be treated as its own discovery group; hosts will no longer be members of the built-in discovery groups (default, discovery group 1, etc). See "Managing Discovery Groups" on page 108 for more information.
- CLI clients earlier than the current revision are not supported.
- Any customizations to your CIMOMConfig.xml will not be preserved, because the file format has changed. The old file will be saved to <installation directory>\SavedData for reference. The customizations in the old CIMOMConfig.xml file must be manually merged into the file shipped with 6.0 and you must restart the management server before the customizations are applied to the updated management server.

- **Files backed up to %MGR_DIST%\SavedData**

  The upgrade will save data to %MGR_DIST%\SavedData. Do not delete this directory.

About Migrating Brocade Fabric Access API–Managed Switches to SMI-S After Upgrading

As noted earlier, The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and the Fabric Access API provider is no longer supported with this release of the management server. Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot complete Discovery Data Collection until you migrate these Brocade switches to the Brocade SMI Agent provider. See "Migrate Your Brocade Switches to SMI-A" on page 50 for instructions on downloading and installing the Brocade SMI-A provider.

About Changes to McDATA and Connectrix Switches After Upgrading

By default after upgrading, the management server is configured to use the SMI-S provider to manage and discover McDATA and Connectrix switches. The migration to SMI-S is not required for McDATA and Connectrix switches as it is with the Brocade Fabric Access API provider. The steps for changing the discovery settings for McDATA and Connectrix switches are explained in the discovery chapter.

About Resetting Archive Mode After Upgrading If You Use Automatic RMAN Backups

After upgrading to Oracle 10g, your Archive mode setting in the Database Admin Utility is reset to the default setting (No Archive Mode). If ARCHIVE MODE was enabled before upgrading, you must access the Database Admin Utility and re-enable Archive Mode in order to continue automatic RMAN backups. See the User Guide in the Documentation Center (**Help** > **Documentation Center**) for the steps.

About CIM Extensions and Backup Manager Hosts After Upgrading

Upgrade CIM extensions on servers with the following functionality:

- **Backup Manager Hosts** – Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Host must be at the same build number as the management server.

  When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host in order to continue to see backup data.
- **Windows hosts using SecurePath** – SecurePath information is not retrieved from legacy CIM extensions.

Upgrading the Management Server and HP SIM for Windows

Important Upgrade Requirements

- Do not upgrade Oracle separately. The upgrade steps have changed with this release of the product. The Storage Essentials management server upgrade wizard migrates and upgrades the Oracle database automatically along with the HP SIM Connector component and the Storage Essentials software. Be sure to start the Storage Essentials upgrade with the Storage Essentials CD–ROM (not the Oracle DVD).
- Exit all external utilities that use Oracle before starting the upgrade wizard.

Step 1 – Read the Support Matrix and Release Notes

Read the support matrix to make sure the servers on which you are upgrading the Storage Essentials management server meet or exceed the requirements. Management server requirements are listed on the **Mgr** platform tab of the support matrix. Also read the release notes for late breaking issues not covered in the installation guide. The release notes and support matrix can be found on the top-level of the management server CD and the CIM extension CDs. Additionally, see "Installation and Upgrade Requirements (Cannot Proceed with Install/Upgrade if Not Met)" on page 9.

Step 2 – Verify that You are Running Storage Essentials Build 5.1 Service Pack 4 or a Later Build 5.1 Service Pack

Verify that you have a working version of the Build 5.1 SP4 Storage Essentials management server and HP SIM Connector before upgrading to Build 6.0. Existing installations that are at Build 5.1 SP1, Build 5.1 SP2, or Build 5.1 SP3 must upgrade to Build 5.1 SP4 or later before upgrading to Build 6.0.

Step 3 – Save Configuration Files for the Global Change Management Business Tool

Make a copy of the configuration files saved through the Global Change Management Business Tool. The configuration files are not retained after you upgrade the product. These files are located in the advisors/saved-configuration area on the management server. Place these files back after the upgrade or re–install. If you do not use Global Change Management or do not wish to keep the old configurations, you can ignore this step.

Step 4 – Manually Upgrade HP SIM (Required Only When HP SIM is Running on a Separate Server)

Skip this step to manually upgrade HP SIM if Storage Essentials and HP SIM are installed on the same server. When the two are installed on the same server, the Storage Essentials installation wizard automatically checks for HP SIM and walks you through the upgrade. Upgrade HP SIM in this step if HP SIM is running on a separate server.

IMPORTANT: Stop the AppStorManager service prior to starting this step.

- If you are running an earlier version of HP SIM 5.1 on Windows in a dual server Storage Essentials and HP SIM configuration, you must manually upgrade HP SIM. Your integrated environment will be non-operational until after the completion of the Storage Essentials installation wizard and HP SIM Connector upgrade. The manual installation of HP SIM is only required if HP SIM and Storage Essentials are installed on separate servers.
- Install HP SIM 5.1 or later using the HP SIM CD–ROM included with your Storage Essentials software on the designated HP SIM server following the steps in this section.
- If HP Systems Insight Manager is installed on a separate server, you must first upgrade the HP SIM server separately to HP SIM 5.1. If you are running HP SIM 5.1 on the HP SIM server, you are not required to upgrade the HP SIM server. Continue to "Step 5 – Manually Export the Database" on page 45 if the HP SIM server is running version 5.1. Follow the steps below if HP SIM needs to be upgraded.

NOTE: Earlier versions of HP SIM (earlier than 5.1) run on the Oracle 9i database and are not compatible with this release of Storage Essentials.

1. Stop the AppStorManager service on the Storage Essentials server.
2. Log on to the HP SIM Windows server and put the HP SIM CD in the CD drive of the HP SIM server or double-click the HP SIM **setup.exe** file if you have copied the HP SIM installation files to a network or local drive.
3. Follow the instructions on the HP SIM upgrade screens. As a best practice, upgrade only the following components that are required to install and set up Storage Essentials:
   - System Management Homepage
   - HP Systems Insight Manager
4. Accept the default options on each HP SIM screen. You can optionally install/upgrade other HP SIM components at a later time by running the HP SIM CD again on the HP SIM server and following the instructions in the HP SIM documentation once the Storage Essentials installation is complete.
5. Reboot the HP SIM server when prompted at the end of the HP SIM installation.
6. Verify you can start the HP SIM service and log into HP SIM without any errors.
7. Log out of HP SIM.
8. Stop the HP SIM service.

Step 5 – Manually Export the Database

Manually export the database and create an image of the server.

Export the database and create an image as described in the following steps. Make sure you select Export HPSIM Schema so that HP System Insight Manager data is exported.

IMPORTANT: Make sure you save the backup in a directory structure that is not part of the management server installation directory.

1. Stop the services for HP SIM and HP Storage Essentials (AppStorManager) before you run the Database Admin Utility.
2. Use the Database Admin Utility to export your Oracle database. Be sure to select **Export HPSIM Schema** in the Database Admin Export window so that HP System Insight Manager data is exported. See "Database Maintenance and Management" on page 263.

   As a best practice it is highly recommended that you backup the management server to create a restorable image of the server using the backup tool of your choice.

Step 6 – Start the Storage Essentials Upgrade Wizard and Resolve Any Minimum Requirement Issues

1. Exit all external utilities that use Oracle before starting the upgrade wizard.
2. Put the Storage Essentials for Windows Management Server installation CD in the CD-ROM drive of the management server running Storage Essentials and HP SIM or on the separate server on which Storage Essentials is installed if you are running a separate server configuration. The Storage Essentials upgrade wizard starts automatically and the Welcome to Storage Essentials screen is displayed.
3. Click **Next**. The System Inspection screen is displayed briefly while the Storage Essentials installation wizard scans your system and determines that you are upgrading. As long as the system requirements are met, the Getting Started with an Upgrade screen is displayed.

   IMPORTANT: The Storage Essentials upgrade wizard stops AppStorManager, the service for HP Storage Essentials host, even if you cancel the upgrade program without making any changes. Restart the service after cancelling setup.exe to bring your system back to an operational state.

   The following checks are performed before the Storage Essentials installation wizard starts. If any of these checks fail, the installation wizard will not start until the requirement is met. See "Pre-installation Checklist (Installations and Upgrades)" on page 8 and the support matrix and release notes (**Documentation** > **Support Matrix** or **Release Notes**, accessible from any Storage Essentials installation wizard screen) for more details on the requirements:

   - Only one instance of the installation wizard can be running.
   - Screen resolutions less than 800x600 pixels will cause the upgrade to fail.
   - You must be logged into the machine with administrator privileges or the upgrade will fail.

- The server must be running a supported operating system or the upgrade will fail. Refer to the support matrix for a valid operating system.
- Microsoft Internet Explorer 6.0 SP1 or later must be installed or the upgrade will fail.
- TCP/IP must be installed or the upgrade will fail.
- *The upgrade will fail if SNMP and the SNMP trap service is not installed and enabled. The upgrade program tells you SNMP must be enabled and SNMP trap services must be installed. The upgrade will not go beyond a certain point until you enable SNMP and SNMP trap services.
- If insufficient disk space in `%Temp%` is detected the upgrade will fail. You must have at least 2 GB of free disk space on the drive where %temp% is located.

4. Read the overview information on the Getting Started with an Upgrade screen and click **Next**. The Upgrade Locations screen is displayed showing the directories in which the management server components are currently installed.
5. Optional. Select the check box to copy your CIM extensions to the management server only if you want to overwrite the existing CIM extension files. You can copy the CIM extensions from the CIM Extension CD manually to the management server at a later time. Note that this option only copies the CIM extension files to the management server. It does not install the CIM extensions on your hosts.

IMPORTANT: The 6.0 CIM extensions are required on any backup manager hosts to continue collecting backup manager discovery data. Build 5.1 CIM extensions on backup manager hosts are not supported after upgrading. See ”Deploying and Managing CIM Extensions” on page 181 for information on installing CIM extensions.

6. Optional. You can change the location of the Oracle database.
7. Click **Next** to continue. The Verify System Requirements screen is displayed. See the support matrix for complete system requirement details.

NOTE: The Port Availability requirement line may show a warning during an upgrade that can be ignored, as it indicates that the existing management server service has reserved the ports.

8. Click **Next**. The HP Systems Insight Manager Service Account Credentials screen is displayed. Enter the password for the HP Systems Insight Manager. The user name and domain boxes are pre-filled based on the information entered in the Upgrade Locations screen earlier.
9. Click **Next**. The Upgrade Summary screen is displayed showing the selected components to be upgraded.
10. Click **Upgrade** to continue or **Previous** to make changes to the previous screen or **Cancel** if you need to make changes to the server. Once you click **Upgrade**, the upgrade wizard begins migrating the Oracle database and will not allow you to cancel until the migration is complete. The automated Oracle database migration creates a backup of your Oracle 9i database, exports the database, installs Oracle 10g Standard Edition, and imports the database during the upgrade. You can cancel the upgrade once the database migration is complete if desired.

If you click **Cancel** during the upgrade, the Storage Essentials upgrade wizard completes the upgrade of the current component before stopping. Once that component upgrade is complete, the Storage Essentials upgrade wizard prompts you to confirm that you want to cancel. Click **Yes** to cancel or **No** to continue with the installation.You can resume the upgrade by running the Storage Essentials upgrade wizard again.

> **NOTE:** As mentioned earlier, the upgrade wizard stops AppStorManager, the service for the management server HP Storage Essentials, even if you cancel the upgrade program without making any changes. Restart the service after cancelling setup.exe to bring your system back to an operational state.

11. During the upgrade, the Storage Essentials for Windows installation wizard resets all customized Oracle passwords to their default values in order to automatically upgrade the Oracle database that resides on the Storage Essentials server to Oracle 10g. You must change the SIM_MANAGER password HP SIM uses to access the Oracle database back to **quake** by using the mxpassword command and the CLI interface on the HP SIM server during the upgrade process.

    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.

    The SIM_MANAGER password is changed.

    c. Continue with the Storage Essentials upgrade wizard. You can change the SIM_MANAGER password from the default when the Storage Essentials upgrade is done.

    The Installation Complete screen is displayed when the upgrade wizard completes upgrading each component.

    > **NOTE:** If you specified any customized changes using the **Product Health** > **Advanced** option in a prior release, a record of those changes is saved in the `%mgr_dist%\logs\custom.txt` file after upgrading.

12. Click **Finish** to reboot the management server.

Step 7 – Customize Database Passwords

The database passwords are reset during the upgrade. Use the Database Admin Utility to customize your database passwords.

During the upgrade, all Oracle passwords are reset to their defaults, including the TNS listener password, and the passwords for the SYS, SYSTEM, DB_SYSTEM_USER, SIM_MANAGER, RMAN_USER accounts. Please use the Database Admin Utility to change these passwords after upgrading.

Step 8 – Enable RMAN Backup if Desired

RMAN Backup is disabled by default as part of the upgrade process. When you log into the management server after upgrading, you see a message informing you that RMAN Backup is disabled. You should re-enable RMAN backup as soon as possible to continue backing up your data.

Step 9 – Upgrade is Required on the Following CIM Extensions

Upgrade CIM extensions on servers with the following functionality:

- Backup Manager Hosts — Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Hosts must be at the same build number as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host in order to continue to see backup data.
- Windows hosts using SecurePath — SecurePath information is not retrieved from legacy CIM extensions.
- *Host that you want to retrieve cluster information for example: Veritas Cluster Server on Solaris cluster and Microsoft Cluster Server
- *Linux hosts that support QLogic failover

*This is new functionality that requires Build 6.0 of the CIM extension.

Step 10 – Rediscover all Elements

You should rediscover all elements after you do an upgrade by running /Discovery Data Collection.

Discovery is important because:

- Better scalability is provided after discovery.
- Cluster functionality. To use the new functionality, upgrade the CIM extensions to Build 6.0 and rediscovery is required.
- You will see the following issues until you do Discovery:
  - Reports and Capacity Manager/Capacity Explorer show incorrect raw capacity data for storage systems.
  - There is no trunked status indication on Brocade fabrics.
  - No NPIV status indication.
  - No provisioning for HP StorageWorks EVA arrays using Command View EVA.
  - New host modes on storage systems are not available.
  - Backup data collection would be suspended until CIM extensions on Backup Manager Hosts are upgraded to Build 6.0 and they are rediscovered.

Steps That Can be Run Anytime After the Upgrade

The following steps can be completed any time after the upgrade; however, you will have reduced functionality with the product until you complete these steps.

Re-add Remote Sites in Global Reporter

IMPORTANT: After the upgrade, all remote sites in the Global Reporters are removed. This is done so you can upgrade the remote sites to the same version before Global Reporter attempts to gather data. Before you re-add the remote sites, be sure to upgrade them to the same build number as the management server (Build 6.0 CIM extensions).

All sites that provide global reports must be upgraded to the latest build of the management server. Install this build of the management server on all remote sites, then complete the following steps for each management server that is using Global Reporter.

1. You must modify the listener.ora file at each remote site, as described in the following steps. For example, assume you have three remote sites. You must log onto each of these remote sites and modify the listener.ora file at each remote site, as described in the following steps:

   a. Log onto the remote site.

   b. Stop the service for the management server running.

   c. Stop the listener service for Oracle (OracleOraHome92TNSListener).

   d. Open the following file in a text editor on the computer:

   ```
   %ORA_HOME%\network\admin\listener.ora
   ```

   e. After `(ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521)), add the following line:`

   ```
   (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.10.1)(PORT = 1521))
   ```

   where 192.168.10.1 is the IP address of the local host server. Replace 192.168.10.1 with the IP address of your local host.

   The text should now appear as follows:

   ```
   LISTENER =
     (DESCRIPTION_LIST =
       (DESCRIPTION =
         (ADDRESS_LIST =
           (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
           (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.10.1)(PORT = 1521))
         )
       )
     )
   ```

   f. Save the file and exit.

   g. Start the listener service for Oracle (OracleOraHome92TNSListener).

   h. Start AppStorManager.

2. Open the page for Global Reporter (**Reports** > **Storage Essentials** > **Report Configuration** > **Global Reporter** in HP Systems Insight Manager on the Global Reporter server and remove all remote sites listed by clicking the 🗑 button.

3. Click the **Refresh Now** button at the bottom of the page. This action clears the management server database.

4. Add desired remote sites, by clicking the **New Site** button and providing the appropriate information. Refer to the User Guide and online help for more information.
5. To upgrade the database with data from the added sites, click the **Refresh Now** button at the bottom of the page.

Upgrade Your Storage Essentials CLI Clients

CLI clients earlier than Build 6.0 do not work with Build 6.0 of the management server. Refer to the CLI Guide for more information about upgrading your CLI clients.

Upgrade Your CIM Extensions

See "About Upgrading Your CIM Extensions" on page 189 " for details.

Migrate Your Brocade Switches to SMI-A

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider.

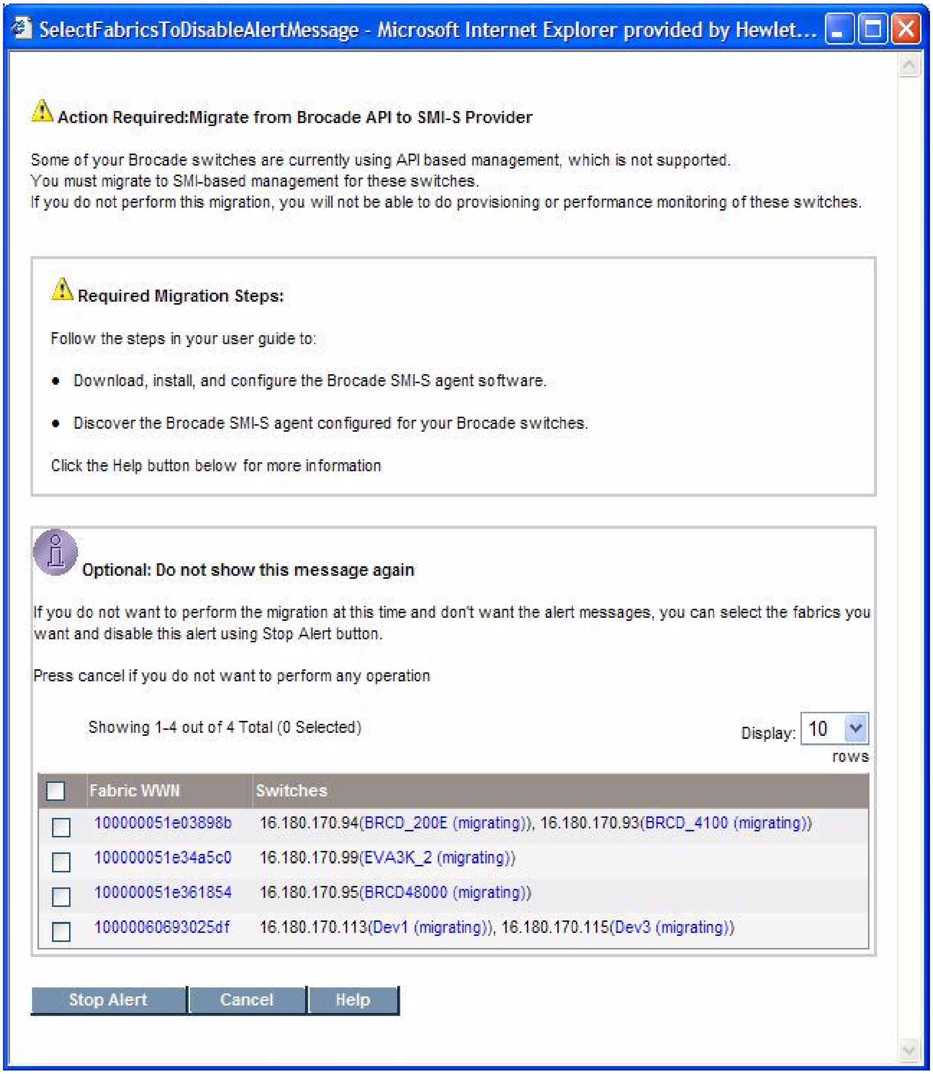
After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Discovery Data Collection schedule. If the Brocade switches were part of a Discovery Data Collection schedule prior to migration, you must manually adjust those schedules to run Discovery Data Collection for the migrated Brocade switches. If the schedules are not adjusted manually, Discovery Data Collection will not run for the migrated switches as per pre-migration schedules.

Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:
   http://www.brocade.com/support/SMIAGENT.jsp
   See the support matrix for your edition for details on the latest supported version for the management server.

2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

3. Log on to the management server. HP Storage Essentials alerts you to migrate your Brocade Fabric Access API switches when you first log on.



SelectFabricsToDisableAlertMessage - Microsoft Internet Explorer provided by Hewlet...

⚠ **Action Required:Migrate from Brocade API to SMI-S Provider**

Some of your Brocade switches are currently using API based management, which is not supported.
You must migrate to SMI-based management for these switches.
If you do not perform this migration, you will not be able to do provisioning or performance monitoring of these switches.

⚠ **Required Migration Steps:**

Follow the steps in your user guide to:

- Download, install, and configure the Brocade SMI-S agent software.
- Discover the Brocade SMI-S agent configured for your Brocade switches.

Click the Help button below for more information

Optional: Do not show this message again

If you do not want to perform the migration at this time and don't want the alert messages, you can select the fabrics you want and disable this alert using Stop Alert button.

Press cancel if you do not want to perform any operation

Showing 1-4 out of 4 Total (0 Selected)

Display: 10 rows

□	Fabric WWN	Switches
□	100000051e03898b	16.180.170.94(BRCD_200E (migrating)), 16.180.170.93(BRCD_4100 (migrating))
□	100000051e34a5c0	16.180.170.99(EVA3K_2 (migrating))
□	100000051e361854	16.180.170.95(BRCD48000 (migrating))
□	10000060693025df	16.180.170.113(Dev1 (migrating)), 16.180.170.115(Dev3 (migrating))

Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

4. Run HP SIM discovery for the Brocade proxy server. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”
5. Run Discovery Data Collection. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”
   The Brocade switches are migrated to the SMI-A provider.

   Important: Before performing any provisioning operations that involve a Brocade switch you must perform Discovery Data Collection for any subset of elements that includes the Brocade switch.

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Discovery Data Collection schedules as described in the following steps:
   a. Select **Options** > **Storage Essentials** > **Discovery** > **Schedule Discovery Data Collection** in HP Systems Insight Manager.
   b. Click the **Edit** (✎) button corresponding to the discovery schedule you want to modify.
   c. Click the **Discovery Groups** tab.
   d. Select the Brocade proxy under the list of discovery groups.
   e. Click **Add Selected Groups To Schedule**.
   f. Click **Finish**.

Check any McDATA and Connectrix Switches

As mentioned earlier, by default after upgrading, the management server is configured to use the SMI-S provider to manage and discover McDATA and Connectrix switches. The migration to SMI-S is not required for McDATA and Connectrix switches as it is with the Brocade Fabric Access API provider.

You must do one of the following after upgrading:

- Before you can discover McDATA and Connectrix switches with SMI-S, you must download and install the McDATA SMI-S provider software. See the document *HP StorageWorks M-Series* at: http://www.hp.com/go/hpsim/providers for instructions. Check this web site periodically to verify that you are running a current version of the SMI-S provider..
- See the following section to change the default from SMI-S if you prefer not to migrate to the SMI-S provider:

  ”Changing the Discovery Settings” on page 130.

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.

In Navisphere add the following to the privilege user section:

```
root@name_of_my_management_server
root@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

The management server service needs to be restarted after installing EMC Navisphere CLI.

About Service Account Credentials

You are asked for service account credentials during a typical installation of HP SIM or during the installation of OpenSSH Services for HP SIM. The user name and password you provide is for the user that is installing HP SIM. This must be an existing user account with administrative privileges. This user account is also used for starting the HP SIM service.

IMPORTANT: If you change the credentials of the service account you provided, for example the password, you must change the credential information for the HP SIM service. You can change the credential information for the service as described in "Changing the Service Account Credentials for the HP Systems Insight Manager Service" on page 53.

During a typical installation of HP SIM, the Service Account Credentials window is displayed. The Domain and Username fields default to the installing account credentials, but these can be edited. Enter the Password for the account. Click **Next**.

IMPORTANT: A user name and password cannot contain a space followed by a double-quote. If you use this character in your user name or password, you will receive an Invalid character error and not be allowed to sign in.

Changing the Service Account Credentials for the HP Systems Insight Manager Service

The HP Systems Insight Manager service uses the service account credentials supplied during the installation. If the service account credentials change, you must make the HP Systems Insight

Manager service aware of these changes. If you do not, the HP Systems Insight Manager service will not start and you will not be able to use HP SIM.

To change the service account credentials for the HP Systems Insight Manager service:

1. Right-click the **HP Systems Insight Manager** service from the services panel.
2. Select **Properties** from the drop-down menu.
3. Click the **Log On** tab.
4. Change the user name (This account) and password on the Log On tab to match the information for the new credentials. If the host is in a domain, specify the account using the domain\username format.

Important Information About Changing the SIM_MANAGER Password

The information Storage Essentials and HP SIM share is stored in a database with the user name SIM_MANAGER and the default password quake. For security reasons, it is strongly recommended you change the password for this database.

NOTE: This step only applies if Storage Essentials and HP SIM are sharing the same Oracle database and HP SIM is using the Oracle appiq instance.

Make sure you keep the new password for SIM_MANAGER 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 change the password for SIM_MANAGER:

1. Log onto the server running Storage Essentials.
2. Stop the AppStorManager service if it is started.
3. Log onto the server running HP SIM.
4. Stop the HP SIM service so that it can not access the database.

   IMPORTANT: Be sure the HP SIM service does not access the Oracle database before you finish changing the password for the Oracle database.

5. Enter the following at the command prompt:

   ```
   C:\> mxpassword -m -x MxDBUserPassword=mynewPass
   ```

   where `mynewPass` is your new password for the Oracle database.

6. Use the Database Admin Utility to change the SIM_MANAGER password in the Oracle database.

   > **IMPORTANT:** You must provide the same SIM_MANAGER password for the mxpassword command and the Database Admin Utility.

   a. To access the Database Admin Utility, go to the `%MGR_DIST%\Tools\dbAdmin` directory on the Storage Essentials management server and double-click **dbAdmin.bat**.
      If you are shown an error message when you start the Database Admin Utility, stop the AppStorManager service and click the **Refresh** button.
   b. Click **Change Passwords** in the left pane.
   c. Select SIM_MANAGER from the **User Name** box.
   d. Type the current password in the **Old Password** box.
   e. Type the new password in the **New Password** box.
   f. Retype the password in the **Confirm Password** box.
   g. Click **Change**.
      The Database Admin Utility changes the password for the specified account.
   h. Restart the HP Systems Insight Manager service.
   i. Restart the AppStorManager service.

Removing Storage Essentials

Follow these steps to remove the HP SIM Connector, HP SIM, Storage Essentials, and Oracle.

Considerations when Uninstalling the SIM Connector

If you need to uninstall the SIM connector at a later time, be aware of the following considerations:

The SIM Connector is the Storage Essentials component that enables communication between HP Systems Insight Manager and Storage Essentials. The SIM Connector consists of two parts, the HP SIM side of the connector and the Storage Essentials side of the connector. In a typical uninstall, both parts of the connector are removed. However, if HP SIM is not functioning, it is possible to remove only the Storage Essentials side of the connector. If the HP SIM side of the connector is not removed, HP SIM will be left in an unknown state. HP SIM will still contain Storage Essentials objects such as menu items and links. However, the Storage Essentials items will not function.

If the SIM Connector Uninstall wizard detects that HP SIM is not available you see a message similar to the following:

```
HP Systems Insight Manager is not available. Click Cancel to exit the
uninstall or Continue to remove only the Storage Essentials SIM
Connector.
```

At this point, you have two options;

1. Cancel the uninstall. After you start HP SIM you can restart the uninstall. (recommended),
2. Continue the uninstall and remove only the Storage Essentials side of the connector.

IMPORTANT: Use the Continue option only if you do not intend to use this installation of SIM either on its own or integrated with Storage Essentials.

To remove Storage Essentials:

1. Stop the service for the management server (make sure HP SIM is/remains running) by doing the following:
   a. Go to the Services window (**Start** > **Control Panel** > **Administrative Tools** > **Services**).
   b. Right-click the **AppStorManager** service in the Services window.
   c. Select **Stop** from the drop-down menu.
2. Open the Add or Remove Programs window (**Control Panel** > **Add or Remove Programs**).
3. Do the following to uninstall the HP SIM Connector.
   a. Select **HP Connector** and click the **Change/Remove** button. The Uninstall SIM Connector wizard starts.

      IMPORTANT: HP Systems Insight Manager must be running in order to completely remove each portion of the Connector software from HP SIM and Storage Essentials. See "Considerations when Uninstalling the SIM Connector" on page 55 for more details.

   b. Select the **Remove** option, then click **Next**.
   c. Enter these credentials:
      - HP SIM Hostname (fully qualified name)
      - HP SIM Administrator name (the name with which you installed HP SIM), using the format: domain\administrator
      - HP SIM Administrator password
   d. Click **Uninstall**. The Uninstall Complete screen is displayed.
   e. Select **No, I will restart my system myself**.
   f. Click **Done**.
4. Uninstall HP SIM (**Start > Programs** > **HP Systems Insight Manager** > **Uninstall HP Systems Insight Manager**). HP SIM is removed from the management server.
5. Do the following to uninstall Storage Essentials**:**
   a. In the Add or Remove Programs window, select Storage Essentials.
   b. Click the **Change/Remove** button. The Uninstall wizard starts.
   c. In the Uninstall wizard screen, select the **Remove** option, then click **Next**.
   d. Click **Uninstall**. The Uninstall Complete screen is displayed.
   e. Select **No, I will restart my system myself**.
   f. Click **Done**.
6. Do the following to remove Oracle and the Oracle instance for Storage Essentials:

a. Open a Command Prompt window on the Storage Essentials management server (**Start** > **Run** > **cmd.exe**, click **OK**).

b. Put the Oracle DVD in the DVD drive of the Storage Essentials management server.

c. Change directory (CD) to the root of the Oracle DVD.

d. Enter the following at the command prompt window on the management server to remove Oracle and the Storage Essentials management server database instance:

```
cscript removeOracle10g.vbs
```

Oracle is removed from the management server.

7. Delete the old Storage Essentials management server installation directory. If the directory is set with Read Only permissions do the following:

   a. Right-click the directory and select **Properties** > **Security**.

   b. HIghlight (click) **Administrator** and click **Full Control** under the **Allow** column.

   c. Select the **General** tab and clear the **Read-only** check box.

   d. Click **OK** and select **Apply changes to this folder, sub-folders and files** radio button.

   e. Click **Ignore All** if you see an error message.

   f. Delete the directory.

8. Delete the installation log files:

   - del %systemdrive%\srnInstsallLogs\*.log
   - del %windir%\srmwiz.ini

3 Installing the Management Server on Linux

NOTE: The Linux management server is not available with Storage Essentials Standard Edition.

See the following topic if you are installing the management server on another supported operating system:

- "Installing the Management Server on Microsoft Windows" on page 7

Important Information About Upgrading

Please contact your Account Representative for upgrades. Upgrading requires assistance from HP Services.

Keep in mind the following:

- **All steps must be completed for the management server to work properly.**
- Linux management server is supported only on the following versions:
  - Redhat 4 (U3 or higher)
  - SUSE 9 (SP3)
  - SUSE 10 or SUSE 10 SP1
- Refer to the product Support Matrix regarding other related software and version requirements.
- For optimal performance, install the management server on a dedicated computer. See the support matrix for your edition for hardware requirements.
- Installation through Virtual Network Computing (VNC) software is not supported.
- During management server installation, double-byte characters are not allowed in the installation path. InstallScript.iap_xml has been modified to display the following message if double-byte characters are entered:

  ```
  The installation path for $PRODUCT_NAME$ may NOT contain double-byte
  characters.
  The installation path must be basic ASCII alphanumric characters, no
  spaces, no international characters, and no double-byte characters.
  Please choose a different installation directory.
  ```

This chapter describes the following installation topics and steps:

- Deployment Types, page 60
- Pre-installation Checklist, page 60
- Installing from a Network Drive, page 64
- Step 1 - Install the Oracle Database, page 64
- Step 2 - Install the Management Server, page 76
- Step 3 - Verify that Processes Can Start, page 79
- Step 4 - Install and Configure HP SIM, page 82

Deployment Types

This product provides two types of deployments:

- **Single box deployment** - HP Systems Insight Manager (SIM) and Storage Essentials are installed on the same server. Follow the instructions in this chapter.
- **Dual box deployment** - HP SIM and Storage Essentials are installed on different servers. When you install HP SIM on a different server, skip "Step 4 - Install and Configure HP SIM" on page 82. After you install HP SIM by using the directions provided in the HP SIM documentation, continue the installation steps with "Step 5 - Install the HP SIM Connector" on page 85.

Pre-installation Checklist

HP SIM

Verify that the following required software is available on your system, and install any that are missing:

- **SSH** - Verify that SSH is installed by entering the following command:

  ```
  # rpm -qa | grep ssh
  ```

  If SSH is not installed, the previous command does not return any results.
- **SNMP** - Verify that SNMP is installed by entering the following command

  ```
  # rpm -qa | grep snmp
  ```

  If SNMP is not installed, the previous command does not return any results.
- **C++ libraries** - Verify that standard C++ libraries are installed by entering the following command:

  ```
  # rpm -qa | grep compat
  ```

  If the libraries are not installed, the previous command does not return any results.
- **Linux glibc library** - Verify that the Linux glibc library is installed by entering the following command:

  ```
  # rpm -qa | grep glibc
  ```

  If the library is not installed, the previous command does not return any results.

Install any missing components from the Linux operating system CD before continuing with the installation.

Pre-requisite RPMs for Oracle on Linux

Verify that your system includes the required packages by using the following command:

```
# rpm -q <package-name>
```

Required RPMs for Oracle 10g on RHEL systems:

- binutils-2.15.92.0.2-10.EL4
- compat-db-4.1.25-9
- control-center-2.8.0-12
- gcc-3.4.3-9.EL4
- gcc-c++-3.4.3-9.EL4
- glibc-2.3.4-2
- glibc-common-2.3.4-2
- gnome-libs-1.4.1.2.90-44.1
- libstdc++-3.4.3-9.EL4
- libstdc++-devel-3.4.3-9.EL4
- make-3.80-5
- xscreensaver-4.18-5.rhel4.2

Required RPMs for Oracle 10g on SUSE 9 systems:

- binutils-2.15.90.0.1.1-32.5
- gcc-3.3.3-43.24
- gcc-c++-3.3.3-43.24
- glibc-2.3.3-98.28
- gnome-libs-1.4.1.7-671.1
- libstdc++-3.3.3-43.24
- libstdc++-devel-3.3.3-43.24
- make-3.80-184.1
- xscreensaver-4.16-2.6
- orarun-1.8-109.15
- sysstat-5.0.1

Required RPMs for Oracle 10g on SUSE 10

- binutils
- glibc-2.4
- gcc-4.1.0
- gcc-c++-4.1.0
- libaio

- libaio-devel
- libstdc++
- make-3.80
- openmotif-libs
- sysstat-6.0.2
- orarun-1.9-21

The preceding information is taken from http:/www.novell.com/products/server/oracle/oracle10g_install.html. RPMs for SLES 9 can be found at http://www.novell.com/products/server/oracle/software.html and RPMs for SLES 10 can be found in the SLES 10 product CD.

NOTE: The **orarun-1.9** package is available from http://ftp.novell.com/partners/oracle/sles-10/orarun-1.9-21.15.i586.rpm.

The list of packages described above for RHEL and SUSE includes all the packages needed for Oracle installation. Some of these packages might be selectively installed depending on the mode of installation followed during OS installation.

Software Dependencies for Storage Essentials

NOTE: The database configuration and creation script is different for Oracle 10g than it was for Oracle 9i. As a result, the management server software Build 6.0 is not supported by Oracle 9i. Management server software builds earlier than 6.0 are not supported on the Oracle 10g platform.

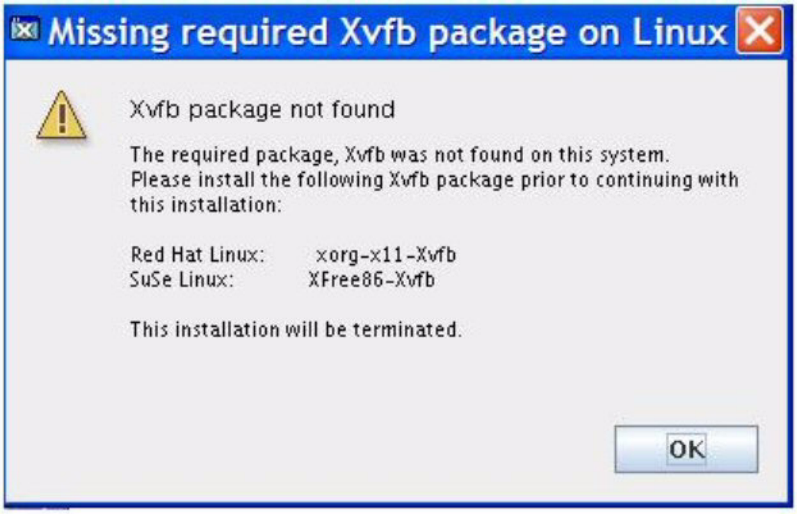
Verify that the following required software is available on your system, and install any that are missing:

- Perl 5.8.3 or above. By default, the OS installs Perl 5.8.3 on SUSE 9 and Perl 5.8.5 on RHEL 4.
- '`Xvfb`' is required for Application Viewer and Reporter. The Application Viewer and Reporter pages show a 'java.lang.NoClassDefFoundError' if '`Xvfb`' is not installed. This package comes with the OS distribution (for both RHEL & SLES) and is installed if Full OS Install is selected.
    - For RHEL, the package name is "`xorg-x11-Xvfb`"
    - For SLES 9,the package name is "`XFree86-Xvfb`"
    - For SLES 10, the package name is "`xorg-x11-Xvf`b"

For RHEL 4 or SUSE 10, if the "`xorg-X11-Xvfb`" package is not installed, the management server installer displays a message that the "Xvfb" package is not installed, and stops the install process. Install the package named "`xorg-X11-Xvfb`" and then re-run the management server installation. This package is available on RHEL 4 OS CD's and SUSE 10 CDs.

For SUSE 9, if the "`XFree86-Xvfb`" package is not installed, the management server installer displays a message that the "Xvfb" package not installed, and stops the install process. Install the package named “XFree86-Xvfb” and then re-run the management server installation. This package is available on the SUSE 9 CD’s.

The following shows a representative example of the error message that would be displayed.



Missing required Xvfb package on Linux

Xvfb package not found

The required package, Xvfb was not found on this system. Please install the following Xvfb package prior to continuing with this installation:

```
Red Hat Linux:    xorg-x11-Xvfb
SuSe Linux:       XFree86-Xvfb
```

This installation will be terminated.

Figure 1 Missing Xvfb Package Message

Verify Network Settings

Verify the network configuration for the management server:

1. Verify that the appropriate DNS server entries are present in `/etc/resolv.conf`. Verify that the correct DNS suffixes are mentioned in the order of preference in which they need to be appended to hostnames.

   For example:

   ```
   nameserver 172.168.10.1
   nameserver 172.168.10.2
   search “yourenvironment”.com
   ```

2. From a console window on the management server, enter the following command:

   ```
   ping <hostname>
   ```

   where <hostname> is the hostname (without domain name) of the Linux CMS.

   The ‘ping’ command must ping the IP address of the management server. It must not ping the loopback address (127.0.0.1). If it pings the loopback address, edit the `/etc/hosts` file to make appropriate corrections.

   The `/etc/hosts` file should have entries similar to:

   ```
   127.0.0.1       localhost.localdomain  localhost
   192.168.0.100   myservername.mydomain.com  myservername
   ```

NOTE: If the ping command fails to ping the IP address and instead pings the loopback address, the oracle listener process will fail to start and therefore, the CIMOM process will also fail.

3. Enter the following command:

   ```
   nslookup <hostname>
   ```

   where <hostname> is the hostname (without domain name) of the management server.
4. Enter the following command:

   ```
   nslookup <IP address>
   ```

   where <IP address> is the IP address of the server.
5. Verify that both results from nslookup have the same fully qualified computer name and IP address.

Installing from a Network Drive

Support for installing (or upgrading) from a network drive is limited to NFS mounted network drives only. After the network drive is mounted to the local server, there are no separate network drive-related steps required for the installation (or upgrade).

- Create a directory on which the NFS drive will be mounted:

  ```
  #mkdir /InstallSE
  ```

- Mount the NFS shared network drive from NFS server (example: "pillbox") with shared drive "InstallSE", with strong recommendation to set it as read only.

  ```
  #mount pillbox:/InstallSE /InstallSE
  ```

- Any database ISO files must be loop-mounted and it is strongly recommended to set them to read only mode. Management CD ISO files can be mounted in the same way as shown in the following representative example for the Oracle database. (Names such as Disk1 or Vol1 can be user-configurable, created by user with “mkdir”.) The steps need to be repeated for any other ISO user trying to mount from NFS mount (Database, management server, CIM extension) Example:

  ```
  #mkdir /Disk1
  #mount -o loop,ro /InstallSE/database/linux/<oracle10g.iso>  /Disk1
  ```

  In this example, to install the Oracle database:

  ```
  #/Disk1/InstallDatabase
  ```

Step 1 - Install the Oracle Database

The management server uses a database to store the data it collects from the hardware it monitors. The management server ships with a DVD that includes Oracle 10g Release 2, 10.2.0.1, upgrade to Oracle 10g Release 2, 10.2.0.3, and the October 2007 Critical Patch Update for Oracle 10g Release 2.

The install for Oracle 10g Release 2, 10.2.0.1, will also install the upgrade to Oracle 10g Release 2, 10.2.0.3, and apply the October 2007 Critical Patch Update.

Install the database for the management server on a computer that does not already have Oracle installed. In later steps, you will install the management server on the same machine that you installed Oracle.

Before Installing the Oracle Database

Keep in mind the following:

- Refer to the support matrix for your edition for system requirements.
- Once you start the installation, do not exit. The Oracle installer creates the orauser file within the first few minutes of the installation. This file remains on the system if the installation is stopped before completion. Future installations of the management server database look for the orauser file to verify that the database is installed. If you exit the Oracle installation before the installation is finished, the management server will not run correctly.
- Install the database on the computer on which you plan to install the management server.
- Before you install Oracle, ensure the Linux server has the packages installed that are required by Oracle.
- For both Linux SUSE and RHEL, Oracle 10.2.0.1.0 (32 bit) Standard Edition software is used.
    - For the management server Build 6.0 software, the Oracle install runs in silent mode. (Oracle installs silently showing progress indication in the console through text messages.) This process does not require X-server and DISPLAY settings.
- When you install the database on Linux, files with group-writeable permissions are installed in the `ORA_HOME` directory.

Prerequisites

Before you install the database on a Linux server, do the following:

- Verify that the server is running sh, ksh or bash shell.
- Verify the following directories have write permissions:

  `/`
  `/tmp`
  Parent directory of `ORA_HOME`
- If you are running Red Hat Enterprise Linux AS 4 or Red Hat Enterprise Linux ES 4, delete the existing Oracle user if present, before proceeding with the installation. The installation will fail if there is an existing Oracle user.
- On SUSE Linux systems, on installing the 'orarun' rpm, the Oracle user account gets created automatically. However the oracle user account needs to be enabled by changing the shell entry from '/bin/false' to '/bin/bash' for oracle user in the `/etc/passwd` file.
- Setting of the kernel parameters for Oracle on both Red Hat and SUSE systems is handled by the Oracle installer script and the user need not set the kernel parameters.
- At least 400 MB of free space is required in the `/tmp` directory.
- `ORA_HOME` should have a minimum of 50 GB of free space.

NOTE: If the Oracle installation fails, a re-install will not run successfully because of existing files or existing Oracle user. In such a case, uninstall Oracle using the Oracle uninstall script. Refer to step 6 of "Removing the Management Server" on page 89.

Installing the Database

To install the database:

1. Login to the Linux host as root user.
2. Insert the first Oracle Database DVD and mount it using the following commands:

   ```
   # mkdir -p /mnt/oradisk
   # mount /dev/cdrom /mnt/oradisk
   ```

   where `/dev/cdrom` is the device.
3. Verify that you are in the top level directory:

   ```
   # cd /
   ```
4. Start the installation of the database by entering the following:

   ```
   # /mnt/oradisk/InstallDatabase
   ```

   NOTE: All commands and filenames are case-sensitive.
5. The script will ask if you wish to continue. Enter "y."

6. The oracle installer script checks for required RPMs and terminates if any required RPM is missing. In such case, install the missing RPMs and restart the installation.

```
INFO: Checking for required packages...
ERROR: sysstat is not installed.

ERROR: Please install missing pre-requisite packages
       before proceeding with installation.

Terminating installation.

If the installer finds a different version of a pre-requisite RPM, it will
prompt the user to confirm continuing the installation.

INFO: Checking for required packages...
WARN: Looking for package gcc-4.1.0. Found gcc-4.1.2_20070115-0.11.
WARN: Looking for package gcc-c++-4.1.0. Found gcc-c++-4.1.2_20070115-0.11.

WARN: Version mismatch in pre-requisite packages.
      Oracle may not work with these versions.
Do you want to continue? [y/n]:
y

INFO: Verified pre-requisite packages.
INFO: Proceeding with installation...
```

7. If there is insufficient swap space, the script displays a message saying that the swap space is insufficient and a message similar to the following displays:

```
INFO: Checking swap space...
INFO: Available RAM: 4082752
INFO: Recommended Swap size: 4082752
INFO: Current Swap: 2097144
INFO: Insufficient swap size.
INFO: Creating additional swap space: 1985608
1985608+0 records in
1985608+0 records out
mke2fs 1.38 (30-Jun-2005)
/tmp/swapForOracle1.tmp is not a block special device.
Proceed anyway? (y,n)
```

Enter ‘y’ at the prompt.

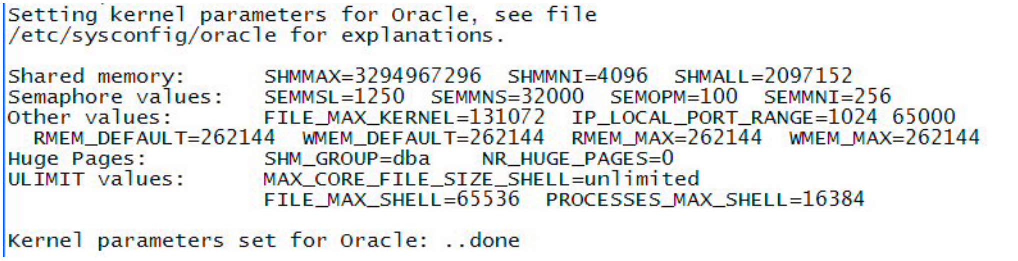
You may be prompted to create multiple swap files. Enter ‘y’ each time you encounter the prompt described above.

8. The temporary disk space in /tmp is checked. If the disk space in /tmp is less that 400 MB, the installation will abort with the below message.

```
ERROR: You need at least 400MB in the /tmp directory.
You only have 100 MB.

Terminating installation.
```

9. Appropriate kernel parameters are automatically set by the installation script.



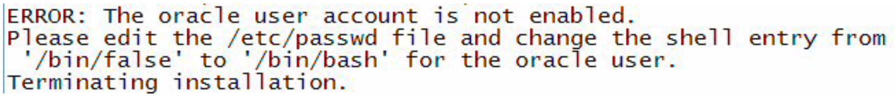
```
Setting kernel parameters for Oracle, see file
/etc/sysconfig/oracle for explanations.

Shared memory:      SHMMAX=3294967296  SHMMNI=4096  SHMALL=2097152
Semaphore values:   SEMMSL=1250  SEMMNS=32000  SEMOPM=100  SEMMNI=256
Other values:       FILE_MAX_KERNEL=131072  IP_LOCAL_PORT_RANGE=1024 65000
  RMEM_DEFAULT=262144  WMEM_DEFAULT=262144  RMEM_MAX=262144  WMEM_MAX=262144
Huge Pages:         SHM_GROUP=dba    NR_HUGE_PAGES=0
ULIMIT values:      MAX_CORE_FILE_SIZE_SHELL=unlimited
                    FILE_MAX_SHELL=65536  PROCESSES_MAX_SHELL=16384

Kernel parameters set for Oracle: ..done
```

Figure 2 Setting Kernel Parameters

10. On SUSE systems, the oracle user account should be enabled prior to starting the installation. If the oracle user is not enabled, an error message is shown as below.



```
ERROR: The oracle user account is not enabled.
Please edit the /etc/passwd file and change the shell entry from
 '/bin/false' to '/bin/bash' for the oracle user.
Terminating installation.
```

Figure 3 Oracle User Account Not Enabled Error

```
On Red Hat systems, if an oracle user is already existing, an error message
is shown indicating that this oracle user needs to be deleted. The following
shows the error message.
```

```
ERROR: This script has detected an existing Oracle user account on this
        system.
       This script requires that no Oracle user account be present prior
        to the installation.
        Please contact your System Administrator to resolve this conflict.
```

11. When prompted, enter the Oracle home directory. The default location for SUSE 9 and SUSE 10 is /opt/oracle, and for RHEL 4 is /home/oracle.

12. When prompted, enter the Oracle installation directory. The default location is opt/oracle.

```
Please enter the Oracle user's home directory. [Default: /home/oracle]
Please enter Oracle installation directory [Default: /opt/oracle]
INFO: Created Oracle users home directory.
```

13. If you are running Red Hat Enterprise Linux AS 4 or RHEL 4.0, you will be asked to enter the password for oracle user. Enter the password when prompted.
14. Enter “y” when asked to start the Oracle Universal Installer. For RHEL 4.0, text similar to the following console output may display. (Representative console output for SUSE 10 and SUSE 10 SP1 is also included at the end of this example following the “Note” information.)

```
Starting Oracle Installer...
Starting Oracle Universal Installer...

Checking installer requirements...

Checking operating system version: must be redhat-3, SuSE-9, redhat-4,
UnitedLinux-1.0, asianux-1 or asianux-2
                              Passed

All installer requirements met.

Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2007-10-24_05-33-55PM. Please wait ...Oracle Universal
Installer, Version 10.2.0.1.0 Production
Copyright (C) 1999, 2005, Oracle. All rights reserved.

Font specified in font.properties not found
[--symbol-medium-r-normal--*-%d-*-*-p-*-adobe-fontspecific]
Font specified in font.properties not found
[--symbol-medium-r-normal--*-%d-*-*-p-*-adobe-fontspecific]
Font specified in font.properties not found
[--symbol-medium-r-normal--*-%d-*-*-p-*-adobe-fontspecific]

Warning: Cannot convert string "<Key>Escape,_Key_Cancel" to type
VirtualBinding
Warning: Cannot convert string "<Key>Home,_Key_Begin" to type VirtualBinding
Warning: Cannot convert string "<Key>Help,_Key_F1" to type VirtualBinding
```

NOTE: The warning messages in the above console output can safely be ignored.

NOTE: The Oracle Installer that comes with the Oracle Database Server Patch 10.2.0.1 does not officially support SUSE 10; however, the Oracle database is supported on SUSE 10. The resulting error messages can be safely ignored. Also, “Failed” and “Not Executed” check complete messages in the pre-requisites result can be safely ignored.

For SUSE 10 and SUSE 10 SP1, text similar to the following displays:

```
INFO: The next step is to start the Oracle Universal Installer.

Start the Oracle Universal Installer ? [y/n]:
y
Starting Oracle Installer...
Starting Oracle Universal Installer...

Checking installer requirements...

Checking operating system version: must be redhat-3, SuSE-9, redhat-4,
UnitedLinux-1.0, asianux-1 or asianux-2
                                      Failed <<<<


>>> Ignoring required pre-requisite failures. Continuing...

Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2007-09-29_07-40-00PM. Please wait ...Oracle Universal
```

```
Installer, Version 10.2.0.1.0 Production Copyright (C) 1999, 2005, Oracle.
All rights reserved.

You can find a log of this install session at:
 /opt/oracle/oraInventory/logs/installActions2007-09-29_07-40-00PM.log

Starting execution of Prerequisites...
Total No of checks: 11

Performing check for CertifiedVersions
Checking operating system requirements ...
Expected result: One of redhat-3,redhat-4,SuSE-9,asianux-1,asianux-2
Actual Result: SuSE-SUSE Linux Enterprise Server 10 (i586)
Check complete. The overall result of this check is: Failed <<<<


Check complete: Failed <<<<
Problem: Oracle Database 10g is not certified on the current operating
system.
Recommendation: Make sure you are installing the software on the correct
platform.

========================================================================
Performing check for Packages
Checking operating system package requirements ...
Check complete. The overall result of this check is: Not executed <<<<


Check complete: Not executed <<<<
OUI-18001: The operating system 'Linux Version SuSE-SUSE Linux Enterprise
Server 10 (i586)' is not supported.
Recommendation: Install the required packages before continuing with the
installation.
............................................................................
.......................... 100% Done.
```

15. Once the installer begins installing Oracle 10g, it cannot be paused or cancelled. The only way to re-install Oracle is to uninstall it and start all over again.
16. Once Oracle 10g is installed successfully, the script automatically executes root.sh from $ORACLE_HOME where $ORACLE_HOME is usually /opt/oracle/product/10.2.0.1.

The following is the output of the script. Your output may differ slightly based on the file paths you entered.

```
Oracle Database 10g Installation : OK
----------------------------------------------------------------------
INFO: Running root.sh...
----------------------------------------------------------------------Runni
ng Oracle10 root.sh script...

The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /opt/oracle/product/10.2.0.1

Enter the full pathname of the local bin directory: [/usr/local/bin]:
Copying dbhome to /usr/local/bin ...
   Copying oraenv to /usr/local/bin ...
   Copying coraenv to /usr/local/bin ...

Creating /etc/oratab file...
Entries will be added to the /etc/oratab file as needed by
Database Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
----------------------------------------------------------------------OK.

The upgrade to Oracle 10g 10.2.0.3 starts after Oracle 10g 10.2.0.1
completes installation.
-------------------------------------------------------------------------
  This script installs Oracle Database 10g Release Patch Set 2
-------------------------------------------------------------------------
INFO : Checking the OS Release...
```

After upgrading to Oracle 10.2.0.3, the installer will execute root.sh from $ORACLE_HOME. The user does not have to open a new terminal window and run the script as mentioned in the following representative example.

```
The following configuration scripts need to be executed as the "root" user.
/opt/oracle/product/10.2.0.1/root.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as "root"
    3. Run the scripts

The installation of Oracle Database 10g Release 2 Patch Set 2 was
successful.
Please check
'/opt/oracle/oraInventory/logs/silentInstall2007-10-24_05-41-14PM.log' for
more details.

Running Oracle10 root.sh script...

The following environment variables are set as:
    ORACLE_OWNER= oracle
    ORACLE_HOME=  /opt/oracle/product/10.2.0.1

Enter the full pathname of the local bin directory: [/usr/local/bin]: The
file "dbhome" already exists in /usr/local/bin.  Overwrite it? (y/n)
```

NOTE: There is no need to overwrite these files as they would not have changed.

Oracle Critical Patch Update

The critical patch update is applied automatically after the installer completes upgrading to Oracle 10.2.0.3. If Oracle 10.2.0.3 upgrade fails, then the critical patch update will exit with a failure.

The installation is done in silent mode and output similar to the following displays when the installation begins:

```
INFO : Checking the OS Release...
Found SUSE LINUX Enterprise Server 9.
Installing Oracle 10g Release 2 Critical Patch Update, October 2007...
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121183
     Patch 6121183 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121242
     Patch 6121242 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121243
     Patch 6121243 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121244
     Patch 6121244 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121245
     Patch 6121245 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121246
     Patch 6121246 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121247
     Patch 6121247 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121248
     Patch 6121248 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121249
     Patch 6121249 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121250
     Patch 6121250 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121257
     Patch 6121257 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121258
     Patch 6121258 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121260
     Patch 6121260 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121261
     Patch 6121261 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121263
     Patch 6121263 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121264
     Patch 6121264 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121266
     Patch 6121266 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6121268
     Patch 6121268 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6394981
     Patch 6394981 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397928
     Patch 6397928 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397929
```

```
     Patch 6397929 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397937
     Patch 6397937 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397938
     Patch 6397938 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397939
     Patch 6397939 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397940
     Patch 6397940 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397941
     Patch 6397941 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397942
     Patch 6397942 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397943
     Patch 6397943 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397944
     Patch 6397944 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397945
     Patch 6397945 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397946
     Patch 6397946 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397947
     Patch 6397947 installed successfully.
INFO: Installing Oracle 10g Release 2, October 2007 CPU : 6397948
     Patch 6397948 installed successfully.
Oracle 10g Release 2, Critical Patch Update, October 2007 is installed.
---------------------------------------------------------------------
```

All logs created while applying October 2007 CPU are located under /tmp/6394981, names being 7-digit patch numbers.

NOTE: InstallDatabase script will not allow Oracle 10g to re-install if the previous installation was terminated before completing. If Oracle 10g has to be re-installed, clear all LOG files under /tmp/6394981 and re-install. Failing to do so may prevent the script from creating new LOG files at the same location.

Accessing the Linux Host

Access the Linux host by doing one of the following:

- **Using the graphics console on the localhost** - Run the following command at the command prompt:

  ```
  # /usr/X11R6/bin/xhost +
  ```

- **Accessing the Linux host from a remote Linux client**

1. Ensure that the X server on the remote client can accept TCP connections:

   a. Open `/etc/X11/xdm/Xservers`

b. Verify that the line for the screen number 0 (the line containing `:0 local`) does not contain the -`nolisten tcp` option. Remove the `–nolisten tcp` option if present. The line should look like:

```
:0 local /usr/X11R6/bin/X
```

c. Enable TCP connections on the X server of the remote client:

SUSE - Edit `/etc/sysconfig/displaymanager` and set the following options to yes: `DISPLAYMANAGER_REMOTE_ACCESS` and `DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN`.

For example: `DISPLAYMANAGER_REMOTE_ACCESS="yes"`

```
DISPLAYMANAGER_XSERVER_TCP_PORT_6000_OPEN="yes"
```

RHEL (for gnome) - Edit `/etc/X11/gdm/gdm.conf` and set the `DisallowTCP` option to false (uncomment if commented)

For example: `DisallowTCP=false`

d. If you made any changes in the configuration files during the previous steps, reboot the system for the changes to take effect.

2. Run the following command at the command prompt:

```
# /usr/X11R6/bin/xhost +
```

Then, set the display to your client. Refer to the documentation for your shell for more information.

- **Accessing the Linux host from a remote Windows client** - Start up a local X server, connect through xterm to the remote system and set your DISPLAY environment variable appropriately by using the following commands:

```
# DISPLAY=<ip-address>:displaynumber.screennumber
```

where `<ip-address>` is the address of the client from which the Installer script is launched.

```
# export DISPLAY
```

For Example:

```
# DISPLAY=172.168.10.15:0.0
# export DISPLAY
```

Step 2 - Install the Management Server

If you are installing the management server from a network drive, follow the instructions as described in "Installing from a Network Drive" on page 64.

IMPORTANT: Run the entire installation from the same X client window. Starting a new X session will result in the loss of environment variables required by the installer.

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.
- In this release, no RPM entry is created for management server on Linux.

- When you install the management server on Linux, you must install the software using a POSIX (Portable Operating System Interface) shell, such as sh. C Shell is not supported.
- 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.
- You must install the management server on a machine with a static IP address.
- When you install the management server on Linux, the following files from InstallAnywhere are left with writable permissions, and they should not be modified. Modifying them may impact other installations that use InstallAnywhere:
  - `$mgr_dist/Uninstall_<product_name>/.com.zerog.registry.xml`
    where $mgr_dist is the location where the management server is installed
  - `/var/.com.zerog.registry.xml`
- Verify that the required software is available on your system as described in "Software Dependencies for Storage Essentials" on page 62.

Management server installation on Linux requires a non-loopback IP address to start the Management Server (appstormanager service). Linux requires the Fully Qualified Domain Name and the IP address on separate lines on /etc/hosts for the management server to start. This is the OS default.)

The following is an example of the acceptable format:

```
# cat /etc/hosts
127.0.0.1 localhost.localdomain  localhost
15.115.235.13 meet.lab.usa.co.com  meet
```

The following format is unacceptable:

```
# cat /etc/hosts
meet.lab.usa.co.com.meet
localhost.localdomain.localhost
```

SLES10 may have an entry for 127.0.0.2 in /etc/hosts against the host name for that system. Comment out or remove the line that maps the IP address 127.0.0.2 to the systems fully qualified hostname. Retain only that line that contains the actual IP address mapped to the fully qualified host name.

Example:

```
    #  cat /etc/hosts
    #
    127.0.0.1     localhost
    127.0.0.2     demo.novell.com demo
    192.168.1.5   demo.novell.com demo
```

In the example shown above, remove or comment the line in bold as shown in the middle line.

To install the management server:

1. Access the Linux host as described in "Accessing the Linux Host" on page 75.

2. **If installing from CD-ROM:**

   Insert the CD-ROM for installing the management server in the CD-ROM drive of the server and mount it by using the following commands:

   ```
    # mkdir -p /mnt/installer
    # mount /dev/cdrom /mnt/installer
   ```

   where /dev/cdrom is the CD device.

   If installing from network NFS mount:

   Create /mnt/installer directory on the server where the NFS drive (for example, /installSE) is mounted and where management server will be installed:

   Then, create a directory on which the NFS drive will be mounted:

   ```
   #mkdir /InstallSE
   ```

   Mount the NFS shared network drive from NFS server (example: "pillbox") with shared drive "InstallSE", with strong recommendation to set it as read only.

   ```
   #mount pillbox:/InstallSE  /InstallSE
   #mkdir /mnt/installer
   ```

   Loop mount the ManagerCDLinux.iso to the /mnt/installer directory.

   ```
   #mount -o loop,ro /InstallSE/ManagerCDLinux.iso /mnt/installer
   ```

   For more information about installing from a network drive, see ”Installing from a Network Drive” on page 64 in this chapter.

3. Enter the following at the command prompt (if you mounted the CD device at the `/mnt/installer` location)

   ```
    # /mnt/installer/InstallManager.bin
   ```

4. When you see the introduction screen, Select **Next**.

5. When you are asked for an installation directory, you can select the default or choose your own. To choose your own directory, select the **Choose** button. You can always display the default directory by selecting the **Restore Default Folder** button. When you are done, select **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 your edition for information about supported hardware.

7. Do one of the following:

   - Select **Install** if you agree with the pre-installation summary.
   - Select **Previous** if you want to modify your selections.

   The management server is installed.

CAUTION: Do not select 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. Enter the following at the command prompt:

   ```
   # /etc/init.d/appstormanager start
   ```

IMPORTANT: You will have to set the new Oracle 10g database to ARCHIVE MODE in order to enable automatic RMAN backups. See the User Guide in the Documentation Center (Help > Documentation Center) for steps.

Step 3 - Verify that Processes Can Start

After you install the management server, verify the process for the management server has started. It may take some time for the process to start depending on the server's hardware. The process must be running to monitor and manage your elements. Refer to the appropriate section for your operating system.

Verify that the processes for Oracle and the management server have started.

1. To verify the Oracle processes have started, enter the following at the command prompt:

   ```
   # /etc/init.d/dbora status
   ```

Output resembling the following is displayed:

```
##########################################################################
#                  Begin of   O R A C L E   status section               #
##########################################################################

Kernel Parameters
Shared memory:  SHMMAX= 3294967296  SHMMNI= 4096  SHMALL= 2097152
Semaphore values:  SEMMSL, SEMMNS, SEMOPM, SEMMNI:  1250 32000 100 256

Database-Instances
Instance * is down \(autostart: N\)
Instance APPIQ is up \(autostart: Y\)

TNS-Listener: up

Process list for user oracle:
  PID TTY      STAT   TIME COMMAND
17158 ?        Ss     0:00 ora_pmon_APPIQ
17176 ?        Ss     0:00 ora_psp0_APPIQ
17187 ?        Ss     0:00 ora_mman_APPIQ
17200 ?        Ss     0:00 ora_dbw0_APPIQ
17209 ?        Ss     0:00 ora_dbw1_APPIQ
17212 ?        Ss     0:02 ora_lgwr_APPIQ
17214 ?        Ss     0:00 ora_ckpt_APPIQ
17216 ?        Ss     0:00 ora_smon_APPIQ
17218 ?        Ss     0:00 ora_reco_APPIQ
17220 ?        Ss     0:00 ora_cjq0_APPIQ
17222 ?        Ss     0:00 ora_mmon_APPIQ
17224 ?        Ss     0:00 ora_mmnl_APPIQ
17230 ?        Ss     0:00 ora_qmnc_APPIQ
17281 ?        Ss     0:00 ora_q000_APPIQ
17584 ?        Ss     0:00 ora_q001_APPIQ
4655 ?        Sel    0:00 /opt/oracle/product/10.2.0.1/bin/tnslsnr
                             listener -inherit
##########################################################################
#                      End of   O R A C L E   section                    #
##########################################################################
```

2. If you find your processes for Oracle have not started, you can start by entering the following at the command prompt:

   ```
   # /etc/init.d/dbora start
   ```

   If you need to stop the process for Oracle, enter the following at the command prompt:

   ```
   # /etc/init.d/dbora stop
   ```

IMPORTANT: If you are starting the processes manually, start the Oracle process before the process for the management server.

3. To verify that the required processes for the management server have started, enter the following at the command prompt:

   ```
   # /etc/init.d/appstormanager status
   ```

   The following is displayed if the processes have started:

   ```
   Checking for Cimom Service...
   Cimom Service - RUNNING.

   Checking for appstormanager service...
   appstormanager service - RUNNING.
   ```

4. If you find your processes for the management server have not started, you can start the process by entering the following at the command prompt:

   ```
   # /etc/init.d/appstormanager start
   ```

   If you need to stop the process, enter the following at the command prompt:

   ```
   # /etc/init.d/appstormanager stop
   ```

5. The appstormanager service is available with the following options:

   ```
   # /etc/init.d/appstormanager
   ```

   Usage: `/etc/init.d/appstormanager { start | stop | restart | status | force-reload }`

6. If the status indicates that the CIMOM service is not running, then one of the following is true:
   - The CIMOM service has not yet started. It usually takes some time for the CIMOM process to start.
   - The TNS listener process is not running. This happens when the hostname is wrongly mapped to the loopback address (127.0.0.1) in the `/etc/hosts` file. Verify that `ping <hostname>` pings the IP address for the host and not the loopback address. If it pings the loopback address, edit the `/etc/hosts` file and make the appropriate corrections. After verifying that the correct IP address is being pinged, follow steps mentioned in the following bullet to remove the management server and the Oracle database.
   - The APPIQ database was not created successfully, and the management server needs to be re-installed. If this is the case, uninstall the management server as described in steps 1 through 5 of "Removing the Management Server" on page 89. Then remove the APPIQ database by doing the following-

     1. As root user, stop the Oracle services by executing the following

        ```
        /etc/init.d/dbora stop
        ```

     2. Login as oracle user

        ```
        su - oracle
        ```

     3. As oracle user, execute the following command to delete the APPIQ database-

        ```
        dbca -silent -deleteDatabase -sourceDB APPIQ
        ```

4. Check to see if the file /etc/oratab has an entry that looks like

   ```
   APPIQ:/opt/oracle/product/10.2.0.1:Y
   ```

   If it does, then as the root user, delete the line and save the file.

5. If they exist, as root user, delete the APPIQ directories under `/opt/oracle/product/10.2.0.1/oradata` and `/opt/oracle/product/10.2.0.1/admin`:

   ```
    rm -rf /opt/oracle/product/10.2.0.1/oradata/APPIQ
   rm -rf /opt/oracle/product/10.2.0.1/admin/APPIQ
   ```

Do not remove the Oracle Software. Install the management server as described in "Step 2 - Install the Management Server" on page 76.

Step 4 - Install and Configure HP SIM

IMPORTANT: The steps in this section are only for installing and configuring HP SIM on the same server as Storage Essentials. If you are installing HP SIM on a different server, skip this section. After you install HP SIM by using the directions provided in the HP SIM documentation, continue the installation steps with "Step 5 - Install the HP SIM Connector" on page 85.

NOTE: Remove any existing version of postgreSQL before installing HP SIM.

To install HP SIM:

1. Download the HP SIM installation file from http://www.hp.com/go/hpsim.
2. Change the file permission by entering the following command:

   ```
   # chmod 700 HPSIM-Linux_C.05.01.00.00.bin
   ```

3. Enter the following command:

   ```
   #./HPSIM-Linux_C.05.01.00.00.bin
   ```

4. Configure HP SIM to use the Oracle database by entering the following command:

   ```
   # /opt/mx/bin/mxoracleconfig
   ```

   You will be prompted for information about the Oracle database:

   - Host: Fully qualified domain name of the server (for example, `host1.rose.hp.com` or `host2.domain1.rose.hp.com`)
   - Port:1521
   - Database Name: APPIQ
   - Username: SIM_MANAGER
   - Password: use the new password if you have changed the password, otherwise input the default password "quake"
   - Jar File: /opt/oracle/product/10.2.0.1/jdbc/lib/classes12.jar

NOTE: This path may differ if Oracle is not installed in the default path

- Force[N]: For fresh installations, select the default [N]. If the initial installation fails, select [Y] for subsequent installations.
- Select defaults for the rest of the options and install.

5. Initialize and configure HP SIM by executing the following command:

   ```
   #/opt/mx/bin/mxinitconfig -a
   ```

   NOTE: The initialization is done in the background and takes several minutes.

6. Verify that the mxdomainmgr, mxdtf, and mxinventory daemons are running. Mxinventory is an HP SIM database process. If mxinventory is not running, you cannot browse to HP SIM. Verify these processes are running by executing the following command:

   ```
   #ps -ef | grep mx
   ```

Change the SIM_MANAGER Password (Optional)

The information HP SE and HP SIM share is stored in a database with the user name SIM_MANAGER and the default password quake. For security reasons, it is strongly recommended you change the password for this database.

NOTE: This step only applies if HP SE and HP SIM are installed on the same server.

Make sure you keep the new password for SIM_MANAGER 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 change the password for SIM_MANAGER:

1. Log onto the server running HP SIM
   - Start the HP SIM service if it is not already started.
     Verify that the mxdomainmgr and mxdtf daemons are running by executing the following command:
     ```
     # ps -ef | grep mx
     ```
     If necessary, start the HP Systems Insight Manager service:
     ```
     # /opt/mx/bin/mxstart
     ```
2. Stop the appstormanager service, if it is started:

   ```
   /etc/init.d/appstormanager stop
   ```

3. Enter the following at the command prompt:

```
[/opt/mx/bin]# ./mxpassword -m -x MxDBUserPassword=mynewPass
```

   where `mynewPass` is your new password for the Oracle database.

4. Run the following command to stop the HP Systems Insight Manager service so that it cannot access the database:

```
# /opt/mx/bin/mxstop
```

> **IMPORTANT:** It is very important that the HP Systems Insight Manager service does not access the Oracle database before you are finished with changing the password for the Oracle database.

5. Use the Database Admin Utility to change the SIM_MANAGER password in the Oracle database.

> **IMPORTANT:** You must provide the same SIM_MANAGER password for the mxpassword command and the Database Admin Utility.

a. To access the Database Admin Utility, go to the `/opt/productname/tools/dbAdmin Directory`.

b. The dbAdmin utility uses Perl. To set Perl in your path, enter the following command:

```
# . /opt/productname/install/setvars.sh
```

where `/opt/productname` is the directory containing the software.

c. Set the DISPLAY environment variable to point to the host that is running an X-Server.

For example: `# export DISPLAY=<host-IP>:0.0`

d. Run the dbAdmin utility by entering the following command:

```
#  perl dbAdmin.pl
```

e. If you are shown an error message when you start the Database Admin Utility, stop the appstormanager service by running the following command, and then selecting **Refresh**:

```
# /etc/init.d/appstormanager stop
```

f. Select **Change Passwords** in the left pane.

g. Select SIM_MANAGER from the **User Name** combo box.

h. Enter the current password in the **Old Password** box.

i. Type the new password in the **New Password** box.

j. Reenter the password in the **Confirm Password** box.

k. Select **Change**.

The Database Admin Utility changes the password for the specified account. Select **EXIT** to exit the Database Admin Utility.

l. Restart the HP Systems Insight Manager service:

```
# /opt/mx/bin/mxstart
```

m. Restart the appStorManager service.

```
# /etc/init.d/appstormanager start
```

Step 5 - Install the HP SIM Connector

The HP SIM Connector lets Storage Essentials communicate with HP SIM. Install the HP SIM Connector on the same server running Storage Essentials.

To install the HP SIM Connector:

1. Stop the appstormanager process with the following command:

   ```
   # /etc/init.d/appstormanager stop
   ```

2. Make sure these three HP SIM mxdomainmgr, mxdtf, and mxinventory processes are running on the HP SIM server by using the following command:

   ```
   # ps -ef | grep mx
   ```

3. Set the DISPLAY environment variable using the following commands:

   ```
   # DISPLAY=<ip-address>:displaynumber.screennumber
   # export DISPLAY
   ```

   where `<ip-address>` is the address of the client from where the Installer script is launched.

   ```
   For Example:
   # DISPLAY=172.168.10.15:0.0
   # export DISPLAY
   ```

4. Insert the CD-ROM for installing Storage Essentials in the CD-ROM drive of the server running Storage Essentials and mount by using the following commands:

   ```
   # mkdir -p /mnt/HPSIMConnector
   # mount /dev/cdrom /mnt/HPSIMConnector
   ```

   where `/dev/cdrom` is the CD device.

5. Start the Connector installer (for SUSE and RHEL) with the following command:

   ```
   # /mnt/HPSIMConnector/SIMConnectorInstall.bin LAX_VM
   <install_loc>/jre/bin/java
   ```

   Where `<install_loc>` is the directory containing the software.

6. Follow the instructions on the screen for completing the installation.

7. When you see the HP SIM Information screen, provide the following information:

   - **HP SIM Hostname** - Name of the server on which you installed HP SIM. Do not use localhost or an IP address. The FQDN (fully qualified domain name) is required if the server is part of a domain (for example: `server.domain.xxx.com`).
   - **HP SIM Administrator Name** - Provide the Administrator name that is used to access HP SIM.
   - **HP SIM Administrator Password** - Provide the password for the Administrator.

   NOTE: The HP SIM Administrator will be assigned the HP Storage Essentials Administrator role (Domain Admin). See "About Roles" on page 349 for more information.

8. Complete the installation by following the instructions on the screen.

9. After the installation is complete, restart the HP SIM process by entering the following command:

   ```
   # /opt/mx/lbin/hpsim restart server
   ```

10. Verify that the HP SIM mxdomainmgr, mxdtf, and mxinventory processes are running by entering the following command:

    ```
    # ps -ef | grep mx
    ```

    NOTE: You can also verify that the HP SIM processes are running by waiting until you can browse to the HP SIM server (https://<HP SIM Host Name>:50000).

11. Start the Storage Essentials process by entering the following command:

    ```
    # /etc/init.d/appstormanager start
    ```

12. Verify that the Storage Essentials process has started by entering the following command:

    ```
    # /etc/init.d/appstormanager status
    ```

Considerations when Uninstalling SIM Connector

If you need to uninstall the SIM connector at a later time, be aware of the following considerations:

The SIM connector consists of two parts, the HP SIM side of the connector and the Storage Essentials side of the connector. In a typical uninstall, both parts of the connector are removed. However, if HP SIM is not running or cannot be contacted, it is possible to go ahead and remove only the Storage Essentials side of the connector. In this case, HP SIM will still contain Storage Essentials objects such as menu items, links, queries, and collections. However, the Storage Essentials items will not function.

If the SIM Connector Uninstaller detects that HP SIM is not available, you see a message similar to the following:

```
HP Systems Insight Manager is not available. Click Cancel to exit the
uninstall or Continue to remove only the Storage Essentials SIM
Connector.
```

The following is a description of your options:

- Cancel the uninstall. (Recommended option). After cancelling the connector uninstall, you can restart HP SIM. Once it is up, you can restart the uninstall.
- Continue the uninstall. This removes only the Storage Essentials side of the connector.

NOTE: Choose the Continue option only if you do not intend to use this installation of SIM in the future, either on its own or integrated with Storage Essentials.

Step 6 - Configure SUSE Linux for Use with Business Tools

If you are running the management server on SUSE Linux, and Storage Essentials and HP SIM are on the same machine, you must complete these steps if you intend to use Business Tools. Only the root user can perform these steps.

1. Restart the HP SIM process by entering the following command:

    ```
    # /opt/mx/lbin/hpsim restart server
    ```

2. Restart Storage Essentials by entering the following command:

   ```
   # /etc/init.d/appstormanager restart
   ```

3. Enter the following command:

   ```
   # . <productname>/install/setvars.sh
   ```

   where <productname> is the directory containing the software, the default value being `/opt/HP_Storage_Essentials`

4. Run `appiqconfig` and input the HP SIM credentials. Use the default settings when applicable. Run `appiqconfig` by entering the following commands:

   ```
   # cd <productname>/cli/bin/
   ```

   where <productname> is the directory containing the software, the default value being /opt/HP_Storage_Essentials.

   ```
   # ./appiqconfig -username <name> -password <passwd> -server <ip/name>
   -transport <transport> -port <port>
   ```

Step 7 - Browse to HP SIM Home Page

1. Wait until HP SIM is fully started. HP SIM has fully started when you can bring up the HP SIM Home page.
2. Start the Storage Essentials (appstormanager) process by using the following command:

   ```
   # /etc/init.d/appstormanager start
   ```

3. You should now be able to access HP SIM from a web browser using the URL https://<FQDN of HP SIM server>:50000 (for example https://example.domain.com:50000). The host name must be fully qualified.
4. Supply the login for the user that was used to install HP SIM.

Step 8 - Configure Firefox

Firefox should be properly configured before accessing the management server from a Linux client.

The RHEL 4 OS distribution comes with Firefox. RHEL 4 (U3) includes Firefox version v1.0.7 which is not supported. RHEL 4 (U4) includes the supported Firefox version v1.5.0.3.

The SUSE OS distribution does not come with Firefox.

To install and configure Firefox v1.5.0.1 or later on Linux:

1. Download Firefox from http://www.mozilla.com/firefox/all.html
2. Extract the depot in a suitable location such as `/usr/sbin`
3. Run the following commands:

   ```
   # cd <USER_HOME_DIR>/.mozilla/plugins
   # ln -s /opt/<product_name>/jre/plugin/i386/ns7
   /libjavaplugin_oji.so .
   ```

   NOTE: Remember the dot at the end of the command.

4. Go to the `/usr/sbin/firefox` directory. Set the DISPLAY appropriately and open an X-server on your client.

5. Launch Firefox by entering the following command:

   ```
   # /usr/sbin/firefox/firefox
   ```

6. Open Firefox Preferences by selecting **Edit** > **Preferences**.
7. Select **Connection Settings** and set the **Manual proxy configuration** appropriately. Select the **Use this proxy server for all protocols** checkbox.
8. Select the **Content** tab and disable the pop-up blocker.

Step 9 - Import a Storage Essentials License

You can add or delete licenses from **Deploy** > **Storage Essentials** > **License Manager** > **Manage Storage Essentials Keys** in HP SIM.

Installing the Java Plug-in on Linux

Java 2 Runtime Environment is required to access several features in the management server, such as System Manager. If your Web browser is running on Linux, you must manually install the Java plug-in as described in this section.

To install the Java plug-in:

1. Go to the following URL and download the installation file for the Sun JRE when asked:

   ```
   http://<management_server>/servlet.html?page=JavaPluginLinux
   ```

   where `<management_server>` is the hostname of the management server.
2. In a terminal window, execute the downloaded file in a directory where you want the JRE installed.

   This executable installs the Sun JRE on your computer.

   The Java plug-in for your Web browser is available in the following file:

   ```
   $JRE_HOME/plugin/i386/ns7/libjavaplugin_oji.so
   ```

   where `$JRE_HOME` is the directory containing the JRE installation.
3. Set the executable permission of the downloaded file:

   ```
   chmod +x downloaded_file_name
   ```

4. In a terminal window, go to the `$HOME/.mozilla/plugins` directory. Create a `plugins` directory if it does not exist.
5. Remove any existing links to the Java plug-in that are in this directory. You may use the `rm libjavaplugin_oji.so` command in a terminal window to remove an existing symbolic link to the Java plug-in.
6. Create a symbolic link to the Java plug-in by using the following command:

   ```
   ln -s $JRE_HOME/plugin/i386/ns7/libjavaplugin_oji.so .
   ```

NOTE: Remember the dot at the end of the command.

NOTE: If you create this symbolic link in any directory other than `$HOME/.mozilla/plugins`, your browser will not be able to use this new Java plug-in.

7. If you are a root user on the server and you want to make the plug-in available to all users, create a symbolic link to the Java plug-in that is in the `plugins` directory under the browser's installation directory.

   NOTE: Any existing plug-ins in a user's home directory take precedence over this system-wide plug-in.

8. Restart your Web browser.

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.

In Navisphere add the following to the privilege user section:

```
root@name_of_my_management_server
root@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

The management server service needs to be restarted after installing EMC Navisphere CLI.

Removing the Management Server

To remove the management server from Linux:

1. Access the Linux host and login as user “root” as described in ”Accessing the Linux Host” on page 75.
2. To uninstall the management server, enter the following at the command prompt:

```
<install_loc/productname>/Uninstall_<productname>
/Uninstall_<productname>
```

where `<install_loc/productname>` is the directory containing the software, the default value being `/opt/<product_name>`

3. To remove leftover files from the management server, remove the directory for the management server by entering the following at the command prompt:

   ```
   # rm -rf <install_loc>
   ```

   where `<install_loc>` is the directory containing the software, the default value being `/opt/<product_name>`

4. If you want to remove the EMC WideSky API that installed with the management server, enter the following command to remove the directory containing the API:

   ```
   # rm -rf /var/symapi/
   ```

   Remove the file `/var/.com.zerog.registry.xml`

5. If you are going to reinstall a new build of the management server, make sure you keep the file `/var/opt/oracle/orahome`. This file lets you install a new build of the management server by assuming you kept the same Oracle installation.

6. To remove the Oracle instance containing the data for the management server, mount the Oracle DVD as described in the steps for installing Oracle.

   a. Execute `/mnt/oradisk/UninstallDatabase` to delete the management database and uninstall Oracle 10g completely. After the database is deleted, the Oracle 10g instance is removed. Console output similar to the following displays and you will see a message similar to that shown: “Removing <management server> database...”.

```
INFO : Checking the OS Release...
Found SUSE LINUX Enterprise Server 9.
INFO: Checking System architecture...
OK.
#### This script uninstalls Oracle 10.2.0.1 for Storage Essentials ####
###############################################################
#                  Begin of   O R A C L E   shutdown section
###############################################################
Shutting down Oracle services (only those running)

###############################################################
#                   End of   O R A C L E   section                #
###############################################################
Removing Storage Essentials database...
Uninstalling Oracle ...
Starting Oracle Universal Installer...
Checking installer requirements...
Checking operating system version: must be redhat-3, SuSE-9, redhat-4,
UnitedLinux-1.0, asianux-1 or asianux-2
                                Passed
All installer requirements met.
Checking Temp space: must be greater than 80 MB.   Actual 42712 MB    Passed
Checking swap space: must be greater than 150 MB.   Actual 8195 MB    Passed
Preparing to launch Oracle Universal Installer from
/tmp/OraInstall2007-10-25_05-23-36PM. Please wait ...Oracle Universal
Installer, Version 10.2.0.1.0 Production
Copyright (C) 1999, 2005, Oracle. All rights reserved.
Starting deinstall
Deinstall in progress (Thu Oct 25 17:23:43 IST 2007)
Configuration assistant "Oracle Database Configuration Assistant" succeeded
Configuration assistant "Oracle Net Configuration Assistant - Deinstall
Script" failed
...................  35% Done.
...................  70% Done.
................... 100% Done.
Deinstall successful
End of install phases.(Thu Oct 25 17:24:41 IST 2007)
End of deinstallations
Please check
'/opt/oracle/oraInventory/logs/silentInstall2007-10-25_05-23-36PM.log' for
more details.
Oracle Database 10g Uninstallation : OK
Clearing up the Oracle installation
------INFO: Removing database startup script...
---------------------------------------------------------------
warning: /etc/profile.d/oracle.sh saved as /etc/profile.d/oracle.sh.rpmsave
```

```
no crontab for oracle
Done.
```

7. Verify that the directory `/opt/oracle` AND the account "oracle" do not exist.

   NOTE: Files created during Oracle install are removed along with the oracle user account. Since SLES systems require an oracle user account to be present before installing, make sure the correct version orarun RPM is installed before installing Oracle 10g again. For SLES9, orarun RPM can be found at:
   http://ftp.novell.com/partners/oracle/sles-9/
   For SLES10, orarun RPM can be found in the product CD.

8. Reboot the server.

Upgrading the Linux Management Server from Build 5.1 to Build 6.0 (Contact Your Account Representative Before Upgrading)

IMPORTANT: Please contact your Account Representative for upgrades. Upgrading requires assistance from HP Services.

Prior to beginning the upgrade, ensure your system and software environment meets the version requirements for the upgrade, as stated in the Support Matrix and related documents.

IMPORTANT: As part of upgrading the management server, related passwords are set to their defaults. See the User Guide in the Documentation Center (**Help > Documentation Center**) for more information on default passwords. It is recommended that you customize your passwords following the upgrade process.

Considerations Before You Upgrade

Before you begin, consider the following:

- Refer to the Release Notes for late breaking information about upgrading the management server.
- The latest build of the software requires you to migrate your Brocade switches to the Brocade SMI-Agent Provider (SMI-A). Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot do Discovery Data Collection until you migrate Brocade switches to the Brocade SMI Agent provider.

- The latest build of the software requires you to upgrade some of your CIM Extensions. Please refer to “About Upgrading Your CIM Extensions” (in the Deploying and Managing CIM Extensions chapter) for details.
- The installation will fail if there is insufficient temporary space. You must have at least 2 GB in the /tmp directory.
- After you upgrade the software, you are required to run HP SIM Discoveryand do Discovery Data Collection on all new and existing managed elements. This allows the software to gather any new data that is associated with the new features available in the latest release.
- Windows hosts using SecurePath – SecurePath information is not retrieved from legacy CIM extensions.
- After you upgrade, you need to rediscover backup details. Make note of your Backup Manager hosts. Refer to Backup Managerfor a list of Backup Manager hosts.
- The following elements are not supported even though they were supported in Service Pack 4, Build 5.1 of the management server:
  - Cisco switches with firmware versions earlier than 3.1.x for switches discovered through SMI-S. You need to upgrade to version 3.2.(2c) if you want to discover the Cisco switches through SMI-S.
  - Brocade SMI-A versions prior to 120.6.0a. You need to upgrade to at least version 120.6.0a.
- You should try to complete the upgrade and its subsequent steps in one session, which may take several hours, depending on your network configuration.
- It is necessary to perform Discovery Data Collection after you upgrade to repopulate the database.
- Upgrade and start the Windows proxy service first and then the management server.
- Some upgrade-related steps are required after the upgrade, as indicated later in this section.
- Any customizations to your CIMOMConfig.xml will not be preserved, because the file format has changed. The old file will be saved for reference. The customizations in the old CIMOMConfig.xml file must be manually merged into the file shipped with 6.0 and you must restart the CMS before the customizations are applied to the updated CMS. Depending upon the customizations, starting the CMS using the default CIMOMConfig.xml file can have varying impacts.
  - If end-users change the port number of some of the discovery groups and then start the CMS using the default config file, the discovery groups may not start up since the default ports may be in use.
  - If end-users modify the repository location and start the CMS using the default config file, the system fails to locate the discovered elements in the new repository created in the default location. If this happens, reapply the customizations to the new CMS or end-users will have problems running discovery or collecting data.
- Users who wish to continue gathering backup data from their backup manager hosts must update the CIM extensions on those hosts. The procedure for upgrading the CIM extension on a backup managing host is the same as for any host.

- The Brocade switch manufacturer no longer supports the Brocade Fabric Access API provider and as a result, this release of the management server does not support the Brocade Fabric Access API after updating.
- If you are installing from a network drive, see the section at the beginning of this chapter, "Installing from a Network Drive" on page 64

Upgrade Overview

The following table summarizes the steps to upgrade the management server, and the steps following the table provide additional information about the upgrade process. Make sure you have a functional management server before starting the upgrade. Also, be sure you have completed any necessary pre-upgrade steps prior to starting the upgrade.

NOTE: Systems running an integrated Storage Essentials Build 5.1.1 and HP SIM Version 5.0 must upgrade HP SIM to Version 5.1, or higher (supported versions only), before upgrading to Storage Essentials Build 6.0.0

Table 1:

Upgrade	New Install	Description
upgradeAppStorManager.sh	Not Applicable	Initiates the upgrade process Checks for prerequisite conditions and exits if any condition is not satisfied. Stops running services and exports current database to a temporary location
uninstallOracle9i.sh	Not Applicable	Removes the existing Oracle 9i installation, clears remaining files and removes the Oracle user account
InstallDatabase	InstallDatabase	Installs Oracle 10g
Install Management Server	Install Management Server	Installs Management Server. Upgrades code base and database schema files, if an existing Management Server installation is discovered
Install/Upgrade HP SIM	Install or Upgrade HP SIM	Install/Upgrade HP SIM, if required

Table 1:

Upgrade	New Install	Description
migrateData.sh	Not Applicable	Verifies if the database is created properly and imports database exported by upgradeAppStorManager.sh
Install HP SIM Connector	Install HP SIM connector for Build 6.0.0	Install SIM connector for Build 6.0.0

Steps to Upgrade the Management Server

Step 1 - Read the Support Matrix and Release Notes

Read the support matrix and release notes. Read the support matrix to make sure the servers on which you are upgrading the management server meet or exceed the requirements. Management server requirements are listed on the Manager Platform (Mgr Platform) tab of the support matrix. Also, read the release notes for late breaking issues not covered in the Installation Guide. The release notes and support matrix can be found on the top-level of the management server CD and the CIM extension CDs.

Step 2 - Verify that You Are Running Build 5.1 Service Pack 4 or a Later 5.1 Service Pack

Verify that you have a working Build 5.1, SP4 management server before upgrading to Build 6.0. Existing installations that are at Build 5.1, SP1, Build 5.1, SP2, or Build 5.1, SP3, must upgrade to Build 5.1, SP4 or later prior to upgrading to Build 6.0. In an integrated Storage Essentials/SIM environment, you must also upgrade to the Service Pack 4 connector. If using the HP Kit in an integrated Storage Essentials/SIM environment, you must first install SP3, if you are not currently at SP3 or SP4.

Step 3 - Save Configuration Files for the Global Change Management Business Tool

Make a copy of the configuration files saved through the Global Change Management Business Tool. The configuration files are not retained after you upgrade the product. These files are located in the “advisors/saved-configuration” area on the management server. Place these files back after the upgrade or reinstall. If you do not use Global Change Management or do not wish to keep the old configurations, you may ignore this step.

Step 4 - Upgrade HP SIM

Upgrade HP SIM in this step. In the case of a dual box installation, the SIM upgrade procedure should be carried out on the server where HP SIM is installed.

- If you are running a version before HP SIM 5.1, you should upgrade HP SIM during this step.
- Stop appstormanager services prior to starting this step.
- Your integrated environment will be non-operational until after the completion of the connector upgrade in a later step.

Step 5 - Run the upgradeAppStorManager Script

Run the upgradeAppStorManager.sh script from the Oracle disk to begin the upgrade process.

- The script upgradeAppStorManager.sh initiates the upgrade process. It checks for prerequisite conditions and exits if any condition is not satisfied. It stops running services and exports the current database to a temporary location. All output will be logged to a time stamped file named `upgradeAppStorManager_<timestamp>.log` in `/var/tmp/.appstor`.
- The upgradeAppStorManager.sh script stops the management server before proceeding with Oracle9i uninstall.
- The upgradeAppStorManager.sh script also stops the HP SIM services before proceeding with Oracle 9i uninstall. For a dual-box integrated system, where HP SIM is installed on a remote box, the SIM service must be stopped manually before executing upgradeAppStorManager.sh. If the SIM connector is installed, the script will prompt the user to uninstall the connector before running the upgrade script. Uninstalling the HP SIM connector is described earlier in this chapter, following the installation steps, in the section "Considerations when Uninstalling SIM Connector" on page 86. Make sure the HP SIM service is running before and after uninstalling the SIM connector.
- In a SIM/SE integrated setup, in order to upgrade the Oracle database, the password for SIM_MANAGER oracle user account must be reset to its default value ('quake'). If the password for the SIM_MANAGER Oracle user account was changed and is not the default password, the following actions apply.
  - In a single box deployment, an attempt will be made to automatically change the password used by SIM using the "mxpassword" command. If the script detects that this command failed, the following message is shown:

```
Unable to reset password of Oracle user account SIM_MANAGER.

In order to upgrade the Oracle database, the password of Oracle user account
SIM_MANAGER must be reset to its default value.

Please run the following command given to reset the password:
/opt/mx/bin/mxpassword -m -x MxDBUserPassword=quake

Continue if the password is reset [y/n]
```

    In such case, execute the mxpassword command in a separate shell window and continue the upgrade procedure by typing 'y' at the prompt.

  - In a dual box deployment, the user has to manually run the mxpassword command on the remote SIM system. The following message is shown:

    WARNING: In order to upgrade the Oracle database, the password of Oracle user account SIM_MANAGER must be reset to its default value.

    Please run the command given below on the system where SIM is installed to reset the password.

    mxpassword -m -x MxDBUserPassword=quake

Continue if the password is reset [y/n]

At this time, you should login to the remote SIM system and run the mxpassword command to reset the password at the SIM end, and then continue the upgrade procedure by typing 'y' at the prompt.

Step 6 - Run the uninstallOracle9i Script

NOTE: Before running uninstallOracle9i.sh, make sure that AppStormanager service is not running. You should also make sure that the HP SIM service is not running.

Run the uninstall script to uninstall the Oracle 9i installation.

- Run the uninstall script "uninstallOracle9i.sh" from the Oracle disk to uninstall the Oracle 9i installation. This removes the existing Oracle 9i installation, clears remaining files, and removes the Oracle user account. All output will be logged to a timestamped file named uninstallOracle9i_<timestamp>.log in /var/tmp/.appstor.

  NOTE: After Oracle9i is uninstalled, ensure that the oracle listener and other oracle processes are NOT running. Execute the following command and verify that the command does not show any active processes:

  ```
  ps -ef | grep oracle | grep -v grep
  ```

  If any oracle processes are still running, stop them by executing the kill command as shown in the following:

  `kill -9 <process-id>` (where <process-id> is the id of each process returned by the previous command)

- If you are running SuSE Linux on the machine, for SLES 9, you must install the orarun-1.8-109.15 RPM to create an Oracle user account. This user account was removed by uninstallOracle9i.sh in the previous script. (The RPM for SLES 9 is at http://www.novell.com/products/server/oracle/software.html.)
- After installing the RPM, enable the oracle user account by editing the file /etc/passwd and setting the path to the shell for this account.

  NOTE: For more information about uninstalling Oracle using the scripts, see the Troubleshooting section in this Installation guide "Troubleshooting Installation/Upgrade" on page 379.

Step 7 - Install the Oracle 10g Database

Install the database.

- Run the script `InstallDatabase` from the Oracle disk to install the database. All output will be logged to a time stamped file named InstallDatabase_<timestamp>.log to `ORACLE_HOME`.

- An Oracle account is created automatically for Red Hat Linux machines. If the Oracle account is not enabled for SUSE Linux machines, then the InstallDatabase script will exit with an error. To enable the account on SUSE Linux machines, edit `/etc/passwd` and set the path to the shell.
- Once Oracle 10g is installed, source the orahome created after the Oracle 10g installation by running `. /var/opt/oracle/orahome` and note there is a space between the period (.) and /var.

Step 8 - Upgrade the Management Server

Install the Management Server from the Management Server disk to perform the upgrade.

- Install the management server as described in this chapter, "Step 2 - Install the Management Server" on page 76. The installation process will determine that the previous management server build has been found and will ask if you want to upgrade the management server. Select **Next** to continue the upgrade process.

The following needs to be done only if the integrated SIM/SE setup is in shared mode. For example, if SIM is using SE's database (single or dual box), execute the commands in the order shown.

NOTE: If HP SIM is installed/upgraded, then the HP SIM database must be re-initialized. If the SIM_MANAGER oracle user account password was changed and is not the default password ('quake'), ensure that you have completed the action as described in the Upgrading section of this chapter, "Run the upgradeAppStorManager Script".

- Execute the following command to reset HP SIM:

```
/opt/mx/bin/mxinitconfig -r
```

- Then execute the following command to configure HP SIM:

```
/opt/mx/bin/mxinitconfig -a
```

Step 9 - Import the Database

Import the database that was exported by upgradeAppStorManager.sh previously, using the migrateData script that is present in the Oracle disk.

- Run migrateData.sh to import data exported by upgradeAppStorManager.sh.
- All output will be logged to a time stamped file named migrateData_<timestamp>.log to `/var/tmp/.appstor`.

Step 10 – Upgrade the HP SIM Connector

Upgrade the HP SIM connector by referring to the HP SIM connector installation steps described in this chapter previously, "Step 5 - Install the HP SIM Connector" on page 85. Be sure to follow the important directions in the following note.

IMPORTANT: It is critical that you start SIM before you start Storage Essentials. Do the following: Restart the HP SIM process by entering the following command:

```
# /opt/mx/lbin/hpsim restart server
```

Then verify that the HP SIM mxdomainmgr, mxdtf, and mxinventory processes are running by entering the following command:

```
# ps -ef | grep mx
```

You can also verify that the HP SIM processes are running by waiting until you can browse to the HP SIM server (https://<HP SIM Host Name>:50000)

Do not start appstormanager service until HP SIM login page displays, otherwise connector might not work properly.

Step 11 - Start Management Server

Start the appstormanager service after the HP SIM service has started. To verify if HP SIM has started, verify if you are able to launch the SIM login page. The HP SIM login URL is https://<hpsim-server>:50000.

Execute the following command to start the management server (appstormanager service):

```
    /etc/init.d/appstormanager start
```

Step 12 - Customize Database Passwords

During the upgrade, all Oracle passwords are reset to their defaults, including the TNS listener password, and the passwords for the SYS, SYSTEM, DB_SYSTEM_USER, SIM_MANAGER, RMAN_USER accounts. Please change these passwords using the Database Admin tool after the upgrade is completed successfully. This is stated in the console output that is displayed during the upgrade process. If you change the SIM_MANAGER password, you will also need to update HP SIM using the “mxpassword” command as described in this chapter.

Step 13 - Enable RMAN Backup if Desired

RMAN Backup is disabled by default as part of the upgrade process. When you log into the management server after upgrade, you will see a message informing you that RMAN Backup is disabled. You should re-enable RMAN Backup as soon as possible so you do not stop backing up your data.

Step 14 - Upgrade Selected CIM Extensions

Upgrade CIM extensions on servers with the following functionality:

- Backup Manager Hosts - Backup information is not gathered from legacy CIM extensions. In order for backup information to be gathered by the management server, the CIM extensions on the Backup Manager Host must be at the same software version as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host in order to continue to see backup data.
- Windows hosts using SecurePath – SecurePath information is not retrieved from legacy CIM extensions.

- Host for which you want to retrieve cluster information (i.e., Veritas Cluster Server on Solaris cluster and Microsoft Cluster Server). (This is new functionality that requires version 6.0 of the CIM extension.)
- Linux hosts that support QLogic failover. (This is new functionality that requires version 6.0 of the CIM extension.)

Step 15 - Rediscover All Elements

You should rediscover all elements after you do an upgrade by doing HP SIM Discoveryand Discovery Data Collection. Doing HP SIM Discoveryand Discovery Data Collection is important because:

- Better scalability is provided after discovery.
- Cluster functionality. To use the new functionality, upgrade CIM Extensions to version 6.0. Rediscovery is required.
- You will see the following issues until you do HP SIM DiscoveryandDiscovery Data Collection:
  - Reports and Capacity Manager/Capacity Explorer show incorrect raw capacity data for storage systems.
  - There is no trunked status indication on Brocade fabrics.
  - No NPIV status indication.
  - No provisioning for 3PAR storage systems and HP StorageWorks EVA arrays using Command View EVA 5.03, 6.0.1, 6.0.2, or 7.x.
  - New hosts modes on storage systems are not available.
  - Backdata collection would be suspended until CIM extensions on Backup Manager Hosts are upgraded to version 6.0 and they are rediscovered.

Steps that Can Be Run Anytime after the Upgrade

The following steps can be completed anytime after the upgrade; however, you will have reduced functionality with the product until you complete these steps.

Re - Add Remote Sites in Global Reporters

After the upgrade, add remote sites in Global Reporters. This topic is covered in more detail in this guide, in the chapter, Installing the Management Server on Microsoft Windows.

IMPORTANT: After upgrade, all remote sites in the Global Reporters are removed. This is done so you can have a chance to upgrade the remote sites to the same build before Global Reporter attempts to gather data. Before you re-add the remote sites, be sure to upgrade them to the same build as the management server.

Migrate Your Brocade Switches to SMI-A

The latest build of the software requires you to migrate your Brocade switches to SMI-A. Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch.

Any Brocade switches that are managed with the Brocade Fabric Access API provider will be quarantined after upgrading the management server. The management server retains the data for the API switches after upgrading, but you cannot do Discovery Data Collection until you migrate Brocade switches to the Brocade SMI Agent provider.

The latest build of the software requires you to upgrade some of your CIM Extensions. See "About Upgrading Your CIM Extensions" on page 189.

You will need a new proxy server for Brocade. See the support matrix for requirements.

About Migrating Your Brocade Switches to SMI-A

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Discovery Data Collection schedule. If the Brocade switches were part of a Discovery Data Collection schedule prior to migration, you must manually adjust those schedules to run Discovery Data Collection for the migrated Brocade switches. If the schedules are not adjusted manually, Discovery Data Collection will not run for the migrated switches as per pre-migration schedules.

Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

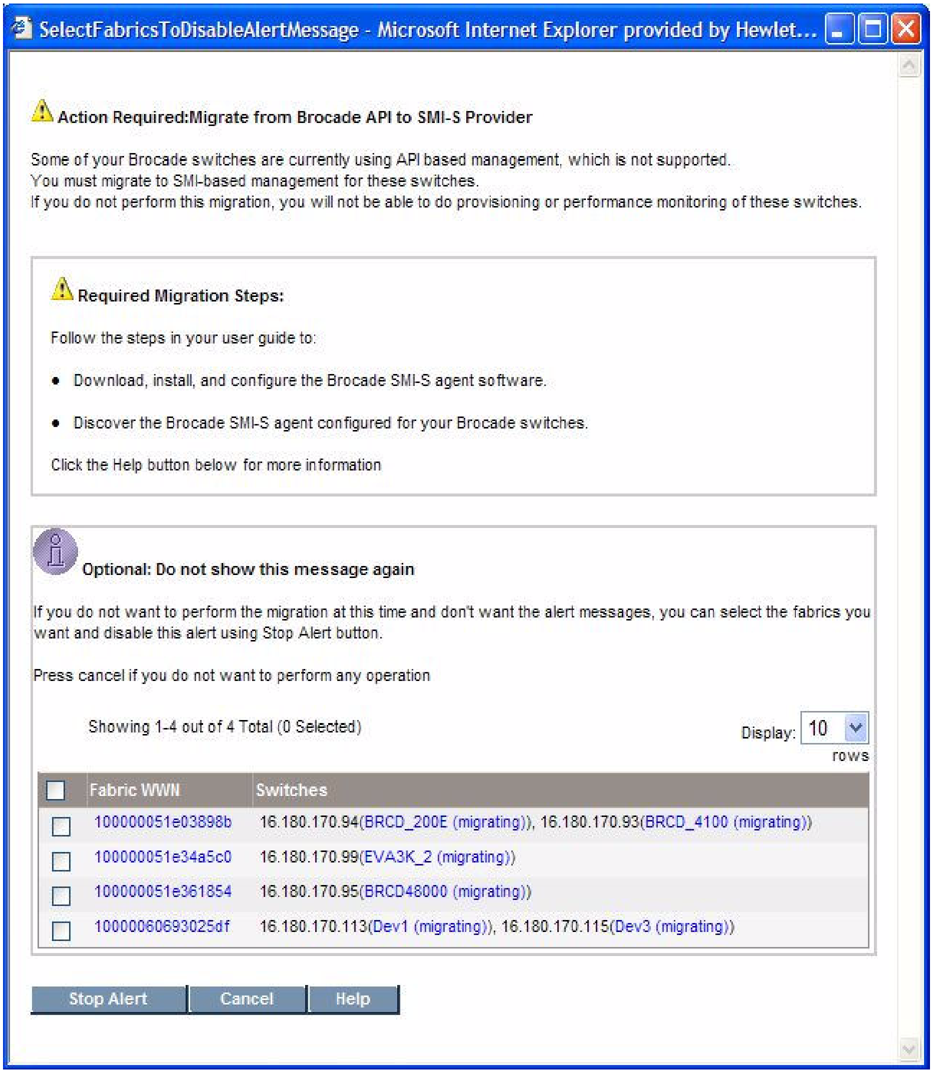
1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:

   http://www.brocade.com/support/SMIAGENT.jsp

   See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the

installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

3. Log on to the management server. HP Storage Essentials alerts you to migrate your Brocade Fabric Access API switches when you first log on.



SelectFabricsToDisableAlertMessage - Microsoft Internet Explorer provided by Hewlet...

⚠ Action Required:Migrate from Brocade API to SMI-S Provider

Some of your Brocade switches are currently using API based management, which is not supported.
You must migrate to SMI-based management for these switches.
If you do not perform this migration, you will not be able to do provisioning or performance monitoring of these switches.

⚠ Required Migration Steps:

Follow the steps in your user guide to:

- Download, install, and configure the Brocade SMI-S agent software.
- Discover the Brocade SMI-S agent configured for your Brocade switches.

Click the Help button below for more information

Optional: Do not show this message again

If you do not want to perform the migration at this time and don't want the alert messages, you can select the fabrics you want and disable this alert using Stop Alert button.

Press cancel if you do not want to perform any operation

Showing 1-4 out of 4 Total (0 Selected)

Display: 10 rows

□	Fabric WWN	Switches
□	100000051e03898b	16.180.170.94(BRCD_200E (migrating)), 16.180.170.93(BRCD_4100 (migrating))
□	100000051e34a5c0	16.180.170.99(EVA3K_2 (migrating))
□	100000051e361854	16.180.170.95(BRCD48000 (migrating))
□	10000060693025df	16.180.170.113(Dev1 (migrating)), 16.180.170.115(Dev3 (migrating))

Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

4. Run HP SIM discovery for the Brocade proxy server. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

5. Run Discovery Data Collection. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

The Brocade switches are migrated to the SMI-A provider.

> **IMPORTANT:** Before performing any provisioning operations that involve a Brocade switch you must perform Discovery Data Collection for any subset of elements that includes the Brocade switch.

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Discovery Data Collection schedules as described in the following steps:

   a. Select **Options** > **Storage Essentials** > **Discovery** > **Schedule Discovery Data Collection** in HP Systems Insight Manager.

   b. Click the **Edit** (✎) button corresponding to the discovery schedule you want to modify.

   c. Click the **Discovery Groups** tab.

   d. Select the Brocade proxy under the list of discovery groups.

   e. Click **Add Selected Groups To Schedule**.

   f. Click **Finish**.

Upgrade Your CLI Clients

CLI Clients earlier than Build 6.0 do not work with Build 6.0 of the management server. Refer to the CLI Guide for more information about upgrading your CLI clients.

Upgrading Your CIM Extensions

It is preferable to upgrade all CIM extensions to the same version as the management server, as some functionality may be unavailable when earlier CIM Extensions are used. See "About Upgrading Your CIM Extensions" on page 189 in the Deploying and Managing CIM Extensions chapter.

4 Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries

Before you can use the management server, you must execute the Discovery process to make the software aware of the elements on your network, such as switches, storage systems, NAS devices, and tape libraries. Discovery obtains a list of elements and information about their management interface and dependencies.

NOTE: The management server can discover only elements with a suitable management interface. See the support matrix for your edition for information about supported hardware.

IMPORTANT: Before you can execute the Discovery process, you must have imported the HP Storage Essentials license. For instructions, see "Managing Licenses" on page 171.

HP Storage Essentials Standard Edition supports a subset of the elements supported by Enterprise Edition. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported elements. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in HP Storage Essentials).

NOTE: In HP Storage Essentials, a device is called an element; In HP Systems Insight Manager, a device is called a system.

NOTE: For more information about the procedures performed in the HP SIM user interface, see the HP SIM documentation at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html.

This chapter contains the following information:

About Discovery

When HP Storage Essentials is integrated with HP SIM, Discovery and Discovery Data Collection are performed using HP SIM's discovery user interface pages. This allows you to use credentials and perform discovery and data collection tasks in HP SIM and enables hardware and software health status polling, monitoring, and event management for storage, servers, switches, infrastructure, and other elements on your network, such as enclosures, racks, clients and printers.

IMPORTANT: When HP Storage Essentials is integrated with HP SIM, if you initiate discovery from the HP Storage Essentials Discovery Setup page, you will significantly limit the functionality of the integrated solution. The HP Storage Essentials discovery pages are designed primarily for HP Storage Essentials when it is used as a standalone product. In an integrated environment, the HP Storage Essentials Discovery Setup pages can be used for troubleshooting discovery issues specific to HP Storage Essentials or to enable product health monitoring. For more information, see "Troubleshooting" on page 379.

Before you begin the Discovery process, note the following:

- If you have a problem discovering an element, try enabling Troubleshooting Mode. For more information, see "Troubleshooting Mode" on page 396.
- If HP Storage Essentials detects a device manager URL for an element, the URL is added to the HP SIM Tools & Links page in the System Web Application Pages section.
- For elements that support multiple discovery protocols (for example, SNMP and SMI-S), only one protocol at a time is supported for a given element. If you want to change the protocol used to discover an element that has already been discovered, delete the element before attempting to rediscover it with a different protocol. For more information, see "Deleting Discovered Elements" on page 164.

Scheduling Discovery Tasks

When scheduling discovery tasks, observe the following:

- When HP Storage Essentials is integrated with HP SIM, we recommend that you do not schedule your HP SIM automatic discovery tasks to repeat over time because when the HP SIM discovery is finished, the automatic discovery tasks initiate the HP Storage Essentials discovery process. Allowing automatic discovery tasks to repeat will cause HP Storage Essentials to unnecessarily repeat its identification discovery step against devices that are already discovered.
- Discovery Data Collection does not default to an automatic schedule. In most cases, we recommend running Discovery Data Collection once a day during off-peak hours. For more information, see "Discovery Data Collection" on page 153.
- For a device to be discovered, you must be able to ping it successfully from HP SIM.

Discovery of SMI-S Devices

When HP Storage Essentials is integrated with HP SIM, HP SIM's native discovery of SMI-S devices is disabled, and SMI-S discovery is handled by HP Storage Essentials.

Note the following:

- Storage systems managed by HP Storage Essentials show a subtype of Storage Essentials Managed, and do not show the SMI subtype on the HP SIM System tab.
- Storage systems managed by HP Storage Essentials are listed in the HP SIM Storage Essentials Systems collection.
- HP SIM data collection from SMI-S devices is disabled to avoid duplicate data collection.
- The storage tables in HP SIM's Data Collection reports are not populated with data because HP SIM's SMI-S data collection is disabled.

> **CAUTION:** If you already have HP SIM set up when you add HP Storage Essentials, any data that HP SIM has collected about SMI-S devices will be removed from the database when you install the HP SIM Connector.

- Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of HP Storage Essentials cannot be added to discovery groups. These elements are listed separately and can be placed independently into scheduled Discovery Data Collection tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. (For more information, see "Using Discovery Groups" on page 162).

Discovery of Elements in a Storage Area Network (SAN)

To obtain information about the SAN, discover the following elements in the following order:

1. HP Storage Essentials management server. For more information, see "Discovering the HP Storage Essentials Management Server" on page 112.
2. Fibre Channel switch or fabric proxy. The Fibre Channel switch contains a list of all elements in the fabric. The management server obtains a detailed listing of all elements connected to the switch fabric.
   - Brocade is an example of a proxy-based switch. For more information, see "Discovering Brocade Switches" on page 116.
   - Cisco's SMI-S is an example of an embedded solution. For more information, see "Discovering Cisco Switches" on page 121.
3. A storage device or storage proxy. Include a proxy that has a direct connection or a SAN connection to a native device manager. For example:
   - Command View EVA and Hitachi HiCommand Device manager are examples of a proxy-based solution. For more information, see "Discovering HP StorageWorks EVA Arrays" on page 143 and "Discovering HDS Storage Systems" on page 139.
   - The SVP is an embedded solution for the XP array. For more information, see "Discovering HP StorageWorks XP Arrays" on page 145.
   - LSI storage systems are an example of systems that do not require a proxy because they can be accessed directly by communicating with the array controller. For more information, see "Discovering LSI Storage Systems" on page 139.

4. A host containing a Host Bus Adapter (HBA). All Fibre Channel host bus adapters look for available elements attached to the HBA. This information is gathered by CIM extensions and sent to the management server.

> **NOTE:** Since CIM extensions have not been installed yet, the management server will not be able to obtain this data when you perform discovery for elements. For more information, see "Deploying and Managing CIM Extensions" on page 181 and "Discovering Applications, Backup Hosts and Hosts" on page 297.

Using Credentials

Element credentials are entered as global (**Options > Protocol Settings > Global Settings**) or system protocol settings (**Options > Protocol Settings > System Protocol Settings**).

This section contains the following information:

- Using WBEM Settings, page 108
- Choosing Between System and Global Credentials, page 108

Using WBEM Settings

- For elements you want to discover and manage in HP Storage Essentials, you must enter each element's credentials as Web-Based Enterprise Management (WBEM) settings in the HP SIM user interface regardless of the protocol used to discover the element.
- When you use HP SIM and SNMP to discover devices that will be managed by HP Storage Essentials, provide the SNMP credentials in the WBEM settings section on the System Protocol Settings page (**Options** > **Protocol Settings** > **System Protocol Settings**). Only the WBEM credentials are passed from HP SIM to HP Storage Essentials. Any credential information entered in the SNMP settings section on the System Protocol Settings page is not passed from HP SIM to HP Storage Essentials.

Choosing Between System and Global Credentials

- If you are using non-standard ports for an element or the element is behind a firewall, you must use system protocol settings to discover that element and provide the port that is used. If an element is using the default port, you do not need to enter the port number.
- Make sure the credentials you enter are correct. When system credentials are not supplied, the system tries global credentials (if available) for the element.
- Any passwords specified on the HP SIM Global Protocol Settings page are used during system identification. Sensitive passwords, such as root or domain administrator passwords, should not be specified here if there is a risk of sending these to untrustworthy systems.
- Using global credentials may increase the amount of time discovery takes. If you define three global credentials, HP SIM and HP Storage Essentials will each attempt to access the element three times, once for each credential. If there are 100 elements to discover and 3 global credentials, there will be a total of 600 interrogations made. With system credentials, only the defined credentials for an element are used.
- Be careful when using global protocol settings because they can cause problems when discovering certain elements. If you want to use global protocol settings, use them selectively.

For example, in the phased discovery described in "Discovering Elements" on page 113, you could discover your switches first. In this case, you would enter only the global credentials that apply to the switches. After successfully running the switch discovery task, you would replace the switch credentials with the global protocol settings for the next set of elements you want to discover.

- Some elements lock you out without warning after multiple failed login attempts. This can also occur with hosts, depending on your security settings. If you enter several sets of global credentials, HP SIM will try each set in the order it was entered. When the element is passed to HP Storage Essentials, HP Storage Essentials tries each credential again. If there are too many failed login attempts, you may be locked out of the element.

Discovery Steps

NOTE: Before starting the discovery process, review the information in Table 2 on page 2 carefully to make sure you are using the process correctly.

Overview

When HP Storage Essentials is integrated with HP SIM, discovery is performed from the HP SIM discovery user interface pages. Discovery includes the following tasks:

1. Testing your SMI-S Providers (Optional), page 109
2. Configuring the Selective Discovery Filter (Optional), page 109
3. Configuring the HP SIM Connector to Pass Devices with the DNS Name (Optional), page 110
4. Signing in to HP SIM, page 110
5. Enabling Product Health Monitoring, page 111.
6. Discovering the HP Storage Essentials Management Server, page 112.
7. Discovering Elements, page 113.

Testing your SMI-S Providers (Optional)

If you want to verify that an SMI-S provider is configured correctly, run the `wbemdisco` tool. See the *Troubleshooting for SMI-S providers* document at http://www.hp.com/go/hpsim/providers for instructions.

Configuring the Selective Discovery Filter (Optional)

During discovery, HP SIM sends HP Storage Essentials the IP address and credential information for the elements it has processed. The HP SIM Connector restricts the elements passed to HP Storage Essentials to the types of elements that HP Storage Essentials supports. If you want to selectively filter the elements that are passed from HP SIM to HP Storage Essentials in discovery operations, use the selective discovery filter to define the set of devices that can pass from HP SIM to HP Storage Essentials.

For example, if HP SIM is monitoring a large number of servers, and a subset of those servers has SAN-attached storage that you want to monitor with HP Storage Essentials, you can use the selective discovery filter to configure the environment so only that subset of servers is processed by both HP Storage Essentials and HP SIM.

For more information, see ”Selective Discovery Filter” on page 155.

Configuring the HP SIM Connector to Pass Devices with the DNS Name (Optional)

By default, HP SIM passes IP addresses to HP Storage Essentials. You can configure the HP SIM Connector to pass elements to HP Storage Essentials so that the DNS name is displayed in HP Storage Essentials discovery lists.

To configure the HP SIM Connector to pass the DNS name:

1. Open the file `C:\Program Files\HP\Systems Insight Manager\config\globalsettings.props`.
2. Edit the following property as follows: `StorageEssentialsSendIPAddress=false`.
3. Save and close the file.
4. Restart HP SIM.

NOTE: The `StorageEssentialsSendIPAddress` property is reset to `true` if you reinstall the HP SIM Connector.

Signing in to HP SIM

IMPORTANT: If your Web browser has an option for blocking pop-ups, disable it. The management server uses pop-ups for dialog boxes.

To sign in to HP SIM, open a web browser and enter `https://<fully qualified domain name of localhost>:50000` in the Address box. For example: `https://example.domain.com:50000`.

IMPORTANT: If you are using the integrated solution, do not start HP SIM from the program files menu or the Desktop icon. To access all of the HP Storage Essentials features, you must sign in to HP SIM using the URL that includes the fully qualified domain name.

The HP SIM First Time Wizard opens the first time an administrative rights user runs the HP SIM application. If you choose to run the wizard, follow the on-screen instructions with the following exceptions:

- You must import your Storage Essentials license before setting up and running discovery with the First TIme User wizard. The discovery will fail if you have not imported the Storage Essentials license. If you see the HP Systems Insight Manager First Time wizard, do not click the **Do not automatically display this dialog again** check box. After you import the Storage Essentials license, restart the HP SIM First Time wizard (**Options** > **First Time Wizard** from HP

SIM) and set up your HP SIM discovery. See Step 8 – Obtain and Apply a Storage Essentials License Key Before Setting Up Discovery on HP SIM, page 26.

- Enter the requested information including SNMP Read community strings.
- Do not enter global WBEM user names and passwords on the WBEM page.
- Do not run the initial discovery process at the end of the wizard.

See the *HP Systems Insight Manager User Guide* for more information about the First Time Wizard.

Enabling Product Health Monitoring

Enabling this functionality allows you to monitor the database health and available disk space for the HP Storage Essentials management server.

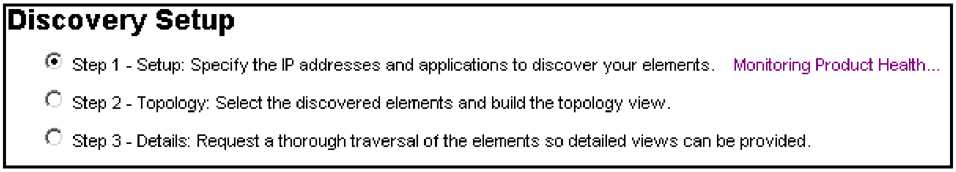
To enable product health monitoring:

1. Select **Tools** > **Storage Essentials** > **Home** on the HP SIM home page menu.

   The HP Storage Essentials home page opens in a separate web browser window.

2. From the HP Storage Essentials home page, click **Discovery**, and then click **Setup** in the upper-right pane of the HP Storage Essentials window.

   The Discovery Setup page appears.



Discovery Setup

● Step 1 - Setup: Specify the IP addresses and applications to discover your elements. Monitoring Product Health...

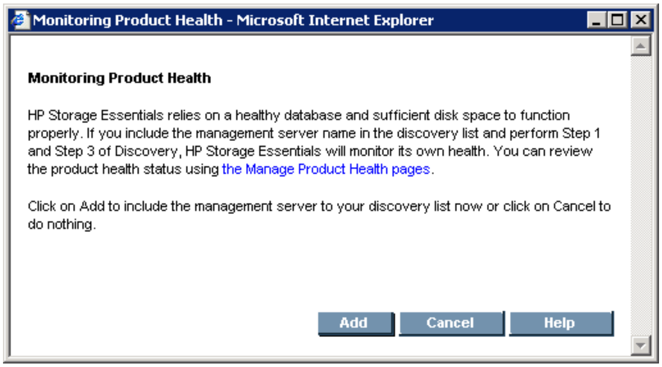
○ Step 2 - Topology: Select the discovered elements and build the topology view.

○ Step 3 - Details: Request a thorough traversal of the elements so detailed views can be provided.

Figure 4 Discovery Setup page

3. Click the **Monitoring Product Health** link.

   The Monitoring Product Health window appears.



Monitoring Product Health - Microsoft Internet Explorer

Monitoring Product Health

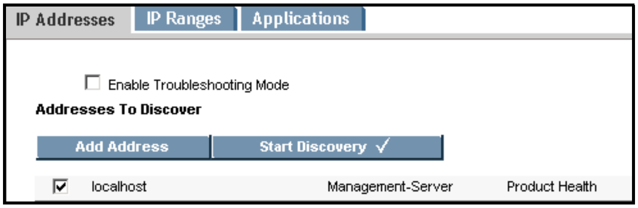
HP Storage Essentials relies on a healthy database and sufficient disk space to function properly. If you include the management server name in the discovery list and perform Step 1 and Step 3 of Discovery, HP Storage Essentials will monitor its own health. You can review the product health status using the Manage Product Health pages.

Click on Add to include the management server to your discovery list now or click on Cancel to do nothing.

Figure 5 Monitoring Product Health window

4. Click **Add**.

The Discovery Setup, Step 1 - Setup page shows the HP Storage Essentials management server as `localhost`.



□ Enable Troubleshooting Mode

Addresses To Discover

☑ localhost Management-Server Product Health

Figure 6 HP Storage Essentials Management Server “localhost”

Discovering the HP Storage Essentials Management Server

You do not need to install a CIM extension on the management server because it is monitored through a built in CIM extension that is installed automatically during the HP Storage Essentials installation. Built-in credentials are used to access the localhost.

To discover the HP Storage Essentials management server:

1. Select **Options** > **Discovery**.

   The Automatic discovery page appears.
2. Click **New**.
3. Enter a name for the discovery task in the Name box.
4. Clear the **Automatically execute discovery every** check box.
5. Enter the IP address of the management server in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** box.

   NOTE: See *Creating a new discovery task* in the HP SIM online help for more information.
6. Click **OK** to save the task.

   NOTE: If HP SIM and HP Storage Essentials are installed on a single machine, skip to step 8; the management server will already be listed in HP SIM’s All Systems collection.
7. Select the task you created and click **Run Now**.

   HP SIM pings the HP Storage Essentials management server. If the ping is successful, the management server is added to HP SIM’s All Systems collection.
8. Update the system protocol settings for the HP Storage Essentials management server:

   a. Click **All Systems** in the System and Event Collections pane.

   b. Click the name or IP address of the HP Storage Essentials management server in the System Name column of the system table view page.

   c. From the System page, click the **Tools & Links** tab.

   d. Click the **System Protocol Settings** link.

e. In the WBEM settings section, select **Update values for this protocol** and **Use values specified below**.

f. Enter the user name and password for the HP Storage Essentials management server (the administrator account) in the format `domain\administrator` or `servername\administrator`.

9. Select **Options > Discovery**.
10. Select the discovery task you created in step 2, and then click **Run Now**.
11. When the discovery task is complete, click the **Run SE Discovery Data Collection Now** link in the For Storage Essentials (SE) discoveries section above the list of tasks.
12. Click **Get Details** to run discovery data collection and complete the discovery process for the HP Storage Essentials management server.

Discovering Elements

HP recommends a phased discovery process in which you create separate tasks for groups of elements. Discover your elements in the following order:

1. Switches and switch proxies (for more information, see "Discovering Switches" on page 115).
2. Storage systems (for more information, see "Discovering Storage Systems" on page 133).
3. NAS devices and tape libraries (for more information, see "Discovering NAS Devices and Tape Libraries" on page 149).
4. Applications, backup servers and hosts are discovered later after you install the CIM extensions (for more information, see "Deploying and Managing CIM Extensions" on page 181 and "Discovering Applications, Backup Hosts and Hosts" on page 297).

Use the following procedure for each discovery task:

1. Decide if you will use global or system credentials for the discovery task. For tips on how to choose the credential type that best suits your environment see "Choosing Between System and Global Credentials" on page 108.
2. If you decide to use global credentials, enter them now:

NOTE: System credentials are entered later in this procedure.

a. Select **Options** > **Protocol Settings** > **Global Protocol Settings**.

b. Enter the settings required to discover the element. For details on the information to enter, see the section in this chapter for the specific element. For example, see "Discovering Brocade Switches" on page 116 for the required Brocade switch information.

c. Click **OK** to save the settings.

IMPORTANT: For best results, enter only global credentials that apply to the set of elements for the current discovery task. When this discovery task is complete, you can delete the element-specific global credentials and enter global credentials for the next set of elements you want to discover.

3. Select **Options** > **Discovery**.
4. Click **New** on the HP SIM Discovery page Automatic tab.
5. Enter a name for the discovery task in the Name box.
6. Clear the **Automatically execute discovery every** check box.
7. Enter the IP addresses of the elements you want to discover in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** box.

NOTE: To use a hosts file to specify systems for an automatic discovery, add the hosts file name to the **Ping inclusion ranges, templates and/or hosts files** box in the Configure general settings section of the Automatic Discovery tab. Use the following statement: `$Hosts_filename` where `Hosts_filename` is the name of the hosts file that you want to use.

NOTE: For more information, see the topic *Creating a new discovery task* in the HP SIM online help.

8. Select the discovery task, and then click **Run Now**.

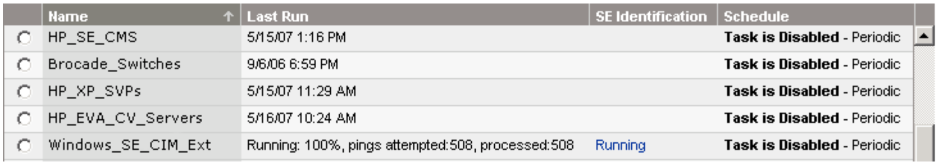
   HP SIM pings each element. If the ping is successful, the element is added to HP SIM's All Systems collection.
9. If you did not enter global credentials (at step 2), enter system credentials for your elements:
   a. Click **All Systems** in the System and Event Collections pane.
   b. Click the element name or the IP address in the System Name column of the system table view page.
   c. Click the **Tools & Links** tab.
   d. Click the **System Protocol Settings** link.
   e. Enter the settings required to discover the element. For details on the information to enter, see the section in this chapter for the specific element. For example, see "Discovering Brocade Switches" on page 116 for the required Brocade switch information.
   f. Click **OK** to save the settings.

NOTE: To update the system protocol settings for multiple systems select **Options > Protocol Settings > System Protocol Settings**.

10. Select **Options > Discovery**.

11. Select the discovery task created in step 4, and then click **Run Now**.

    When complete, the task monitor shows 100%. Within two minutes, the status in the SE Identification column changes from Pending to Running. You can click the **Running** link to view the HP Storage Essentials Discovery progress table.

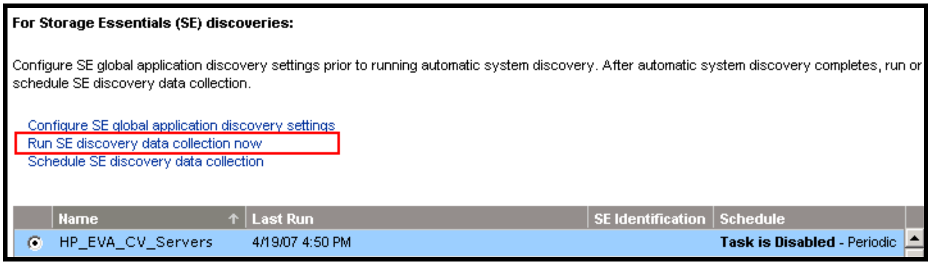


	Name	Last Run	SE Identification	Schedule
○	HP_SE_CMS	5/15/07 1:16 PM		**Task is Disabled** - Periodic
○	Brocade_Switches	9/6/06 6:59 PM		**Task is Disabled** - Periodic
○	HP_XP_SVPs	5/15/07 11:29 AM		**Task is Disabled** - Periodic
○	HP_EVA_CV_Servers	5/16/07 10:24 AM		**Task is Disabled** - Periodic
○	Windows_SE_CIM_Ext	Running: 100%, pings attempted:508, processed:508	Running	**Task is Disabled** - Periodic

Figure 7 HP Storage Essentials Discovery progress table

NOTE: SE discovery processing might finish before the SE Identification column shows status as Running. To monitor the progress of the discovery, select **Tasks & Logs > View Storage Essentials Logs**.

12. To obtain details about your discovered elements, click the **Run SE Discovery Data Collection Now** link in the For Storage Essentials (SE) discoveries section above the list of tasks.



For Storage Essentials (SE) discoveries:

Configure SE global application discovery settings prior to running automatic system discovery. After automatic system discovery completes, run or schedule SE discovery data collection.

Configure SE global application discovery settings
Run SE discovery data collection now
Schedule SE discovery data collection

	Name	Last Run	SE Identification	Schedule
●	HP_EVA_CV_Servers	4/19/07 4:50 PM		**Task is Disabled** - Periodic

Figure 8 Run SE Discovery Data Collection Now link

NOTE: You can also select **Options > Storage Essentials > Discovery > Run Discovery Data Collection** to access this functionality.

IMPORTANT: You must run discovery data collection to obtain information about your elements. Run discovery data collection when the network is not busy because this step takes some time to finish. For more information, see "Discovery Data Collection" on page 153.

13. Click **Get Details**.
14. To verify that discovery was successful, select **Tools > Storage Essentials > System Manager**.

    The Topology page appears and shows your discovered elements.

Discovering Switches

Use the workflow in "Discovering Elements" on page 113 to discover switches. This section provides information about supported switches, including the information to enter in HP SIM during the Discovery process. For more information on switch support, see the support matrix in the Documentation Center (**Help** > **Documentation Center** in HP Storage Essentials).

IMPORTANT: All SMI-S switches require a user name and password.

Table 4 Overview of Switch Discovery Requirements

Element	Discovery Requirements	For More Information
Brocade switches (SMI-S)	IP address and the user name and password from the Brocade SMI Agent security setup.	See Discovering Brocade Switches, page 116.
CNT switches	IP address and the port number for the InVsn Software that manages the switch and the user name and password.	See Discovering CNT Switches, page 120.
Cisco switches (SMI-S)	IP address of the Cisco switch and the user name and password of the switch.	See Discovering Cisco Switches, page 121.
Cisco switches (SNMP)	IP address of the Cisco switch. Enter the SNMP read-only community string as the user name and enter the password.	See Discovering Cisco Switches, page 121.
QLogic, and HP M-Series switches (SMI-S)	IP address of the SMI-S switch and the user name and password of the switch.	See Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems, page 123.
Sun StorEdge, QLogic, and HP M-Series switches (SNMP)	IP address of the Sun StorEdge, QLogic, or HP M-Series switch. Enter the SNMP read-only community string as the user name and enter the password.	See Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems, page 123.
McDATA and EMC Connectrix switches	Additional steps required for discovering these switches vary according to the network configuration.	See Discovering McDATA and EMC Connectrix Switches, page 124.

Discovering Brocade Switches

The management server uses the Brocade SMI-S Provider (also known as the Brocade SMI Agent) to discover Brocade switches. Before you can discover Brocade switches with SMI-S, however, you must download and install the Brocade SMI Agent software. See the *HP StorageWorks B-Series* document for instructions at: http://www.hp.com/go/hpsim/providers. Check this web site periodically to verify that you are running a current version of the Brocade SMI Agent. For more information on Brocade SMI Agent versions, see the support matrix.

IMPORTANT: With this release, discovery of Brocade switches through the Fabric Access API is not supported. For information on migrating existing Brocade API switches to SMI-S, see "Migrating Brocade API Switches to SMI-S After Upgrading" on page 117.

Migrating Brocade API Switches to SMI-S After Upgrading

After successfully upgrading the management server, any Brocade switches that use the Brocade Fabric Access API provider must be migrated to the Brocade SMI-A provider. The management server will prompt you to migrate your Brocade switches the first time you log on to the management server after the upgrade and will display the Brocade API switches that need to be migrated.

Until you migrate your Brocade switches to SMI-A, data such as topology and zoning from the Brocade switch will be stale and you will be unable to use the Brocade switch to perform provisioning or gather port performance statistics through the Brocade switch. The Brocade Fabric Access API switches are quarantined and you will have the option to migrate to the Brocade SMI-A provider at your discretion in case your SAN policy requires that you validate the new Brocade SMI Agent provider before migrating your Brocade switches.

The quarantined API-managed Brocade switches retain their historical data and that data remains intact during the migration to the SMI-A provider.

After migrating the Brocade switches to SMI-A, the Brocade SMI-A proxy server is placed in its own discovery group. This new discovery group is not part of any Discovery Data Collection schedule. If the Brocade switches were part of a Discovery Data Collection schedule prior to migration, you must manually adjust those schedules to run Discovery Data Collection for the migrated Brocade switches. If the schedules are not adjusted manually, Discovery Data Collection will not run for the migrated switches as per pre-migration schedules.

However, new data will not be collected for the quarantined Brocade switches until you migrate the switches to the SMI-A provider. Follow these steps to migrate your Brocade switches to the Brocade SMI-A provider:

1. Download the Brocade SMI Agent v120.6.0a provider software and its Installation Guide from the Brocade website:

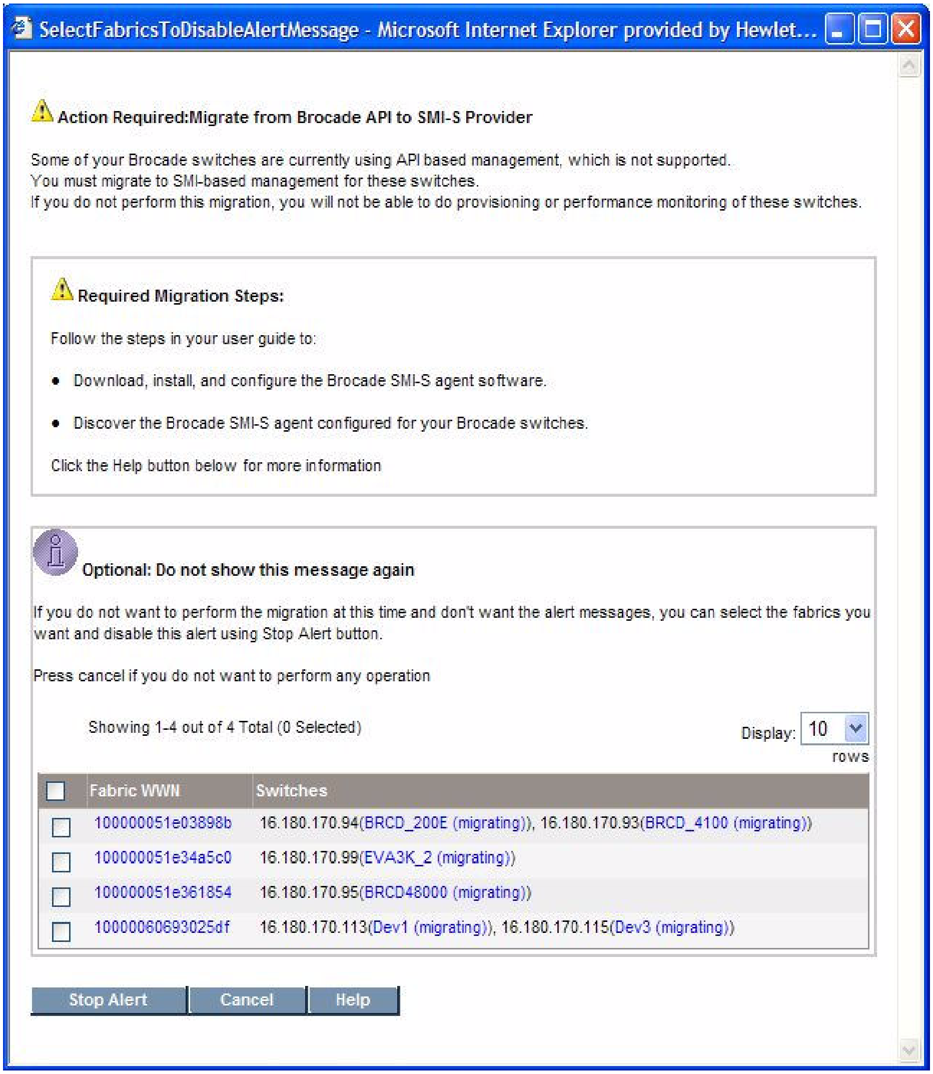
   http://www.brocade.com/support/SMIAGENT.jsp

   See the support matrix for your edition for details on the latest supported version for the management server.
2. Install the Brocade SMI Agent with a minimum version of 120.6.0a and configure the proxy servers on the server with which you will manage your Brocade access points following the installation and configuration instructions included in the Brocade v120.6.0a Installation Guide. Refer to the Brocade document for SMI-A requirements.

Comply with the installation notes included in the following document:
ftp://ftp.compaq.com/pub/products/storageworks/smisproviders/brocade_provider.pdf

This document is written for an earlier version of the Brocade SMI Agent, but the installation notes and other information also apply to v120.6.0a of the Brocade SMI Agent software.

3. Log on to HP Systems Insight Manager and access the Storage Essentials management server (from HP SIM, select **Tools** > **Storage Essentials**).The HP Storage Essentials alerts you to migrate your Brocade Fabric Access API switches when you first log on.


SelectFabricsToDisableAlertMessage - Microsoft Internet Explorer provided by Hewlet...

⚠ Action Required:Migrate from Brocade API to SMI-S Provider

Some of your Brocade switches are currently using API based management, which is not supported.
You must migrate to SMI-based management for these switches.
If you do not perform this migration, you will not be able to do provisioning or performance monitoring of these switches.

⚠ Required Migration Steps:

Follow the steps in your user guide to:

- Download, install, and configure the Brocade SMI-S agent software.
- Discover the Brocade SMI-S agent configured for your Brocade switches.

Click the Help button below for more information

Optional: Do not show this message again

If you do not want to perform the migration at this time and don't want the alert messages, you can select the fabrics you want and disable this alert using Stop Alert button.

Press cancel if you do not want to perform any operation

Showing 1-4 out of 4 Total (0 Selected)

Display: 10 rows

□	Fabric WWN	Switches
□	100000051e03898b	16.180.170.94(BRCD_200E (migrating)), 16.180.170.93(BRCD_4100 (migrating))
□	100000051e34a5c0	16.180.170.99(EVA3K_2 (migrating))
□	100000051e361854	16.180.170.95(BRCD48000 (migrating))
□	10000060693025df	16.180.170.113(Dev1 (migrating)), 16.180.170.115(Dev3 (migrating))

Your Brocade switches are quarantined until you migrate to the SMI-A provider. The migration message is displayed each time you log on to the management server until each Brocade switch is migrated to the new Brocade SMI-A provider or you choose to disable the message.

4. Run HP SIM discovery for the Brocade proxy server. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”
5. Run Discovery Data Collection. See the chapter, “Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries.”

   The Brocade switches are migrated to the SMI-A provider.

   > **IMPORTANT:** Before performing any provisioning operations that involve a Brocade switch you must perform Discovery Data Collection for any subset of elements that includes the Brocade switch.

6. If you were using discovery schedules to collect details for Brocade switches prior to migrating them to SMI-A, add the new discovery group for the Brocade proxy server to your pre-existing Discovery Data Collection schedules as described in the following steps:
   - **a.** Select **Options** > **Storage Essentials** > **Discovery** > **Schedule Discovery Data Collection** in HP Systems Insight Manager.
   - **b.** Click the **Edit** (✎) button corresponding to the discovery schedule you want to modify.
   - **c.** Click the **Discovery Groups** tab.
   - **d.** Select the Brocade proxy under the list of discovery groups.
   - **e.** Click **Add Selected Groups To Schedule**.
   - **f.** Click **Finish**.

When discovering Brocade switches, note the following:

- Before performing any provisioning operations that involve a Brocade switch you must run Discovery Data Collection for any subset of elements that includes this Brocade switch.
- Configure the proxy switch with the most recent version of the Brocade firmware. For the latest details on firmware requirements, see the support matrix for your edition.

Discovery Information for Brocade Switches

To discover Brocade switches, enter the following information in HP SIM:

- IP address of the Brocade SMI-S proxy server you want to discover.
- If you selected an HTTPS port other than the default (5989) in the Brocade SMI Agent HTTPS Port Configuration window, enter this in HP SIM by editing the system protocol settings for the switch.
- User name and password from the SMI Agent setup. The user name and password depend on the security settings you configured when you installed the Brocade SMI Agent:
  - For Brocade SMI Agent installed on Windows:
    - If you selected **Yes** in the Brocade SMI Agent Enabling Security window, and you enabled Windows domain authentication, the username and password are the Windows domain administrator account username and password.

    - If you selected **Yes** in the Brocade SMI Agent Enabling Security window, and you disabled Windows domain authentication, the username and password are the Windows local administrator account username and password.
    - If you selected **No** in the Brocade SMI Agent Enabling Security window, you can enter any username and password because security for the proxy server was not enabled.
- For Brocade SMI Agent installed on Linux or Solaris, see the Brocade SMI Agent documentation for more information about SMI Agent security for Linux or Solaris.

Discovering CNT Switches

The management server uses the CNT SMI-S provider to discover CNT switches. 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 support matrix for the required InVSN version for your switch model.

IMPORTANT: The InVsn credentials are used by the SMI-S provider. Make sure the SMI-S provider is enabled as described in the discovery process for CNT Switches.

When discovering CNT switches, note the following:

- 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 Gigabit Interface Converters (GBICs).

Discovery Process for CNT Switches

To discover CNT switches:

1. Discover the host running the InVSN software.
    a. Select **Options** > **Discovery** to open the HP SIM Automatic Discovery page.
    b. Click **New** on the HP SIM Discovery page Automatic tab.
    c. Enter a name for the discovery task in the Name box.
    d. Clear the **Automatically execute discovery every** check box.
    e. Enter the IP address of the host running the InVSN software in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** box.
    f. Select the discovery task and click **Run Now**.

        HP SIM pings the host. If the ping is successful, the element is added to HP SIM's All Systems collection.

    g. Select **Options** > **Protocol Settings** > **System Protocol Settings** and select the host you discovered as a target and provide the port number for the host in the WBEM section.
2. Take the following steps 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. Make the following entry in the file: `cimomenabled=TRUE`

c. Save the file, and then restart the InVsn software.

3. Enter the following information in HP SIM:
   - Primary IP address of the host running the InVsn software you want to discover.
   - Namespace. If the `//root/cntfabric` namespace for the InVSN software is not already included in the `wbemportlist.xml` file in `<HP SIM install directory>/config/identification`, add it in the format `<interopnamespace name="root/cntfabric"/>`.
   - Port number for the InVsn software. Enter the port number in the WBEM section of the System Protocol Settings page (**Options** > **Protocol Settings** > **System Protocol Settings**).
   - User Name for the login to the InVsn software.
   - Password for the login to the InVsn software.

Discovering Cisco Switches

The management server discovers Cisco switches through SNMP and SMI-S connections, depending on the switch model. See the support matrix for your edition for details on supported switch models and firmware revisions.

Note the following when discovering Cisco switches with SNMP:

- HP SIM does not allow blank passwords. Since Cisco SNMP switches do not use a password, enter anything for the password.
- 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.
- The management server groups active zone sets in all Virtual SANs (VSANs) in a fabric into a zone set called ACTIVE, which 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:CISCO1:ZONE1.
- No ports are reported for uninstalled blades or GBICs.
- To receive events from Cisco switches, verify that the SNMP trap community string is set to match the community string defined in the HP Storage Essentials custom properties (the default is `public`), and make sure the SNMP traps are configured to be sent to the management server. For more information, see ”Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 133

Note the following when discovering Cisco switches with SMI-S:

- Before you can discover Cisco switches with SMI-S, you must download and install the Cisco cimserver software. See the *HP StorageWorks C-Series* document for instructions. You can access this document at: http://www.hp.com/go/hpsim/providers.
- Enable the CIM Server for Cisco switches discovered through the SMI-S provider.
  - **a.** On the Cisco switch, enter the following command to display the Common Information Models (CIM) configurations and settings:
    ```
    cisco_switch# show cimserver
    ```
  - **b.** To enter configuration mode, enter the following:
    ```
    cisco_switch# config
    ```
  - **c.** To enable access to the server, enter the following:
    ```
    cisco_switch# cimserver enableHttps
    ```
    And/or
    ```
    cisco_switch# cimserver enableHttp
    ```
  - **d.** To enable the CIM Server, enter the following:
    ```
    cisco_switch(config)# cimserver enable
    ```
  - **e.** To exit configuration mode, enter the following:
    ```
    cisco_switch(config)# exit
    ```
- If you are using the SMI-S provider, discover all Cisco switches in a fabric If you discover only one switch, inactive zones and zone sets residing on other switches are not displayed on the management server.

Discovery Information for Cisco Switches

IMPORTANT: Provide the SNMP credentials in the WBEM settings section on the System Protocol Settings page (**Options** > **Protocol Settings** > **System Protocol Settings**). Only the WBEM default credentials are passed from HP SIM to HP Storage Essentials. Any default credential information you set up in regards to SNMP is not passed from HP SIM to HP Storage Essentials.

To discover Cisco switches, enter the following information in HP SIM:

- System name or primary IP address of the Cisco switch you want to discover.
- Do one of the following:
  - For Cisco switches with SNMP connections: Provide the user name for the switch. This is the public community SNMP string for the switch.
  - For Cisco switches with SMI-S connections: Provide the switch user name.
- HP SIM does not allow blank passwords. Do one of the following:
  - For Cisco SNMP switches, enter anything for the password.
  - For Cisco SMI-S switches, enter the switch password.

Discovering Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystems

The management server discovers Sun StorEdge switches through an SNMP connection and QLogic and HP M-Series switches are discovered through SNMP or SMI-S. See the support matrix for your edition for details on supported switch models and firmware versions.

Note the following when discovering these switches with SNMP:

- HP SIM does not allow blank passwords. Since these switches do not use a password, enter anything for the password.
- The management server does not support provisioning for Sun StorEdge, QLogic, and HP M-Series switches. Only the active zone set and its zone members are reported.
- To manage a fabric of Sun StorEdge, QLogic, or HP M-Series 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 switches is 162. To change this port, see ”Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 133.
- To receive events from Sun StorEdge, QLogic, and HP M-Series switches, verify that the SNMP trap community string is set to match the community string defined in the HP Storage Essentials custom properties (the default is `public`), and make sure the SNMP traps are configured to be sent to the management server. For more information, see ”Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP” on page 133

Note the following when discovering these switches with SMI-S:

- Before you can discover these switches with SMI-S, you must download and install the cimserver software. For more information, see the document *QLogic SANbox 52xx and 56xx Switches* or *HP StorageWorks M-Series for p-Class BladeSystems* at: http://www.hp.com/go/hpsim/providers.
- You must perform Discovery Data Collection to obtain all available information from QLogic SMI-S switches—otherwise, attributes such as vendor, fabric, and port information will be missing for the QLogic SMI-S switches.

NOTE: You may see an error replicating the switch fabric name for QLogic-based switches. This error can be ignored.

Discovery Information for Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystem Switches

To discover Sun StorEdge, QLogic and HP StorageWorks M-Series for p-Class BladeSystem Switches switches, enter the following information in HP SIM:

IMPORTANT: Provide the SNMP credentials in the WBEM settings section on the System Protocol Settings page (**Options** > **Protocol Settings** > **System Protocol Settings**). Only the WBEM default credentials are passed from HP SIM to HP Storage Essentials. Any default credential information you set up in regards to SNMP is not passed from HP SIM to HP Storage Essentials.

- System name or primary IP address of the switch you want to discover.
- Do one of the following:
  - For switches with SNMP connections, provide the user name for the switch. This is the public community SNMP string for the switch.
  - For switches with SMI-S connections, provide the switch user name.
- HP SIM does not allow blank passwords. Do one of the following:
  - For SNMP switches enter anything for the password.
  - For SMI-S switches enter the switch password.

Discovering McDATA and EMC Connectrix Switches

McDATA and EMC Connectrix switches use SMI-S, the Fibre Channel Switch Application Programming Interface (SWAPI), or SNMP to communicate with devices on the network. The management server can discover multiple instances of Enterprise Fabric Connectivity (EFC) Manager. Use one of the following methods to discover McDATA and Connectrix switches:

Table 5 Discovery Settings for McDATA and Connectrix Switches

Method	**Description**	**Provisioning limitations**
SMI-S Discovery	SMI-S is the default discovery method for new installations. For more information, see Discovering McDATA and Connectrix switches with SMI-S, page 126.	The SMI-S 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 and nicknames are not supported.
SWAPI setting through a Proxy	You will need to connect through the proxy instead of the switch. For more information, see "Discovering McDATA and Connectrix Switches through a Proxy with SWAPI" on page 127.	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.

Table 5 Discovery Settings for McDATA and Connectrix Switches

Method	Description	Provisioning limitations
SNMP setting Through a Proxy	Contact the switch through a proxy. You can use this option with EMC Connectrix™ Manager and EFC Manager to contact the switch. For more information, see "Discovering McDATA and Connectrix Switches through a Proxy with SNMP" on page 128.	This SNMP setting through a proxy does not let you manage or access information about zones, zone sets, or zone aliases.
Contacting the switch directly (SNMP)	Contact the switch by its IP address or DNS name. This connection uses SNMP. See the support matrix for your edition for details on switch models (**Help > Documentation Center** in HP Storage Essentials). For more information, see "Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP" on page 129.	This SNMP setting provides view-only access to the active zone set and its members. You cannot create, modify, and/or delete a zone set or its members.

Keep in mind the following:

- SMI-S is the default method for discovering McDATA and Connectrix switches. If you need to migrate to SMI-S or change the discovery settings, see "Changing the Discovery Settings" on page 130.
- You can only choose one discovery method for McDATA and Connectrix switches. For example, if you use SMI-S, you cannot discover additional McDATA and Connectrix switches with SWAPI or SNMP.
- If you use EFC Manager or Connectrix Manager, see the support matrix for your edition to verify the version requirements.
- Brocade 5000ni switches running in McDATA mode are managed by the Brocade SMI Agent and not by McDATA SMI-S. For more information, see "Discovering Brocade Switches" on page 116.
- Managing McDATA and Connectrix switches through SWAPI is not supported on management servers running on Linux.
- If you change the discovery settings, the user ID and password will no longer work. For this reason, HP recommends setting this property before discovering any McDATA or Connectrix switches. If you must change the configuration, see "Changing the Discovery Settings" on page 130.
- After you discover a McDATA or Connectrix switch through a proxy, the IP address displayed next to the name of the switch is 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 (**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.

- 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 "Managing McDATA and EMC Connectrix Switches" on page 132.
- All McDATA or Connectrix switches in a fabric must be managed by the same EFC Manager or Connectrix Manager. Do not have more than one EFC Manager or Connectrix Manager to a fabric for McDATA or Connectrix switches.
- If you want the management server to receive SNMP traps from McDATA or Connectrix switches, do one of the following:
  - If you discovered Connectrix Manager or EFC Manager, enable SNMP trap forwarding to the management server only on the Connectrix Manager or EFC Manager, not on the individual switches.
  - If you discovered Connectrix or McDATA switches directly, enable SNMP trap forwarding on the switches, not in any other management software.
- For more information about the SNMP port and community string, see "Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP" on page 133.

Discovering McDATA and Connectrix switches with SMI-S

Before you can discover McDATA and Connectrix switches with SMI-S, you must download and install the McDATA SMI-S provider software. See the document *HP StorageWorks M-Series* at: http://www.hp.com/go/hpsim/providers for instructions. Check this web site periodically to verify that you are running a current version of the SMI-S provider.

Note the following when discovering these switches with SMI-S:

- Before attempting to discover your switches, ensure that EFC Manager or Connectrix Manager is installed and configured or add your switches to the SMI-S provider.
- For upgrades only: To migrate your existing switches to SMI-S, follow the procedure in "Changing the Discovery Settings" on page 130.
- Discovering McDATA and Connectrix switches with SMI-S is the default setting. To view or change the discovery settings, see "Changing the Discovery Settings" on page 130.
- You can install only one instance of the SMI-S provider on the HP Storage Essentials management station.
- Installation of the McDATA SMI-S provider is not supported on Linux systems.
- A McDATA or Connectrix switch cannot be managed by more than one SMI-S provider.
- When you install the SMI-S provider, there are two modes:
  - In coexist mode the SMI-S provider communicates with EFC Manager or Connectrix Manager and adds all the switches in the managed list of EFC Manager or Connectrix Manager.
  - In direct mode, you must add each switch to the SMI-S provider with its IP address, credentials and switch type. You can use a McDATA's `manageswitch.bat` file to manage the addition and deletion of switches.

- If you selected direct mode during the SMI-S provider installation, when you add switches, you must enter the switch type based on the McDATA model number even if your switch is an OEM model. For more information about the switch type, see your McDATA documentation.
- The SMI-S provider can be installed on the same server as EFC Manager or Connectrix Manager.
- If you selected coexist mode during the SMI-S provider installation you can have only one EFC Manager or Connectrix Manager server.
- If you are using EFC Manager or Connectrix Manager you cannot add managed switches in direct mode. To add switches in direct mode you must remove them from EFC Manager or Connectrix Manager first.
- If the SMI-S provider is installed on a machine other than the HP Storage Essentials management server, network links between them must pass http traffic on port 5988 (default) or https on port 5989. The port used by the SMI-S provider can be configured. See your switch documentation for more information.

SMI-S Discovery Information for McDATA and Connectrix Switches

To discover McDATA and Connectrix switches, enter the following information in HP SIM:

- IP address of the system running the McDATA SMI-S provider.
- User name for the McDATA provider.
- Password for the McDATA provider.

NOTE: The user name and password are defined during the SMI-S provider installation. These credentials might be different from the EFC Manager or Connectrix Manager credentials.

Discovering McDATA and Connectrix Switches through a Proxy with SWAPI

With the SWAPI setting, the management server contacts a proxy to obtain information about the switches connected to it. Use EFC Manager or Connectrix Manager for this option. If you do not have EFC Manager or Connectrix Manager, see "Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP" on page 129.

EFC Manager versions 7.0, 1.3 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: EMC customers using the EMC Connectrix Manager (EMC's rebranded EFC Manager) cannot use the EMC Fibre Zone Bridge (EMC's rebranded Bridge Agent) to discover EMC switches using SWAPI. The McDATA SWAPI library is incompatible with EMC's Fibre Zone Bridge Agent.

If the Fibre Zone Bridge Agent is not installed or not needed, you can uninstall it and install McDATA's Bridge Agent. The McDATA Bridge Agent will work with EMC's Connectrix Manager, but it cannot co-exist with EMC's Fibre Zone Bridge Agent.

If you are running Connectrix Manager and you need to have the EMC Fibre Zone Bridge Agent running, you cannot discover EMC Connectrix switches using SWAPI. You must discover them through the SNMP provider, either directly or through a proxy. For more information, see "Discovering McDATA and Connectrix Switches through a Proxy with SNMP" on page 128 and "Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP" on page 129.

Neither McDATA nor EMC officially support running the EMC Connectrix Manager with the McDATA Bridge Agent. Although this configuration has been tested for discovering EMC Connectrix switches using SWAPI, you should check with your EMC or McDATA representative to determine the implications of this configuration.

1. For McDATA switches only, install the McDATA Bridge Agent. To communicate with EFC Manager, the management server requires the Bridge Agent. Consult your McDATA representative for more information about the Bridge Agent.
2. Change the discovery setting for McDATA and Connectrix switches to SWAPI following the steps in "Changing the Discovery Settings" on page 130.
3. To discover the proxy, enter the following information in HP SIM:
   - IP address or system name of the EFC Manager or Connectrix Manager you want to discover.
   - User name—Enter the user name for EFC Manager or Connectrix Manager.
   - Password—Enter the corresponding password for EFC Manager or Connectrix Manager.

Discovering McDATA and Connectrix Switches through a Proxy with SNMP

NOTE: Discovering McDATA or Connectrix switches through a proxy using the SNMP protocol does not let you manage or access information about zones, zone sets or zone aliases.

You can use this option with EMC Connectrix Manager and EFC Manager to contact the switch.

IMPORTANT: Provide the SNMP credentials in the WBEM settings section on the System Protocol Settings page (**Options** > **Protocol Settings** > **System Protocol Settings**). Only the WBEM default credentials are passed from HP SIM to HP Storage Essentials. Any default credential information you set up in regards to SNMP is not passed from HP SIM to HP Storage Essentials.

1. Change the discovery setting for McDATA and Connectrix switches to SNMP following the steps in "Changing the Discovery Settings" on page 130.
2. 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.
3. To discover the proxy, enter the following information in HP SIM:
   - IP address or system name of the EFC Manager or 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.
   - Enter anything as a password; HP SIM does not allow an empty password field.
4. Make sure there are no port conflicts for receiving SNMP traps. When the management server is configured to contact the proxy by SNMP, it 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. For information about changing the port, see "Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP" on page 133.
5. Set 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 from all switches managed by the proxy to the management server using the port you selected. For more information, see the documentation for your proxy.

NOTE: The management server uses the Windows SNMP trap service when you run HP SIM and HP Storage Essentials on a Windows server or when the property `cimom.winsnmpTrapService=true` is set. The Windows SNMP trap service is not used on Solaris servers.

Discovering McDATA and Connectrix Switches through a Direct Connection and SNMP

The management server uses SMI-S or SWAPI to discover a McDATA or Connectrix switch through a proxy. If you want to discover McDATA or Connectrix switches directly, you must change the discovery settings to SNMP before you begin the following steps. See "Changing the Discovery Settings" on page 130. See the support matrix for your edition for McDATA switch details (**Help > Documentation Center** in HP Storage Essentials).

To discover a McDATA or Connectrix switch directly:

1. Make sure there are no port conflicts for receiving SNMP traps. When the management server is configured to contact the proxy by SNMP, it 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. For information about changing the port, see "Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP" on page 133.
2. Set 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 then sends traps from all switches managed by that proxy. See the proxy documentation for more information.

   NOTE: The management server uses the Windows SNMP trap service when you run HP SIM and HP Storage Essentials on a Windows server or when the property `cimom.winsnmpTrapService=true` is set. The Windows SNMP trap service is not used on Solaris servers.

3. Enter the following information in HP SIM
   - The IP address or system 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).
   - Enter anything as a password; HP SIM does not allow an empty password field.

Changing the Discovery Settings

To change the discovery settings for McDATA and Connectrix switches:

1. If you have already discovered your switches, delete all McDATA and Connectrix switches as described in "Deleting Discovered Elements" on page 164.
2. Select **Options** > **Storage Essentials** > **Manage Product Health**, and click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.

To enable SNMP:

a. Uncomment the `cimom.useSnmpMcDataProvider` property by removing the pound sign (#) in front of it.

b. Change the `cimom.mcdata.dontUseSmis` property as follows:

```
cimom.mcdata.dontUseSmis=true
```

NOTE: The `cimom.mcdata.dontUseSmis` property exists only in upgrade installations. If the property does not exist on your system, enter it manually.

To enable SWAPI:

a. Comment out the `cimom.useSnmpMcDataProvider` property by placing a pound sign (#) in front of it.

b. Change the `cimom.mcdata.dontUseSmis` property as follows:

```
cimom.mcdata.dontUseSmis=true
```

NOTE: The `cimom.mcdata.dontUseSmis` property exists only in upgrade installations. If the property does not exist on your system, enter it manually.

To enable SMI-S:

a. Comment out the `cimom.useSnmpMcDataProvider` property by placing a pound sign (#) in front of it.

b. Change the `cimom.mcdata.dontUseSmis` property as follows: `cimom.mcdata.dontUseSmis=false`.

1. Click **Save**.
2. Discover the switch. For instructions, see "Discovering Elements" on page 113.

NOTE: If you change the discovery settings, when you discover the switch with the new method, make sure you enter the correct credentials. For example, if you change from SNMP to SMI-S, the required credentials are different. See the section for the specific discovery method for information on the credentials to enter.

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, modify the `cimom.mcdata.exclude` property. Set the property `cimom.mcdata.exclude` to a comma-separated list of Worldwide Names (WWN) of the McDATA and Connectrix switches you want excluded, as shown in the following example:

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

The management server excludes the switches with the following WWNs: 1000080088A07024 and 1000080088A0D0B6

If the `cimom.mcdata.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 (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **Setup**), topology (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **Topology**), and Discovery Data Collection (**Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**), lists. The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **View Logs**) that a provider instance has been created for an excluded element. You can ignore this log message.

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

1. Select **Options** > **Storage Essentials** > **Manage Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the `cimom.mcdata.exclude` property.
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your changes to the text in the Custom Properties box. Remove the pound (#) symbol in front of the property to make sure it is not commented out.
7. Add the WWNs corresponding to the switches you want to exclude from discovery. Separate additional WWNs with a comma, as shown by the following example:

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

   where 1000080088A07024 and 1000080088A0D0B6 are the WWNs for McDATA and Connectrix switches.
8. When you are done, click **Save**.

Managing McDATA and EMC Connectrix Switches

Whenever you add, remove or replace McDATA or EMC Connectrix switches in an already-discovered service processor, you must make the management server aware of those changes by performing Discovery Data Collection to obtain information about the new switches from the service processor. For more information about adding switches, see ”Adding McDATA and EMC Connectrix Switches” on page 132.

When you remove switches from the service processor, you must remove them from the management server. For more information about removing switches, see ”Removing McDATA and EMC Connectrix Switches” on page 133.

When you replace McDATA or EMC Connectrix switches, you add and remove the switches as described previously. For more information, see ”Replacing McDATA and EMC Connectrix Switches” on page 133.

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 124.

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

To run Discovery Data Collection:

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

   During Discovery Data Collection, the software status light changes from green to red. You can view the progress of gathering details by accessing the logs. For more information, see ”Viewing Log Messages” on page 160.

Removing McDATA and EMC Connectrix Switches

After removing switches from a service processor, remove the switches from the management server database. For more information, see ”Deleting Discovered Elements” on page 164.

Replacing McDATA and EMC Connectrix Switches

After replacing switches in the service processor, you must make the management server aware of your changes by removing the old switches from the user interface and then running Discovery Data Collection so the management server can discover the new switches. For more information about Discovery Data Collection, see ”Discovery Data Collection” on page 153. If you are adding switches to a service processor that has not been discovered yet, see ”Discovering McDATA and EMC Connectrix Switches” on page 124.

Changing the SNMP Trap Listener Port and Community String for Switches Discovered with SNMP

The default SNMP trap listener port for all switches is `162`. To change this port for all switches that are discovered through SNMP, modify the `cimom.snmpTrapListenerPort` property.

The default SNMP trap community string is `public`. To change this port for all switches that are discovered through SNMP, modify the `cimom.snmpTrapListenerCommunityString` property.

1. Select **Options** > **Storage Essentials** > **Manage Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Do one of the following:
   - Copy the `cimom.snmpTrapListenerPort` property.
   - Copy the `cimom.snmpTrapListenerCommunityString` property.
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your SNMP trap listener port or SNMP trap community string change in the Custom Properties box. Remove the pound (#) symbol in front of the property to make sure it is not commented out. For example: `cimom.snmpTrapListenerPort=162`.

7. Click **Save**.

Discovering Storage Systems

Use the workflow in "Discovering Elements" on page 113 to discover storage systems. This section provides information about supported storage systems, including the information to enter in HP SIM during the discovery process. For more information on device support, see the support matrix. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in HP Storage Essentials).

Table 6 Discovery Requirements for Storage Systems

Element	Discovery Requirements	For Additional Information
3PAR storage systems	Discover the 3PAR storage system directly.	See Discovering 3PAR Storage Systems, page 135.
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, page 138.
EMC Symmetrix storage system (Including EMC Symmetrix DMX storage systems)	Discover the server running the EMC Solutions Enabler.	See Discovering EMC Solutions Enabler, page 135.
LSI storage systems	Can be discovered two ways: • Entering the IP address/DNS name, user name and password of a controller for an LSI 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 LSI storage system. Discovers all controllers known to the proxy.	See Discovering LSI Storage Systems, page 139.
HDS storage systems	Discover the server running HiCommand Device Manager.	See Discovering HDS Storage Systems, page 139.
HP Modular Smart Array (MSA) storage systems	Discover the server running the MSA SMI-S provider.	See Discovering HP StorageWorks MSA Arrays, page 142.

Table 6 Discovery Requirements for Storage Systems (continued)

Element	Discovery Requirements	For Additional Information
HP EVA storage systems	Discover the server running Command View EVA.	See Discovering HP StorageWorks EVA Arrays, page 143.
HP XP storage systems	Discover the server running the SMI-S provider or the built-in provider.	See Discovering HP StorageWorks XP Arrays, page 145.
IBM storage systems and System Storage SAN Volume Controller	Discover the IBM CIMOM or SVC.	See Discovering IBM Storage Systems or IBM SVCs, page 146.
Sun StorEdge 3510	Discovered through proxy software called Sun StorEdge™ Configuration Service.	See Discovering Sun StorEdge Storage Systems, page 148.
Sun StorEdge 6920 and 6940	Discover the storage system directly.	See Discovering Sun StorEdge 6920 and 6940 Storage Systems, page 149.
Sun StorEdge 6130	Discover the storage system directly.	See Discovering Sun StorEdge 6130 Storage Systems, page 149.
Xiotech storage systems	Discover the storage system directly.	See Discovering Xiotech Storage Systems, page 149.

Discovering 3PAR Storage Systems

To discover a 3PAR storage system, the SMI-S server for the 3PAR storage system must be running. By default, the 3PAR SMI-S server is not started on the array. To start the SMI-S server, start the InForm CLI and run the following command:

```
startcim
```

This command starts the SMI-S server within a minute or so.

NOTE: You do not need to provide the interop namespace because the management server includes the interop namespace for 3PAR storage systems in its default list.

To discover 3PAR storage systems, enter the following information in HP SIM

- The IP address or system name for the storage system.
- User name of the storage system.
- Password of the storage system.

Discovering EMC Solutions Enabler

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. See the EMC documentation for details.

To discover Symmetrix storage systems, you must create and configure a VCM volume on the storage system. The VCM database on the Solutions Enabler host must also be configured. For more information, see the *EMC Solutions Enabler Symmetrix CLI Command Reference*.

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. You 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)

Using Only One Subnet

To allow Solutions Enabler to respond correctly, limit the management server to a single subnet. If your management server is on two or more subnets, discovering a storage array through Solutions Enabler might not work. Limiting the management server to a single subnet allows Solutions Enabler to respond correctly.

Excluding EMC Symmetrix Storage Systems from Discovery

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

To exclude one or more Symmetrix storage systems from discovery, 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 the following serial numbers: 000183500570 and 000183610580.

If the `cimom.symmetrix.exclude` property is not specified, 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 (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **Setup**), topology (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **Topology**), and Discovery Data Collection (**Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**), lists. 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 LogsTasks & Logs** > **View Storage Essentials Log**) 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**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command.

   ```
   #cimom.symmetrix.exclude=000183500570,000183500575
   ```
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. 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**.

Excluding EMC Symmetrix Storage Systems from a Forced 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 the 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.

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

4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. 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.

   NOTE: To find the serial number, double-click the storage system in System Manager, and then click the **Properties** tab.

7. When you are done, click **Save**.
8. To force a refresh for elements that are not configured to skip the refresh, select the **Force Device Manager Refresh** option on the Discovery Data Collection page.
9. Click **Get Details** to run discovery data collection.

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. 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 a CLARiiON storage system, you must have already installed all required software components for that CLARiiON storage system, such as the Navisphere Host Agent. See 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 LSI Storage Systems

When discovering LSI storage systems, note the following:

- Discover all controllers on an LSI storage system by entering the IP address of each controller. The management server discovers these controllers as one single storage system.
- The management server must have the User Name box populated to discover the LSI storage system. Even if your LSI storage system does not have a user name set, you must enter something in the User Name box.
- To obtain drive-related statistics, install a proxy host. Ensure that the proxy host has at least one LUN rendered by each controller of the array.
- A license key is required for each storage system. The key is obtained from the web site specified on the Activation Card that shipped with your storage system.
- LSI storage systems do not require a password for discovery data collection. If you do not want to use the management server for provisioning on LSI storage systems, select the **Do Not Authenticate** option. The management server will still monitor the LSI storage system; however, you will not be able to do provisioning tasks.
- After discovering LSI controllers on an LSI array, the array is displayed as having three controllers on the HP SIM All Systems page. Two of these elements are displayed as unmanaged, but one is displayed as the accessible storage system for the array.
- If an LSI storage system that has two controllers with different IP addresses is discovered and identified with one password, and you change the password on the array and for both addresses in HP SIM, the password might not be updated correctly in HP Storage Essentials. In this case, subsequent data collections will fail, and the array might be reported as `missing`. To work around this, delete the array access point on the HP Storage Essentials Discovery Data Collection page (**Options > Storage Essentials > Discovery > Run Discovery Data Collection**) and then rediscover the array in HP SIM.

Discovery Information for LSI Storage Systems

To discover LSI storage systems, enter the following information in HP SIM:

- IP address or system name of the controller or proxy you want to discover.
- User name for the storage system. Even if your LSI storage system does not have a user name, you must enter something in the User Name box.
- HP SIM does not allow blank passwords. If the storage system does not have a password, you can enter any value in the password field.

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 that 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.

The management server communicates with HiCommand Device Manager through a non-secure 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. For more information, see "Communicating with HiCommand Device Manager Over SSL" on page 412.

Discovery Information for HDS Storage Systems

To discover HDS storage systems, enter the following information in HP SIM:

- The name or IP address of the server.
- If HiCommand Device Manager listens on a port other than 2001, enter the port number.
- 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 can 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 (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **Setup**), topology (**Tools** > **Storage Essentials** > **Home** > **Discovery** > **Topology**), and Discovery Data Collection (**Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**), lists. The management server does not display additional information about excluded elements in the user interface. The management server, however, does mention in the logs (**Tools** >

Storage Essentials > **Home** > **Discovery** > **View Logs**) that a provider instance has been created for an excluded element. You can ignore this message in the logs.

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

1. Select **Options** > **Storage Essentials** > **Manage Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command.

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

4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. Add the serial numbers corresponding to the HDS storage systems you want to exclude form 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**.

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.

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**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following command.

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

4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Remove the pound (#) symbol in front of the property to make sure it is not commented out. 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.

   > **NOTE:** To find the serial number, double-click the storage system in System Manager, and then click the **Properties** tab.

7. When you are done, click **Save**.
8. To force a refresh for elements that are not configured to skip the refresh, select the **Force Device Manager Refresh** option on the Discovery Data Collection page.
9. Click **Get Details** to run discovery data collection.

Discovering HP Storage Systems

You can discover the following HP storage systems. For model information, see the support matrix.

- Discovering HP StorageWorks MSA Arrays, page 142
- Discovering HP StorageWorks EVA Arrays, page 143
- Discovering HP StorageWorks XP Arrays, page 145

Discovering HP StorageWorks MSA Arrays

Before you can discover MSA arrays, you must download and install the HP MSA SMI-S Provider software. See the HP StorageWorks Modular Storage Array document at: http://www.hp.com/go/hpsim/providers for more information. Check this web site periodically to verify that you are running a current version of the SMI-S provider.

Keep in mind the following:

- MSA volumes must be deleted in the reverse order of their creation. For example, if you have six volumes, and you want to delete the second one you created, you must delete the volumes one at a time, starting with the volume created sixth and continuing with the fifth, fourth, third, and then the second.
- The Array Configuration Utility (ACU) application should not be running when HP Storage Essentials is using the MSA provider.
- The management URL on the Tools & Links tab for the MSA can be used only if the ACU is installed on the same host as the SMI-S provider and the Execution Mode is set to Remote Service. See the ACU *Readme* file for information about execution modes and how to change them.
- Selective Storage Presentation (SSP) for the array must be enabled for provisioning to work.

- The MSA SMI-S provider updates its cache every four minutes. If the array is managed by an application other than HP Storage Essentials, changes to the array configuration might not be reflected by a Discovery Data Collection task that ran before the cache update.

Discovery Information for an MSA

To discover an MSA, enter the following information in HP SIM:

- IP address of the server running the MSA SMI-S provider
- User name for accessing the MSA SMI-S provider
- Password for accessing the MSA SMI-S provider

Discovering HP StorageWorks EVA Arrays

The management server uses the built-in EVA provider. Before discovering EVA arrays, note the following:

- HP StorageWorks Command View EVA must be installed on a server before you can discover an HP EVA storage system.
- If you have both active and standby Command View EVA proxy machines, you can discover both the proxy machine that is actively managing the array, and the proxy machine that is not actively managing the array. If you discover only the proxy machine that is not actively managing the array, then only top level array information is collected.

  If both proxy machines are discovered, keep them in the same discovery group. They can be moved to other discovery groups, but they must be moved together to the same group at the same time. When discovering the proxy machines separately, the machine that has already been discovered must be in the Default discovery group. For more information about discovery groups, see "Using Discovery Groups" on page 162.
- EVA arrays can only be provisioned if they are actively managed by the Command View server that they are discovered through.
- When an EVA is discovered by the built-in EVA provider, a cache is created and populated with the current array configuration. Each subsequent cache refresh will start 30 minutes after completion of the previous cache refresh. The time the cache refresh takes depends on factors such as the EVA configuration, model, and SAN traffic.

  When you perform a provisioning operation (creating, deleting, or modifying a pool or volume), the cache information about provisioning is immediately updated. If you provision an EVA using Command View EVA or a different management station, the cached information about the EVA will not be accurate until the cache is refreshed.

Discovery Information for an EVA

To discover an EVA, enter the following information in HP SIM:

- IP address of the server running Command View EVA.
- User name for accessing the Command View server.
- Password for accessing the Command View server.

NOTE: The user name and password are the credentials of the Command View EVA administrator login.

Obtaining SNMP Traps using Command View EVA

You must configure Command View EVA so it can send SNMP traps from the EVA to HP Storage Essentials. When the management server receives these SNMP traps, it converts them to WBEM Indications for display in its Event Manager. HP Storage Essentials then forwards the events to HP SIM's event console.

Community String Requirements

- The default community string for Command View EVA 6.x is `Public` and the default community string for HP Storage Essentials is `public`. The community strings must be a case-sensitive match, so if you are using the default values in HP Storage Essentials and Command View EVA 6.x, you must change the community strings to a case-sensitive match.
- If you are using the default community strings for Command View EVA 7.x and HP Storage Essentials, no changes to the community strings are needed. If you change the community strings to non-default values, then they must be a case-sensitive match.

CAUTION: Other applications (such as HP SIM) may be using the default community strings to communicate with Command View EVA. If you change the community string in Command View EVA, you might break Command View EVA’s connection to other applications. If a change is needed, we recommend changing the community string in Storage Essentials to match the string in Command View EVA.

Obtaining SNMP traps from Command View

To obtain SNMP traps from Command View EVA:

1. Verify that the community strings follow the rules in ”Community String Requirements” on page 144. For information on viewing or changing community strings, see ”Viewing or Changing the Community String in HP Storage Essentials” on page 144, ”Viewing or Changing the Community String in Command View EVA 6.x” on page 144, or ”Viewing or Changing the Community String in Command View EVA 7.x” on page 145.
2. Configure event and host notification. For instructions, see ”Configuring event and host notification in Command View EVA” on page 145.

Viewing or Changing the Community String in HP Storage Essentials

To view or change the community string:

1. Select **Options** > **Storage Essentials** > **Manage Product Health**.
2. Click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the `cimom.snmpTrapListenerCommunityString` variable.
   The management server uses the value that is listed last, so be sure to search to the end of the page to locate the latest build.

5. Click **Close** to return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Change the value by entering `cimom.snmpTrapListenerCommunityString=<value>` where `<value>` is the desired community string value.
8. Click **Save**.

Viewing or Changing the Community String in Command View EVA 6.x

To view or change the community string:

1. Open the `c:\hsvmafiles\nsaserver.ini` file in a text editor on the Command View EVA server.
2. Find the line `Authority=Public`

   This example shows the Command View EVA 6.x default: `Public`.
3. Change the value to the desired community string. For example, if you want to change the community string to `public`, enter `Authority=public`
4. Restart the service for Command View EVA.

Viewing or Changing the Community String in Command View EVA 7.x

To view or change the community string:

1. Open the `C:\Program Files\Hewlett-Packard\Sanworks\Element Manager for StorageWorks HSV\config\cveva.cfg` file in a text editor on the Command View EVA server.
2. Find the following command lines:

   ```
   # Authority. Default = Public
   authority Public
   ```
3. Change the community string to the desired value. For example, if you want to change the community string to `public`, enter `authority public`
4. Restart the service for Command View EVA.

Configuring event and host notification in Command View EVA

See the HP StorageWorks Command View EVA user guide for instructions on configuring Command View EVA event notification. The Command View EVA documentation is available at http://www.hp.com/support/manuals.

Discovering HP StorageWorks XP Arrays

You can discover HP StorageWorks XP Arrays by using the following methods:

- Discovering HP XP Arrays by Using Command View XP and SMI-S, page 145
- Discovering HP XP Arrays by Using Command View XP Advanced Edition, page 146
- Discovering HP XP Arrays by using the built-in XP Provider, page 146

NOTE: HP StorageWorks Command View XP should be installed on a server before you discover an HP XP storage system.

Discovering HP XP Arrays by Using Command View XP and SMI-S

Before you can discover XP arrays, you must download and install the XP SMI-S Provider software. For instructions, see the HP StorageWorks XP Disk Array and Command View XP document for your version of Command View XP. You can access this document at: http://www.hp.com/go/hpsim/providers. Check this web site periodically to verify that you are running a current version of the SMI-S provider. See the support matrix for your edition for details.

IMPORTANT: The Command View XP SMI-S provider does not return information related to external storage available to the HP XP storage arrays, including the external LDEVs. As a result, that information is not available in the management server user interface or reports.

To discover an HP XP array using Command View XP and SMI-S:

- IP address or system name of the Command View XP server you want to discover.
- User name for accessing the XP SMI-S provider
- Password for accessing the XP SMI-S provider

Discovering HP XP Arrays by Using Command View XP Advanced Edition

HP StorageWorks Command View XP Advanced Edition must be installed on a server before you discover an HP XP storage system.

To discover an HP XP array using Command View XP Advanced Edition, enter the following information in HP SIM:

- IP address or system name of the server running Command View XP Advanced Edition.
- User name for accessing Command View XP Advanced Edition.
- Password for accessing Command View XP Advanced Edition.

Discovering HP XP Arrays by using the built-in XP Provider

To discover an HP XP array using the built-in XP Provider, enter the following information in HP SIM:

- IP address or system name of the XP storage system you want to discover.
- User name for accessing the XP storage system.
- Password for accessing XP storage system.

NOTE: The user name and password must be for a Partition Storage Administrator account.

Discovering IBM Storage Systems or IBM SVCs

Before you can discover an IBM storage system or an IBM System Storage SAN Volume Controller, you must have the IBM CIM Agent installed. For Enterprise Storage Server (ESS) devices, the IBM CIM Agent is called "CIM Agent for ESS"; for DS devices and mixed DS and ESS environments, use the "CIM Agent for DS Open (API)". It is best not to install the IBM CIM Agent on the HP Storage Essentials management server. For more information, see the *CIM Agent for DS Open (API) - Installation and Configuration Guide* for details on configuring the CIM Agent. Briefly, this procedure entails:

1. Installing the software (ESS devices only).

   The installation checks for the existence of the ESSCLI. If the ESSCLI is not installed, installation of the CIM Agent cannot proceed.

2. Configuring the 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. Unless a secure connection is required between the management server and the CIM Agent, it is best to use port 5988 and protocol HTTP.

3. Changing the default authentication method in order to discover the CIM Agent.

   a. Stop the IBM CIM Agent service, and then edit the `cimom.properties` file in `C:\Program Files\IBM\cimagent`.

   b. Open the `cimom.properties` file and change the following property to false:

   ```
   DigestAuthentication=False
   ```

4. Using the `setuser` command to configure a user to access the CIM Agent.

   The user credentials specified here are used to access the CIM Agent and are specified in the HP SIM discovery task. The credentials are not necessarily the same as those used to login to the ESS Specialist management utility or the DS Storage Manager.

5. Using the `setdevice` command to configure the ESS and DS devices that are managed through the CIM Agent.

   The `setdevice` command requires a valid user with the necessary privileges to access and configure the ESS or DS storage systems.

   a. Navigate to `\Program Files\ibm\cimagent\setdevice`.

   b. Do one of the following:

   - For ESS devices, enter `cmd addess <ipaddress> <username> <password>` where `ipaddress` is the IPaddress of the management console server of the ESS device and `username` and `password` are the management console credentials.
   - For DS devices enter `cmd addessserver <ipaddress> <username> <password>` where `ipaddress` is the IPaddress of the management console server of the DS device and `username` and `password` are the management console credentials.

6. Restarting the IBM CIM Agent service.

7. Verifying that the CIM Agent is able to communicate with the storage devices. Enter the following command to verify communication:

   `verifyconfig -u username -p password` where `username` and `password` are the credentials to access CIM Agent and were created by setuser.

Discovery Information for IBM Storage Systems/SVCs

To discover an IBM storage system or an IBM System Storage SAN Volume Controller (SVC), enter the following information in HP SIM:

- IP address or system name for the system running the IBM CIMOM or SVC you want to discover.
- Port number for the IBM CIMOM or SVC if a non-default port is used.
- User name of the IBM CIMOM or SVC.
- Password of the IBM CIMOM or SVC.

> **NOTE:** The IBM CIMOM user name and password are defined with the `setuser` command.

Discovering Sun StorEdge Storage Systems

You can discover the following Sun StorEdge systems. For more details, see the support matrix.

- Discovering Sun StorEdge 3510 Storage Systems, page 148
- Discovering Sun StorEdge 6920 and 6940 Storage Systems, page 149
- Discovering Sun StorEdge 6130 Storage Systems, page 149

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) - Follow the instructions in the readme file that is installed with the SUNWagsdk package.
- Sun StorEdge 3510 SMI-S Provider (SUNW3x10a package) - Follow the instructions in the readme file that is installed with the SUNW3x10a package.

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.

Discovery Information for Sun StorEdge 3510 Storage Systems

To discover an Sun StorEdge 3510, enter the following information in HP SIM:

- IP address or system name of the system running the Sun StorEdge 3510 SMI-S provider.
- User name of the system running the Sun StorEdge 3510 SMI-S provider.
- Password of the system running the Sun StorEdge 3510 SMI-S provider.

Discovering Sun StorEdge 6920 and 6940 Storage Systems

To discover an Sun StorEdge 6920 or 6940 storage system, enter the following information in HP SIM:

- IP address or system name of the storage system you want to discover.
- User name of the storage system you want to discover.
- Password of the storage system you want to discover.

Discovering Sun StorEdge 6130 Storage Systems

To discover an Sun StorEdge 6130 storage system, enter the following information in HP SIM:

- IP address or system name of the controller or proxy you want to discover.
- HP SIM does not allow blank user names. Enter anything for the user name.
- Password for the controller or proxy.

Discovering Xiotech Storage Systems

IMPORTANT: You must have Xiotech's Intelligent Control (ICON) software installed. If you do not have the software, contact your Xiotech representative.

To discover an Xiotech storage system, enter the following information in HP SIM:

- IP address or system name for the storage system. The system’s namespace (`/root/cimv2)`is one of the default namespaces in the `wbemportlist.xml` file on the server running HP SIM, so you do not need to add its namespace.
- HP SIM does not allow blank user names. Enter anything for the user name.
- HP SIM does not allow blank passwords. Enter anything for the password.

Discovering NAS Devices and Tape Libraries

Use the workflow in "Discovering Elements" on page 113 to discover NAS devices and tape libraries. This section provides information about supported NAS devices and tape libraries, including the information to enter in HP SIM during the discovery process. For more information on device support, see the support matrix. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in HP Storage Essentials).

Table 7 Discovery Requirements NAS Devices and Tape Libraries

Element	Discovery Requirements	For Additional Information
HP NAS devices	Discover the device directly.	See Discovering HP NAS Devices on Windows, page 150 and Discovering HP NAS Devices on Linux, page 151.
devices	Discover the device directly.	See Discovering NetApp NAS Devices, page 151.
Sun NAS devices	Discover the server running the SMI-S provider for the Sun NAS Devices.	See Discovering Sun NAS Devices, page 152.
HP and IBM tape libraries	Discover the server running the SMI-S provider for the tape library.	See Discovering HP and IBM Tape Libraries, page 152

Discovering NAS Devices

You can discover the following NAS devices:

- Discovering HP NAS Devices on Windows, page 150
- Discovering HP NAS Devices on Linux, page 151
- Discovering NetApp NAS Devices, page 151
- Discovering Sun NAS Devices, page 152

Discovering HP NAS Devices on Windows

In order to discover an HP NAS device on Windows, you must first install a CIM extension on the device and then modify one of its properties files. For instructions, see "Installing the CIM Extension for Microsoft Windows" on page 281.

To enable NAS support:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the `APPQCime/conf` directory.
3. Copy the `nas.properties-sample` file and paste a copy into the same directory.
4. Rename the copied file to `nas.properties`.

5. Open the file and locate the following line:

   ```
   # Set to true to enable NAS data collection; "false" is the default
   nas=false
   ```
6. Change the value to `true` to enable NAS support, as shown in the following example:

   ```
   nas=true
   ```
7. Save your changes and close the file.
8. Restart the CIM extension.

Discovery Information for HP NAS Devices on Windows

To discover an HP NAS device, enter the following information in HP SIM:

- IP address or system name of the HP NAS device to discover.
- User name of the HP NAS device. You must provide a privileged login.
- Password used to access the HP NAS device.

Discovering HP NAS Devices on Linux

In order to discover an HP NAS device on Linux, you must first install a CIM extension on the device and then modify one of its properties files. For instructions, see "Installing the CIM Extension for SUSE and Red Hat Linux" on page 227.

To enable NAS support:

1. Connect to the NAS device on which you have installed the CIM extension.
2. Browse to the installation directory and open the `/opt/APPQCime/conf` directory.
3. Copy the `nas.properties-sample` file and paste a copy into the same directory.
4. Rename the copied file to `nas.properties`.
5. Open the file and locate the following line:

   ```
   # Set to true to enable NAS data collection; "false" is the default
   nas=false
   ```
6. Change the value to `true` to enable NAS support, as shown in the following example:

   ```
   nas=true
   ```
7. Save your changes, and then close the file.
8. Restart the CIM extension.

Discovery Information for HP NAS Devices on Linux

To discover an HP NAS device, enter the following information in HP SIM:

- IP address or system name of the HP NAS device to discover.
- User name of the HP NAS device. You must provide a privileged login.
- Password used to access the HP NAS device.

Discovering NetApp NAS Devices

Keep in mind the following:

- SMNP must be enabled on the NetApp NAS device before it can be discovered.

- If you want to communicate with the NetApp NAS device through SSL you must set the `cimom.providers.netapp.useSSL` property to `true`. This is a global setting and will cause all NetApp NAS devices to communicate using SSL. For more information, see ”Enabling SSL Communication with a NetApp NAS Device” on page 152.
- If you want the management server to be able to receive events from a NetApp NAS device, you must add the IP address of the management server to the NetApp configuration.
- Administrative HTTP access to the device can be restricted through the `httpd.access` and `httpd.admin.access` options. If you are restricting Administrative HTTP access, 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. For more information, see the NetApp NAS device documentation.

Discovery Information for NetApp NAS Devices

To discover a NetApp NAS device, enter the following information in HP SIM:

- IP address or system name of the NetApp NAS device you want to discover.
- User name of the NetApp NAS device. 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
- Password used to access the NetApp NAS device.

Enabling SSL Communication with a NetApp NAS Device

To enable SSL communication with a NetApp NAS device:

1. Select **Options** > **Storage Essentials** > **Manage Product Health**, and then click **Advanced** in the Disk Space tree.
2. Click **Show Default Properties** at the bottom of the page.
3. Copy the following property:

   ```
   #cimom.providers.netapp.useSSL=true
   ```
4. Click **Close** to return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Uncomment the `cimom.providers.netapp.useSSL` property by removing the pound symbol (#) in front of `cimom.providers.netapp.useSSL`.
7. When you are done, click **Save**.

Discovering Sun NAS Devices

NOTE: You do not need to provide the `interop namespace` because it is included in the management server's list of default namespaces.

To discover a Sun NAS device, enter the following information in HP SIM:

- IP address or system name of the server running the provider for the Sun NAS devices you want to discover.
- User name of the provider for the Sun NAS devices you want to discover. You must provide a privileged login.
- Password used to access the provider for the Sun NAS devices you want to discover. See the HP SIM documentation for more details.

Discovering HP and IBM Tape Libraries

Before you can discover an HP or IBM tape library, you must download and install the corresponding SMI-S provider software.

- See your IBM documentation and the support matrix for your edition for information about the SMI-S provider for IBM tape libraries.
- See the *HP StorageWorks Enterprise Systems Library (ESL) E-Series* document for more information about the SMI-S provider for HP tape libraries. You can access this document at: http://www.hp.com/go/hpsim/providers. Check this web site periodically to verify that you are running a current version of the SMI-S provider. See the support matrix for your edition for details.

To discover an HP or IBM tape library, enter the following information in HP SIM:

- IP address of the system that is running the tape library SMI-S provider.
- User name of the SMI-S provider of the tape library.
- Password of the SMI-S provider of the tape library.

Discovery Data Collection

IMPORTANT: Access Discovery Data Collection by selecting **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**. Do not use the HP SIM **Options** > **Data Collection** command; it is for a different HP SIM feature.

This section contains the following topics:

- About Discovery Data Collection, page 153
- Running Discovery Data Collection, page 154
- Stopping Discovery Data Collection, page 154

About 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:

- Running Discovery Data Collection takes time. You might want to perform this process when the network and the managed elements are not busy.
- Reports show data from the last successful Discovery Data Collection and report cache update. When a scheduled Discovery Data Collection finishes, the report cache refreshes automatically. If you run Discovery Data Collection manually, the report cache updates every 6 hours. For information about refreshing the report cache, see the User Guide.
- During Discovery Data Collection the data you see in the user interface is not updated until the data collection is finished.
- During Discovery Data Collection, the topology in System Manager is recalculated. While the topology is being recalculated, the loading of the user interface in Storage Essentials may be slow. See"Recalculating the Topology" on page 414for more information.
- You can use discovery groups to break up Discovery Data Collection. For example, instead of running Discovery Data Collection for all elements, you could specify only the elements in Discovery Group 1. For more information, see "Using Discovery Groups" on page 162.
- When an element in a discovery group is updated, its dependent elements are also updated.
- You can quarantine elements to exclude them from Discovery Data Collection. For example, if you want to get information about all the elements in a discovery group except for one, you can quarantine that element. For more information, see "Placing an Element in Quarantine" on page 166.
- If a problem occurs with a host or SMI-S element during Discovery Data Collection, the host or element is automatically quarantined. To remove the element from quarantine, see "Removing an Element from Quarantine" on page 166.
- If you want to receive status reports about Discovery Data Collection, see "Configuring E-mail Notification for Discovery Data Collection" on page 398 for information about how to configure this option.
- If an element changes and you run Discovery Data Collection while the provider cache is updating, an error might occur or the gathered details might be inconsistent with the actual element status.

Running Discovery Data Collection

To obtain details about the elements on the network:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.
2. Select **Include infrastructure details**, which gathers the latest information about SAN details. You do not need to select **Include backup details** unless you have already discovered hosts running backup applications and installed CIM extensions on those hosts. For information about

discovering master backup servers, see "Step 1 — Discovering Your Hosts and Backup Manager Hosts" on page 297.

3. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for your storage systems to obtain the latest information. If you do not select **Force Device Manager Refresh**, the management server gathers information from the external databases such as HP, HDS, and EMC storage systems with the assumption that the information in the external database is up to date. See the following topics for more information: "Excluding EMC Symmetrix Storage Systems from a Forced Device Manager Refresh" on page 137 and "Excluding HDS Storage Systems from Force Device Manager Refresh" on page 141.
4. Select **All Discovery Groups**, or click **Specified Discovery Groups** to specify a customized list. If you are running Discovery Data Collection for the first time, select **All Discovery Groups**.

   NOTE: For information on selecting a custom discovery list, see "Creating Custom Discovery Lists" on page 162.

5. Click **Get Details**.

   During Discovery Data Collection, the software changes its status light from green to red, and the HP Storage Essentials log opens and shows the progress of Discovery Data Collection.

   When the software finishes getting all element details, it displays `GETTING ALL DETAILS COMPLETED` on the View Logs page and the status light turns green.

   For information about automating the gathering of all element details, see the User Guide.

Stopping Discovery Data Collection

Discovery Data Collection takes some time. If the network and managed elements are busy, you might need to stop Discovery Data Collection and reschedule it for another time.

IMPORTANT: If you stop Discovery Data Collection, you should reschedule it. This type of collection obtains detailed information about elements in the network.

To stop Discovery Data Collection:

1. Select **Options** > **Storage Essentials** > **Discovery** > **View Logs**.
2. On the View Logs page, 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 Discovery Data Collection.

   NOTE: Existing operations will finish before the management server stops Discovery Data Collection.

4. Schedule a time to resume Discovery Data Collection.

Other Discovery Features

This section contains the following topics:

Selective Discovery Filter

The selective discovery filter allows you to filter the devices that are passed from HP SIM to HP Storage Essentials for discovery operations. The filter is a file that contains a list of IP addresses that should (or should not) be passed to HP Storage Essentials. The filter does not affect device discovery operations in HP SIM, it only restricts the data that is passed from HP SIM to HP Storage Essentials. The filter examines each device HP SIM discovers before passing the discovery information to HP Storage Essentials. In the case of multi-homed devices, the filter operation uses all reported IP addresses for a given device in deciding whether or not to pass data to HP Storage Essentials.

The selective discovery filter file is called `SEDiscoveryFilterList` (with no file extension). The file resides in:

- `<HP SIM install directory>/config` on Windows
- `/etc/opt/mx/config` on Linux

A sample file called `SEDiscoveryFilterList.sample` is available.

NOTE: The sample file is located in `<HP SIM install directory>/config` on Windows and `/opt/mx/config` on Linux.

Editing Rules for the Selective Discovery Filter

Use the following rules when editing the selective discovery filter:

- If you edit the selective discovery filter on a Windows system, do not use Notepad because it will not preserve the file formatting.
- If you want to edit the selective discovery filter file at run time, set the following property to true in the `globalsetting.props` file:

  `StorageEssentialsDiscoveryFilterReload=true`.

NOTE: The `globalsetting.props` file is located in `<HP SIM install directory>/config` on Windows and `/etc/opt/mx/config` on Linux.

This setting allows the HP SIM Connector to access the new filter file without being restarted. After the HP SIM Connector accesses the file, you can change this setting to `false` if there will not be any changes in the future. With the false setting the file will not get loaded again when the filter is needed because the HP SIM Connector uses the cached and compiled filter.

If you update the `globalsetting.props` file, you must restart HP SIM to activate the changes.

- Each line of the `SEDiscoveryFilterList` file indicates a flag, an IP address, or a comment. For example, in the sample selective discovery filter file below, `inclusive` and `exclusive` are flags, items preceded by the pound sign (#) are comments, and the numbers indicate IP addresses or IP address ranges.

```
inclusive
12.34.45.23
14.255.255.23
12.34.45.56 - 12.44.45.34
16.111.*
16.34.*.* - 17.45.7.13
23.22.* - 23.34.*

exclusive
12.35.44.23
#14.24.255.23
12.34.45.67 - 12.44.44.34
16.111.3.*
16.34.23.* - 17.45.7.*
23.22.12.* - 23.34.12.*
```

- Mixing flags, comments, and IP addresses on a single line can result in an invalid line that will not be processed.

Rules for the Inclusive and Exclusive Flags

The filter file uses `inclusive` or `exclusive` flags to indicate inclusive or exclusive filters. IP addresses are checked against and must pass all specified filters, both `inclusive` and `exclusive`.

Use the following rules when entering inclusive and exclusive filters in the selective discovery filter file:

- The `inclusive` flag indicates that only the IP addresses or ranges listed in the `inclusive` section of the file will be included when HP SIM passes the discovered IP addresses to HP Storage Essentials.
- The `exclusive` flag indicates that the IP addresses or ranges listed in the `exclusive` section of the file will be excluded when HP SIM passes the discovered IP addresses to HP Storage Essentials.
- If both filter types exist, `inclusive` filters are processed first.

- If an IP address exists in both the exclusive and inclusive lists, the `exclusive` filter takes priority and the IP address is not passed to HP Storage Essentials.
- If the `inclusive` and `exclusive` flags are missing from the file, any IP addresses in the file will be considered inclusive.
- Any IP addresses, ranges, or patterns that follow the `inclusive` flag are considered part of the `inclusive` list until the end of the file or the exclusive flag.
- Any IP addresses, ranges, or patterns that follow the `exclusive` flag are considered part of the `exclusive` list until the end of the file or the inclusive flag.

IP Address Formats Allowed

Use the following rules when entering IP addresses in the selective discovery filter:

- The IP address format must comply with IP v4. For example, 12.3.4 is invalid.
- Only numbers less than or equal to 255 are allowed. For example, 124.345.254.12 is invalid because 345 is not allowed.
- Use the pound symbol (#) to indicate comments.
- You can use wild cards to specify explicit IP addresses, IP ranges, or IPs.

Characters Allowed

Use the following rules when entering characters in the selective discovery filter:

- Only the digits 0-9 and the following characters are allowed dot (.), dash (-) and wild card (*).
- A wild card stands for a number, not a digit. Only trailing wild cards are allowed. For example, 192.168.144.*, 192.168.*.* or 192.*.*.* are allowed but 19*.34.3*.4 and 198.168.*.144 are not allowed.
- If *.*.*.* or * is included or excluded, it is treated as an invalid entry.
- Invalid entries are ignored.

Configuring the Selective Discovery Filter

To configure the selective discovery filter:

1. Use a text editor to create a file named `SEDiscoveryFilterList` (with no file extension), or make a copy of the sample file (`SEDiscoveryFilterList.sample)` and rename the file to `SEDiscoveryFilterList`.

   NOTE: The sample file is located in `<HP SIM install directory>/config` on Windows and `/opt/mx/config` on Linux.

2. To create an inclusive filter, enter `inclusive` in the file, and then add IP addresses, ranges, or patterns (one per line). Be sure to include all IP addresses that should be passed to HP Storage Essentials. For a sample file, see "Editing Rules for the Selective Discovery Filter" on page 156.
3. To create an exclusive filter, enter `exclusive` in the file, and then add IP addresses, ranges, or patterns (one per line). Be sure to include all IP addresses that should not be passed to HP Storage Essentials.

NOTE: When entering filters, follow the "Editing Rules for the Selective Discovery Filter" on page 156.

4. Save the file in the following directory on the HP SIM management server.
   - Windows: `<HP SIM install directory>/config`
   - Linux: `/etc/opt/mx/config`

Discovering a Single Element using the Manual Tab

IMPORTANT: When HP Storage Essentials is integrated with HP SIM, running discovery from the Automatic tab provides the best feedback for HP Storage Essentials discovery. For instructions on discovering elements from the Automatic tab, see "Discovering Elements" on page 113.

You can use the Manual tab to add a single element that HP SIM has not yet discovered. If you use this method, there is no direct feedback on the status of the HP SIM and HP Storage Essentials operations that take place during discovery. To view HP SIM progress, however, you can check the relevant collection in the user interface.

To discover a single element using the Manual tab:

1. Select **Options** > **Discovery**, and then click the **Manual** tab.
2. Enter the system name or IP address. Simple or fully qualified domain name (FQDN) host names can be entered. However, ranges of host names are not allowed.
3. If you have not entered the WBEM credentials for this system previously, click **More Settings**, and then enter the credentials in the **WBEM Settings** section. For information on credentials, see "Using Credentials" on page 108.
4. Click **Add System** to add the system to the database.

   HP SIM starts the discovery process.

   To view HP Storage Essentials progress, open the HP Storage Essentials Log and click **Refresh** in the next two to three minutes to view the HP Storage Essentials processing status.
5. Select **Tasks & Logs > View HP Storage Essentials Log**. Once the HP Storage Essentials log shows that the element has been processed, click **Details**, select the element, and then click **Get Details**.

Changing Credentials for Discovery

You can change the user name and password the software uses to access an element. Whenever a user name or password changes on an element the management server monitors, the management server must be made aware of the change.

IMPORTANT: These procedures change only the user name and password stored in the database for HPSIM. They do not change an element user name and password.

If you change a credential through the HP SIM CLI, you must run discovery to pass the credential to HP Storage Essentials.

To change a system protocol setting:

1. Select **Options** > **Protocol Settings** > **System Protocol Settings**.
2. Select the target system, and then click **Next**.
3. In the WBEM settings section, select the **Update values for this protocol** check box.
4. If you are changing only a password, enter the new password. If you need to replace a user name with a new one, delete both the old user name and the password and enter new ones.

   To make sure you enter the right credentials, select the **Also run system identification (recommended)** option to have HP SIM verify the credentials.
5. Click **Run Now** for the change to take effect immediately or **Schedule** to make the change later.

To change a global protocol setting:

1. Select **Options** > **Protocol Settings** > **Global Protocol Settings**.
2. Enter the new settings as specified in the documentation for HP SIM.
3. Click **OK**.

   The credential change will be passed to HP Storage Essentials automatically.
4. Run discovery (Optional). For instructions, see the HP SIM documentation.

Saving Discovery Settings to a Hosts File

After you have discovered your elements, you can save the discovery settings of the elements in your discovery list to an HP SIM hosts file. You could use the hosts file during certain upgrade activities or if you have a standby server and need to restore the HP SIM database.

To save discovery settings to a file:

1. Select **Options** > **Discovery** on the HP SIM home page menu.
2. Click the **Hosts Files** tab, and then click **New**.
3. In the Name box, enter a name for the new hosts file (required).
4. Select the **Systems loaded from the central management server, sorted by** option and select the way you want the elements sorted when you save the file. The choices are:
   - IP address
   - System name
   - System type and then by IP address
   - System type and then by System name.
5. Click **Initialize Now** to load the hosts file.

   The content appears in the Contents box.

6. Click **OK** to save the hosts file.

   The saved file appears on the Hosts Files page.

NOTE: See the HP SIM documentation for more information about hosts files.

Importing a Hosts File

NOTE: If you import a Hosts file and use it for discovery in HP SIM, you must discover the HP Storage Essentials management server as described in "Enabling Product Health Monitoring" on page 111 and "Discovering the HP Storage Essentials Management Server" on page 112.

If you have a previous `hosts` file you can import it, rather than re-entering the information. For more information, see "Saving Discovery Settings to a Hosts File" on page 159.

To import a list of hosts:

1. Select **Options** > **Discovery**.
2. Click the **Hosts File** tab.
3. Click **New**.
4. In the Hosts file name box, enter a name for the new `hosts` file. This box is required.
5. Under Initialize contents select **Systems loaded from hosts file**. Enter the file name and location (for example, `c:\doc.txt`) or click **Browse** to browse to the location of the hosts file.
6. Click **Initialize Now** to load the `hosts` file. The contents of the selected file appear in the Contents box.
7. Click **OK** to save the `hosts` file.

NOTE: See the HP SIM documentation for more information about hosts files.

Viewing Log Messages

Use the View Logs page to obtain the status of the following:

- Discovery
- Discovery Data Collection

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

To view logs for these operations:

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

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

For example, if a host was not discovered, the log messages might indicate that 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 Windows Management Instrumentation (WMI).

NOTE: The logs show data from the most recent discovery, test, or data collection task.

Viewing the Status of System Tasks

The Task Dashboard allows you to view the status of the tasks running on the management server. The dashboard provides the name of each task, its latest status, and the time the status was last reported.

To view the status of system tasks:

1. Select **Tools** > **Storage Essentials** > **Home** > **Discovery** > **System Tasks**.
2. To obtain the latest status, click **Get the Latest Status**.

The following task statuses are provided by the Task Dashboard:

Table 8 Task Status descriptions

Status	**Description**
Not Found	This task can not be found on this server.
Completed	This task has been completed successfully.
Failed	This task failed with an error.
Aborted	This task has been aborted by the user or other automated actions.
In Progress	This task is in progress. CPU and disk activities are active on this server.
Queued	This task is scheduled to be executed in the future.
Rejected	This task has been rejected by this server.

Using Discovery Groups

The discovery groups feature is sometimes called *segmented replication* because it allows you to run Discovery Data Collection for a segment of elements. Because The HP Storage Essentials product runs more slowly when Discovery Data Collection is in progress, it is helpful to break the process into segments which can then be run at night or on multiple days. For example, if Discovery Data Collection for all elements takes twelve hours, you could break the elements into several small groups and schedule Discovery Data Collection to run at night on multiple days.

NOTE: For more about data collection, see "About Discovery Data Collection" on page 153.

When planning discovery groups, consider the following requirements and capabilities:

- By default, HP Storage Essentials is configured with a default discovery group plus four additional groups.
- Discovery groups affect the amount of memory needed for HP Storage Essentials. Before configuring discovery groups, check the support matrix for your edition and verify that your system meets the memory requirements for using discovery groups.
- Do not move elements between discovery groups when Discovery Data Collection is running. If you do this, an error will occur when Discovery Data Collection tries to locate elements that were moved.
- An element can be a member of only one discovery group at a time.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of HP Storage Essentials cannot be added to discovery groups. These elements can, however, be placed independently into scheduled Discovery Data Collection tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. For more information, see "Creating Custom Discovery Lists" on page 162.
- When an element in a discovery group is updated, its dependent elements are also updated.
- Each discovery group communicates over a specific port. The defaults ports are:

Table 9 Discovery Group Ports

Default	5986
Discovery Group 1	5984
Discovery Group 2	5982
Discovery Group 3	5980
Discovery Group 4	5978

Creating Custom Discovery Lists

You can create a discovery list for Discovery Data Collection, which will allow you to select a set of discovery groups to use the next time Discovery Data Collection runs.

To create a custom discovery list:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.
2. Click the **Specified Discovery Groups** link.
3. Select the check box next to each item you want to add to the discovery list.

   Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of the product appear in the list individually. You can add individual elements, discovery groups, or both to the same discovery list.
4. Click **Add Selected Discovery Groups to Discovery List** to move them into the Discovery List.

IMPORTANT: Do not run Discovery Data Collection for all discovery groups simultaneously.

5. Click **OK** to save and return to the previous window. The elements are selected in the elements table.
6. Click **Get Details**.

Managing Discovery Groups

You can manage discovery groups from the Discovery Data Collection page.

NOTE: The Default discovery group cannot be edited.

To edit a discovery group:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.
2. Click **Manage Discovery Groups**.

   The Discovery Groups page shows a list of your discovery groups, including the name, port number, and included elements.
3. Click **Edit** ✎.
4. To rename the group, enter a new name in the Name box.
5. To add a member, select the member from the Potential Members section, and then click the **Add Selected Discovery Groups to Discovery Group** button to move it into the Current Members section.
6. To remove a member, select the member from the Current Members section, and then click the **Remove Selected Discovery Groups from Discovery Group** button to move it into the Potential Members section.

   NOTE: The path to the log file for the discovery group is listed at the top of the page.
7. Click **OK** to save the changes.
8. Click **Back to Discovery Page**.

Moving Elements Between Discovery Groups

In the initial discovery, all elements are placed in the Default discovery group. After the initial discovery, you can move elements between discovery groups.

IMPORTANT: Do not move elements between discovery groups when Discovery Data Collection is running. If you do this, an error will occur when Discovery Data Collection tries to discover elements that were moved.

Method 1: Select Discovery Group

To select a new discovery group for an element:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.

   The Discovery Data Collection page appears.
2. Select the check box for the element you want to move.
3. Click **Move to Discovery Group**.

   The Select Discovery Group window appears.
4. Select the new discovery group for the selected element.
5. Click **OK**.

   HP Storage Essentials notifies you that it can take a few minutes to move an element.
6. Click **OK**.

   The elements are moved to the new discovery group.

Method 2: Edit a Discovered Element

To edit a discovered element:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.

   The Discovery Data Collection page appears.
2. Click the **Edit** (✎) button next to the element you want to modify.
3. Select a new discovery group in the **Discovery Group** menu.
4. Click **OK**.

   HP Storage Essentials notifies you that it can take a few minutes to move an element.
5. Click **OK**.

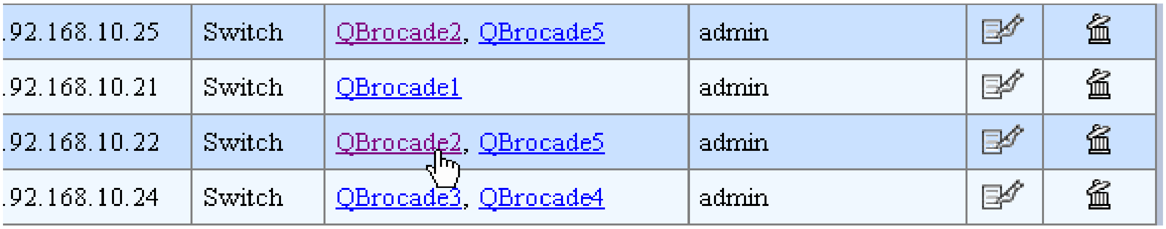
   The elements are moved to the new discovery group.

Deleting Discovered Elements

To remove a discovered element completely you must delete it from both HP SIM and HP Storage Essentials. If you do not do this, the deleted element can reappear under the following circumstances:

- If a scheduled automatic discovery task includes the deleted element, HP SIM will rediscover it during the next discovery.
- If HP Storage Essentials still lists the access point for the element, HP Storage Essentials rediscovers the element during the next Discovery Data Collection.

  You must determine the access points for the element you want to delete. In the following figure QBrocade2 is accessed by two switches: 192.168.10.25 and 198.168.10.22. You must delete both access points to completely remove the element. As a result, the QBrocade5 switch will also be removed because it has the same access points as QBrocade2.



.92.168.10.25	Switch	QBrocade2, QBrocade5	admin	✎	🗑
.92.168.10.21	Switch	QBrocade1	admin	✎	🗑
.92.168.10.22	Switch	QBrocade2, QBrocade5	admin	✎	🗑
.92.168.10.24	Switch	QBrocade3, QBrocade4	admin	✎	🗑

Figure 9 Deleting Discovered Elements from the Management Server

NOTE: If HP Storage Essentials and HP SIM are installed on the same computer, you cannot delete the HP Storage Essentials management server from HP SIM.

Removing an Element

1. Click **All Systems** in the System and Event Collections pane on the HP SIM home page, click **Systems** in the left pane.
2. Select the elements you want to delete.
3. Click **Delete**.
4. If the element is part of an HP SIM automatic discovery task, remove it from the task.
5. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.
6. Select the element you want to delete, and click **Delete**.
7. Select **Tools** > **Storage Essentials** > **Home**
8. Click **Discovery** and then click **Setup**.
9. Select the element you want to delete, and click **Delete**.

Deleting a single element from an access point

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 menu.

     If you are blocking pop-ups you must disable the popup blocker before you can delete the element.
   - In Chargeback Manager—Click the **Delete** (🗑) button for the element you want to delete.
2. If the element has multiple access points, you are asked which one you want to delete. Take one of the following actions:
   - 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.

- 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 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**.
4. Be sure to delete the element from any scheduled automatic discovery task in HP SIM. If a scheduled automatic discovery task includes the deleted element, SIM will rediscover the deleted element during the next automatic discovery task.

Working with Quarantined Elements

When an element is quarantined, it is not included in the Discovery Data Collection process until it is removed from quarantine. For more information, see "Removing an Element from Quarantine" on page 166. If a problem occurs with a host or SMI-S element during Discovery Data Collection, the host or element is automatically quarantined.

Placing an Element in Quarantine

When you click **Get Details** on the Discovery Data Collection page, the management server automatically obtains details for the elements in the selected discovery group. Assume you want to discover all the elements in a discovery group, except for one, which is being taken off of the network for maintenance. You can use the quarantine feature to exclude this element 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 **Set Quarantine**.
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 **Clear Quarantine**.
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.

Updating the Database with Element Changes

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

Keep in mind the following:

- If you are adding, removing or replacing McDATA or Connectrix switches, you must use a different procedure. For more information, see "Managing McDATA and EMC Connectrix Switches" on page 132.
- Running Discovery Data Collection takes time. You might want to run this process when the network and the managed elements are not busy.

To update the database:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.
2. Select **Include infrastructure details**, which gathers information about SAN details.

> **NOTE:** **Include backup details** is used for gathering information for Backup Manager. You do not need to select it unless you have already discovered hosts running backup applications and installed CIM extensions on those hosts. For more information about discovering master backup servers, see "Step 1 — Discovering Your Hosts and Backup Manager Hosts" on page 297.

3. The management server obtains most of its information from device managers for storage systems with external databases, such as HP, HDS, and EMC storage systems. Select **Force Device Manager Refresh** if you want the management server to tell the device managers for your storage systems to obtain the latest information. If you do not select **Force Device Manager Refresh**, the management server gathers information from the external databases based on the assumption the information in the external database is up-to-date.

   For more information, see the following topics: "Excluding EMC Symmetrix Storage Systems from Discovery" on page 136 and "Excluding EMC Symmetrix Storage Systems from a Forced Device Manager Refresh" on page 137.
4. Click **Get Details**.
5. Select **Tasks & Logs** > **View Storage Essentials Log to** View the status of the gathering of element details. For more information, see "Viewing Log Messages" on page 160.

6. Select **Tools > Storage Essentials > System Manager** to access System Manager and verify that the topology is displayed correctly.

5 Managing Licenses

Some of the features described in this chapter are not included in HP Storage Essentials Standard Edition. To determine which features apply to your product, see the List of Features.

Standard Edition supports a subset of the devices supported by Enterprise Edition. For a list of the devices supported by Standard Edition, see your product's *Support Matrix*. The List of Features and the support matrix are also accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

About the License

The management server restricts the number of elements it manages through its license. It is important you keep your license up to date with the requirements of your network. The management server has several different types of license restrictions, as shown in Table 10 on page 171.

Table 10 License Restrictions

Type of Restriction	Description	Unit of Measurement
MAPs	The management software restricts the number of hardware elements it manages through the use of managed access points (MAPs) for hardware. A MAP is the sum of all storage access ports of all hardware elements that the management server manages. See Table 11 on page 173 for more information.	Number of MAPs

Table 10 License Restrictions

Type of Restriction	Description	Unit of Measurement
Backup Size	The management server determines licensing for Backup Manager through gigabytes (GB). The management server compares the number of gigabytes for Backup Manager with what you are backing up. If you are backing up more than your license allows, you are warned the next time you log onto the management server.	Gigabytes (GB)
Raw NetApp Capacity	The Raw NetApp Capacity is the total disk capacity (unformatted capacity) of all discovered NetApp filers.	Terabytes (TB)
Managed Exchange Instances	The management server determines licensing for Microsoft Exchange instances by counting the number of instances of Microsoft Exchange it manages.	Number of instances of Microsoft Exchange the software manages
Managed Database Instances	The total number of instances of the following databases the software manages: • Microsoft SQL Server • Oracle • Sybase Adaptive Server Enterprise • InterSystems Caché This total is broken down by each type of database in the table.	Number of managed databases

Table 10 License Restrictions

Type of Restriction	Description	Unit of Measurement
For File System Viewer	The management server determines licensing for File System Viewer through terabytes (TB). When you purchased File System Viewer, you were given a number of TB you were allowed by the management server to monitor. The management server detects the number of TB that are being monitored on file servers and verifies that number is at or below the purchased amount. You do not have to monitor everything associated with your file server. You can choose to manage only the mount points that are important to you. Only the files associated with these mount points are counted toward the file server TB.	Terabytes (TB)

IMPORTANT: The management server Current Usage Summary is first updated six hours after the management server (AppStorManager) starts, and then the updates occur every 24 hours thereafter. Elements the management server has discovered before the update are not reflected in the Current Usage Summary table. The time for the update is determined when the management server is first started. For example, the first update of the Current Usage Summary table occurs six hours after the management server is first started. The following updates occur every 24 hours. If the management server is started for the first time at noon, the first update of the Current Usage Summary table would occur at 6 p.m. All following updates would always occur at 6 p.m.

MAPs are determined as described in Table 11 on page 173.

Table 11 Determining Managed Access Points

Element	Managed Access Point
Hosts	The managed access points (MAPs) are the number of Fibre Channel ports with a minimum of one MAP. If a host has no Fibre Channel ports, the software assumes one MAP. The software does count direct attached storage, provided it is supported by the management server.
Switches	All ports on a switch are counted as MAPs.

Table 11 Determining Managed Access Points (continued)

Element	Managed Access Point
Storage systems	The MAPs are the sum of all front-facing ports. Storage systems with FA ports the software does not support, such as mainframe attached FICON, are still counted as MAPs. However, the management server does not count MAPs from storage systems it does not support. See the release notes for information about supported storage systems.

Example 1:

Assume you have the following environment:

- Brocade (two switches of 12 ports each, one switch of 16 ports) — Total 40 ports
- McDATA (one switch of 64 ports) — Total 64 ports
- Windows 2000 and Solaris Hosts (10 hosts with two Fibre Channel connection each) — Total 20 ports
- EMC Subsystem (one subsystem with 16 Fibre Channel ports) — Total 16 ports

The software calculates 140 MAPs in this environment.

Example 2:

Assume you have the same configuration above, and you add several devices to your network that the management server does not support. There are still 140 MAPs in this environment, since the management server does not count the ports from devices it does not support.

Example 3:

Assume you have the same configuration as the first example, with two Windows 2000 hosts that are directly attached to storage systems, with no Fibre Channel (FC) connections and with a total of 0 FC ports, as shown in the following figure:

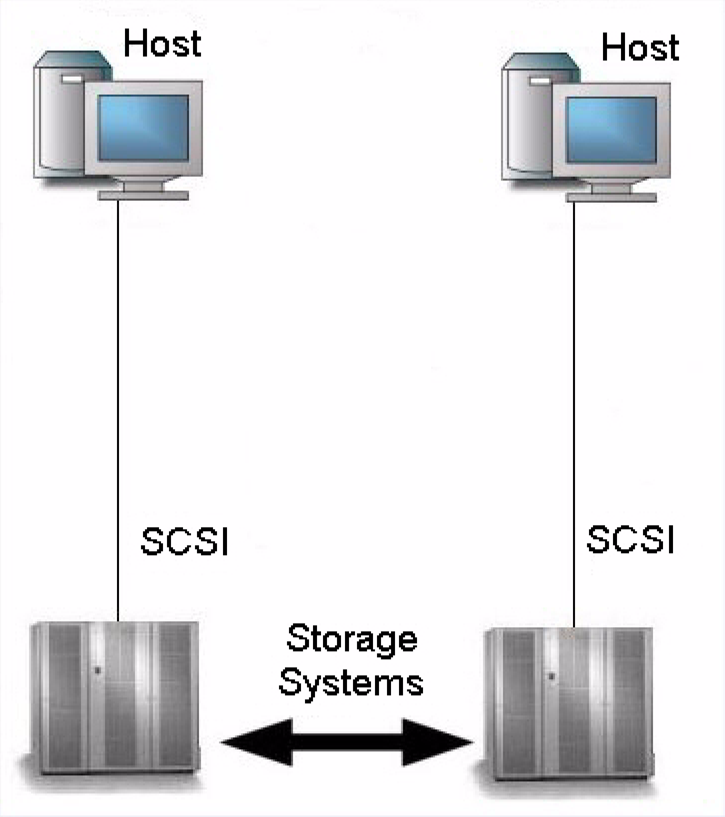


Figure 10 An Example of Direct Attached Storage

The software calculates four MAPs (see the figure), since we assume one MAP for each host, even though it has no Fibre Channel ports. The storage systems are counted, since they are supported by the management server. If you include the MAPs from the first example (140 MAPs), it brings the total to 144 MAPs.

If we had a configuration which included a switch, two managed hosts, and several unmanaged hosts, the MAPs would not be used against the unmanaged hosts.

Some switches allow the user to turn off an unused GBIC. (Gigabit Interface Converter). If a GBIC is turned off, the port is not counted. However, if the GBIC is turned on, or if there is no GBIC, the port is counted.

Importing a License File

If you cannot find the license file you want to import or if you are interested in expanding your license for managing additional elements, follow your organization’s procedures to contact your software or support representative for assistance.

To import a license file,

1. Select **Deploy** > **Storage Essentials** > **License Manager** > **Manage Storage Essentials Keys** in HP Systems Insight Manager or select **Security** > **Licenses** in HP Storage Essentials.
2. Select **Import License File**.
3. Select **Browse**.

   You are shown the file system of the computer being used to access the management server.
4. Select the license file.
5. Select **OK**.

Viewing Cumulative Licenses

Use the View Cumulative License feature to view the complete number of elements the management server supports at the current time. The software adds up the number of licensed components from the licenses and takes into account the expiration date. See Table 10 on page 171 for more information about the licensing capacities displayed.

IMPORTANT: You cannot modify the license file, since it is encrypted. If you want to increase the number of elements the management server is allowed to manage, follow your organization’s procedures to contact your support representative.

To view cumulative licenses:

1. Select **Deploy** > **Storage Essentials** > **License Manager** > **Manage Storage Essentials Keys** in HP Systems Insight Manager or select **Security** > **Licenses** in HP Storage Essentials.
2. Select **View Cumulative Licenses**.

   The properties for the cumulative licenses are displayed:

   Notice in the **Cumulative License** window that each feature has a property that is set to either true or false. If a value for a property is set to true, your license lets you access that feature. Likewise, if the value is set to false, the license does not let you access that feature.

   You can determine how many elements your licenses supports by looking at the **Current Usage Summary** table at the bottom of the page. The cumulative number for each type of licensed capacity is displayed in this table.

Viewing a Specific License

IMPORTANT: Do not manually edit the license. If you want to increase the number of elements the management server is allowed to manage, contact technical support.

To view the content of an individual license:

1. Select **Deploy** > **Storage Essentials** > **License Manager** > **Manage Storage Essentials Keys** in HP Systems Insight Manager or select Security > LIcenses in HP Storage Essentials.
2. Select the 🔍 button corresponding to the license you want to view.

The license’s name and file name are listed, along with its properties.

You can determine how many MAPs and/or managed application licenses (MALs) this license supports by looking at the properties in the license file. However, that can be misleading if you have other licenses that also provide support for MAPs and MALs. It is suggested you look at the cumulative licenses to obtain a total of the MAPs and MALs that are supported. See the topic,”Viewing Cumulative Licenses” on page 175 for more information about viewing cumulative licenses.

The MALs are split into three properties, LICENSE_FSRM_SIZE_TB, LICENSE_MAL_DATABASE, LICENSE_MAL_EXCHANGE. The following properties are used for tracking MAPs and MALs:

- LICENSE_FSRM_SIZE_TB — The amount of space in Terabytes you are allowed for File System Viewer.
- LICENSE_MAL_DATABASE — The number of database application instances, such as Oracle and Sybase Adaptive Server Enterprise, that the management server is allowed to monitor.
- LICENSE_MAL_EXCHANGE — The number of Microsoft Exchange instances the management server is allowed to monitor.
- LICENSE_MAPS — The number of MAPs the management software is allowed to manage.

Deleting a License

IMPORTANT: Before you delete a license, make sure you have made a copy of it. If you delete the wrong license, you may lose access to certain features and/or access to the product. The management server saves the license files in the `“drive where management server installed”\data\licenses` folder.

To delete a license:

1. Select **Deploy** > **Storage Essentials** > **License Manager** > **Manage Storage Essentials Keys** in HP Systems Insight Manager or select **Security** > **Licenses** in HP Storage Essentials.
2. Select **Licenses** from the menu.
3. Select the 🗑 button corresponding to the license you want to delete.

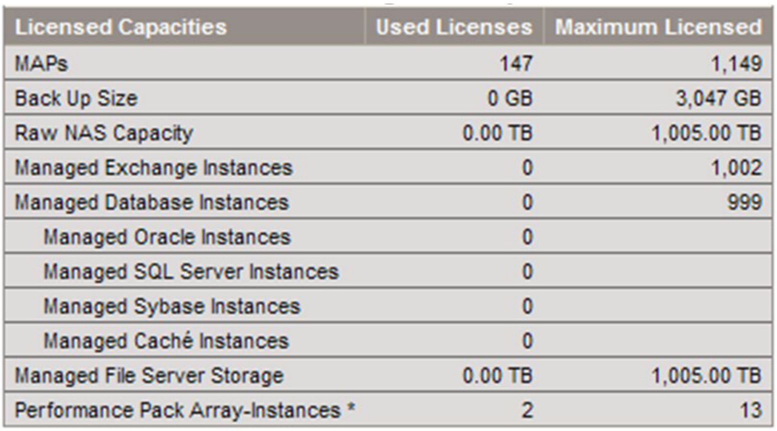
License Setup for Array Performance Pack

The Array Performance Pack license provides the ability to collect and report additional performance data for specified HP EVA arrays. The number of required licenses depends upon the number of arrays you want to include for the additional collection and reporting.

IMPORTANT: You must complete a Discovery Data Collection for the EVA arrays before importing the license and starting the collectors. After importing the license, you can start the data collectors from the Performance Data Collection page (**Optimize** > **Storage Essentials** > **Performance Data Collection**). Although EVA arrays are displayed after you run discovery (**Options** > **Discovery**), you must run a Discovery Data Collection for the collectors to run properly.

As part of the license setup, a license page similar to the following displays the used and maximum numbers of managed arrays.

If your license includes the Array Performance Pack capability, the current usage summary will report how many arrays can have this capability applied.



Licensed Capacities	Used Licenses	Maximum Licensed
MAPs	147	1,149
Back Up Size	0 GB	3,047 GB
Raw NAS Capacity	0.00 TB	1,005.00 TB
Managed Exchange Instances	0	1,002
Managed Database Instances	0	999
Managed Oracle Instances	0	
Managed SQL Server Instances	0	
Managed Sybase Instances	0	
Managed Caché Instances	0	
Managed File Server Storage	0.00 TB	1,005.00 TB
Performance Pack Array-Instances *	2	13

Figure 11 Current Usage Summary Display

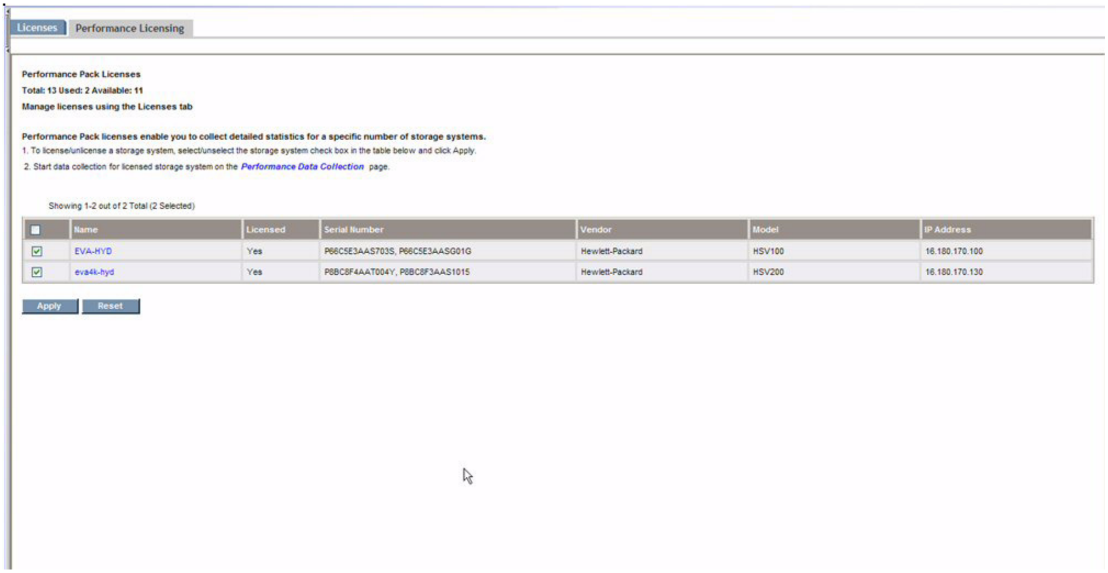
After installing the license(s), you must do the following:

1. Select the **Performance** tab in License Manager, then specify which HP EVA systems you want to have the Array Perfromance Pack capability
2. Select **Confirmation** > **Performance** > **Data Collection**, then start the data collectors for the licensed systems. This is necessary so that reporting data is obtained for the parameters specified. For additional information, please refer t the chapter, *VIewing Performance Data*, in the user guide.

NOTE: You must discover your EVA arrays for the Array Performance Pack to work.

Begin by selecting the **Configuration** tab on the home page. The Data Collection Screen displays.

Select **Enhanced Performance Collection Enabling** to select the EVA arrays you want to include for enhanced performance data collection and reporting.



Performance Pack Licenses
Total: 13 Used: 2 Available: 11
Manage licenses using the Licenses tab

Performance Pack licenses enable you to collect detailed statistics for a specific number of storage systems.
1. To license/unlicense a storage system, select/unselect the storage system check box in the table below and click Apply.
2. Start data collection for licensed storage system on the *Performance Data Collection* page.

Showing 1-2 out of 2 Total (2 Selected)

□	Name	Licensed	Serial Number	Vendor	Model	IP Address
☑	EVA-HYD	Yes	P66C5E3AAS703S, P66C5E3AASG01G	Hewlett-Packard	HSV100	16.180.170.100
☑	eva4k-hyd	Yes	P8BC8F4AAT004Y, P8BC8F3AAS1015	Hewlett-Packard	HSV200	16.180.170.130

Figure 12 EVA Selection Screen

Upgrading License from Standard Edition to Enterprise Edition

You must upgrade your license from Standard Edition to Enterprise Edition to use the following features:

- Provisioning Manager
- Global Reporter
- NetApp Filers
- Managing HP XP Arrays
- Heterogeneous Array Discovery
- Heterogeneous Host Discovery

Perform the license upgrade to Enterpriise Edition as summarized in the following steps. If your Standard Edition software is running a version prior to Build 6.0, you must upgrade it to Build 6.0 or higher before you can upgrade to Enterprise Edition.

Prior to performing the upgrade, refer to the Support Matrix to ensure your system environment will meet the version requirements listed. After the license upgrade, you can discover any additional devices that are now supported by Enterprise Edition, by performing the steps as described in the VIewing Performance Data chapter of the User Guide.

To import and upgrade the license, perform the following steps:

1. Order the Upgrade SKU for the Standard Edition to Enterprise Edition upgrade.

2. Go to the Webware Licensing website to use the HP Password Delivery Service, and redeem the license key for your product order. Webware Licensing will send you a link from which to download a license key.
3. Access the Storage Essentials License Manager in System Insight Manager. Do this by using the **Deploy** > **Storage Essentials** > **License Manager** > **Manage Storage Essentials License Keys** menu choices.
4. Select **Import License File** to download the file.
5. Select **Browse** to see the files on the computer used to access the management server. Then, select the license file you just downloaded.
6. Select **OK** to import the license file. The imported file will upgrade the license; then, you will have the Enterprise Edition features available.

After the upgrade, you can go to the HP Storage Essentials home page to access a brief overview of the features that are now available.

6 Deploying and Managing CIM Extensions

HP Storage Essentials Standard Edition supports a subset of the devices supported by Enterprise Edition. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

Remote CIM Extensions Management

Because every production environment is different, a variety of tools are provided for deploying and managing CIM extensions. The following options are available:

CIM Extensions Management Tool

The CIM Extensions Management Tool works well if you have many remote clients. It allows you to use host lists, and simplifies the task of creating custom host lists. This tool is not integrated into the discovery interface, so you will need to enter the necessary information for each remote host.

For more information, see "The CIM Extensions Management Tool" on page 184.

HP SIM Plug-In

The HP SIM Plug-In is integrated into the HP SIM menus, and uses HP SIM collection to drive deployment. This allows you to leverage the built-in trust relationship, and eliminates the need to specify user names and passwords for many systems that are managed by HP SIM.

For more information, see "The HP SIM Plug-in" on page 188.

Third-Party Tools

If your security environment requires that you customize the CIM extensions, or you have a corporate tool that standardizes the process so that the same procedure is used for every operating system, you may need to use a third-party tool to deploy CIM extensions. Third-party tools are commonly used in large environments that require the use of a request for change (RFC) process.

Command Line Interface

CIM extensions can be remotely managed through the command line interface (CLI). See the CLI guide for information about installing the CLI and using the available commands.

About SSH

Each host being managed must be running a supported SSH daemon. The root or Administrator user must be allowed to log in for most operations. The product ships with OpenSSH for Windows hosts, but we do not have rights to offer an SSH package for other hosts. To deploy CIM extensions on hosts other than Windows, you can choose any SSH package that meets the following criteria and use it with the CIM extension deployment tools:

- Supports SFTP file transfers
- Supports the EXEC channel method of executing remote commands

For UNIX hosts:

The default SSH configuration on some hosts prohibits root login by default. Follow these steps to manually configure SSH to allow root login on UNIX hosts:

1. Use a text editor to open `/etc/ssh/sshd_config`.
2. Change the value of `PermitRootLogin` to `yes`.
3. Restart the SSH daemon.

For Windows hosts:

Keep in mind the following when deploying OpenSSH on a Windows host:

- If you are using a domain, always specify user names so that they include the domain. For example, enter a user name of `<domain1>\<admin>`

  where

  - `domain1` is the domain name
  - `admin` is the username
- If you are not using a domain, do not specify the host name when deploying OpenSSH. For example, enter a user name of `<admin>`

  where

  - `admin` is the user name

If you are running the management server on Windows, you may deploy OpenSSH to Windows hosts using the CIM Extensions Management Tool. See The CIM Extensions Management Tool, page 184.

If you are running the management server on Linux, you must manually install OpenSSH on Windows hosts. To install OpenSSH on a Windows host:

1. Copy the **cp006690.exe** file from the `$JBOSS_DIST/plugin/sedeploy` directory on the management server.
2. Move the **cp006690.exe** file to the Windows host and execute the file to install OpenSSH.

Copying the CIM Extensions to the Management Server

To remotely install the CIM extensions, you must first copy the CIM extensions installation files to the management server.

The following error message is displayed if you attempt to install CIM extensions before they have been copied to the management server:

```
CIM Extensions directory: ..\Extensions is missing or incomplete
```

IMPORTANT: Do not install the CIM extension on the Management Server. A built-in CIM extension is automatically installed on the Management Server during the installation process. If you install a standard CIM extension on the management server, the management server will not operate correctly. You must uninstall the management server software and then re-install.

To copy the CIM extensions installation files onto a Microsoft Windows server:

1. Go to disk 1 of the CIM Extensions CD-ROMs.
2. Double-click **CopyExtensionFiles.exe**.

   NOTE: Do not change the default directory if you are copying the CIM extensions to a Storage Essentials server. You can select any directory if you are copying the CIM extensions to an HP SIM server.

To copy the CIM extensions installation files onto a Linux management server:

1. Log in as root.
2. Mount disk 1 of the CIM Extensions CD-ROMs and change directory to where you mounted it.
3. Run **./CopyExtensionFiles.sh**.

   NOTE: Do not change the default directory if you are copying the CIM extensions to a Storage Essentials server. You can select any directory if you are copying the CIM extensions to an HP SIM server.

Creating Default Logins for Hosts

You can create a default CIM extension login for each type of host on which you intend to install CIM extensions (AIX, HP-UX, Linux, Solaris, Windows). This eliminates the need to use the local OS user/password database for credential verification. The login username and password are known only to the CIM extensions and do not identify real users on the host systems.

To create default logins for hosts:

1. Create a text file named **cxws.default.login** with the following format:

   ```
   -credentials <userid>:<password>
   ```
2. Place the **cxws.default.login** file in the following directory on the management server:

   ```
   %JBOSS4_DIST%\Extensions\[Platform]
   ```
   where `[Platform]` is the host type.

For example, to create a default login for Windows with a user ID of “myname” and a password of “password” you would create the following file:

```
%JBOSS4_DIST%\Extensions\Windows\cxws.default.login
```

The **cxws.default.login** file would contain the following:

```
-credentials myname:password
```

The CIM Extensions Management Tool

CIM extensions can be remotely managed through a graphical user interface called the CIM Extensions Management Tool.

Each host being managed must be running a supported SSH daemon. See ”About SSH” on page 182 for more information.

You must copy the CIM extensions to the management server before you can use the CIM Extensions Management Tool. See ”Copying the CIM Extensions to the Management Server” on page 182 for more information.

The CIM Extensions Management Tool can manage CIM extensions on the following operating systems:

- AIX
- HP-UX
- Linux (i386, IA64, and x86_64)
- Solaris
- Tru64
- Windows

Launching the CIM Extensions Management Tool

To launch the CIM Extensions Management Tool on a Windows management server:

1. Go to the `%MGR_DIST%\Tools\cimeMgmt` directory on the management server.
2. Run `cimeMgmt.cmd`.

To launch the CIM Extensions Management Tool on a Linux management server:

1. Set the DISPLAY environment variable.
2. Enter the following commands:

```
# cd $MGR_DIST/Tools/cimeMgmt
# ./cimeMgmt.sh
```

Adding Remote Hosts

In order to use the CIM Extensions Management Tool, you must create a list of the remote hosts on which you will be deploying and managing CIM extensions. To create a list of remote hosts:

1. In the Hostname box, enter the name of a host.
2. In the Username box, enter the user name used for accessing the host.
3. In the Password box, enter the password used for accessing the host.

4. Click **Add** to add the host to the table.
5. Repeat steps 1 through 4 for each additional host you want to add.
6. Click the **Edit** (✎) button if you want to edit the entry for a host.
7. Click the **Delete** (✕) button if you want to delete a host from the list.

Host Lists

Host lists allow you to save your list of hosts with associated username and password information for subsequent import. In the host list file, the host and user names are presented in clear text, while the passwords are encrypted using a "password" that you enter when exporting the list.

NOTE: The "password" is an encryption key. It does not protect or limit access to the file itself.

NOTE: The CIM extension passwords are always encrypted. If you do not specify a password, then a blank is used as the encryption key.

Importing a Host List

To import a host list:

1. Click **Import hosts**.
2. Browse to the location of the host list file (which will be in `.xml` format), and click **Open**.

   The Enter Password dialog box displays.
3. Enter the password that was used when the file was exported, and click **OK**.

   The host list is loaded into the tool.

   NOTE: If the wrong password is entered, the following message is displayed:

   ```
   Unable to decrypt host list with specified password
   ```

Exporting a Host List

To export a host list:

1. Click **Export hosts**.
2. Browse to the desired location, enter a file name (for example, `myhosts.xml`), and click **Save**.

   The Enter Password dialog box displays.
3. Enter and confirm the password, and click **OK**.

Managing CIM Extensions on Remote Hosts

Once you have added all the hosts that you want to manage, you can select any of the actions from the left panel. Any selected action is run against all of the hosts in the table. The following actions are available:

- **Display host operating system** - Attempts to determine the remote operating system.
- **Display Installed CIM Extension Version** - Contacts the remote system and displays the version of the CIM extension currently installed on it.
- **Deploy CIM Extensions** - Installs the CIM extension on the remote system.
- **Deploy OpenSSH (Windows Hosts Only)** - Deploys OpenSSH on the remote Windows system. This action is only available from a Windows management server.
- **Uninstall CIM Extensions** - Uninstalls the CIM extension on the remote system.
- **Upgrade CIM Extensions** - Upgrades the CIM extension on the remote system.
- **Configure CIM Extensions**- Configures the CIM extension on the remote system. You can configure the TCP port to listen on, the IP address to bind to, and custom credentials for the extension to use.

  > **NOTE:** You can configure the IP address with a specific address if there is only one system in the list. If there is more than one system, you can only use “auto detect” mode, which instructs the host to listen on the IP address looked up from the same host name used to connect to the host.

- **Download configuration** - Downloads the configuration files from the CIM extension on the remote system. The files are saved to the following directory on the management server:

  `<Install Directory>\logs\download\<remote host name>` (on Windows)

  `<Install Directory>/logs/download/<remote host name>` (on Linux)
- **Download logs** - Downloads the log files from the CIM extension on the remote system. The files are saved to the following directory on the management server:

  `<Install Directory>\logs\download\<remote host name>` (on Windows)

  `<Install Directory>/logs/download/<remote host name>` (on Linux)
- **Start CIM Extensions** - Starts the CIM extension on the remote system.
- **Stop CIM Extensions** - Stops the CIM extension on the remote system.
- **Get CIM Extensions Status** - Checks the running status (started or stopped) of the CIM extension on the remote system.

Configuring CIM Extensions

Click the **Go** button next to the **Configure CIM Extensions** action to configure CIM extensions on remote hosts.

The **Configure CIM Extensions** dialog box allows you to configure all the hosts on the list with the specified settings. The tool will create a new CIM extension configuration file for each indicated remote host. A backup copy will be saved on each host with its previous configuration.

The choices in this dialog box are all optional. If they are not specified, they will be omitted from the configuration files.

The **Auto-detect IP address** checkbox will cause the tool to use the host name that was entered in the Hostname box to start the CIM extensions.

NOTE: You cannot use the IP Address box when multiple hosts are listed.

The **Start Extensions on Custom Port** checkbox will start the CIM extension on the specified port.

NOTE: If you configure a CIM extension to use a custom port, you must specify the custom port when setting up data collection from the management server for that host.

The **Use Custom Credentials** checkbox configures the CIM extensions to use a user name and password that you specify. This username and password are known only to the CIM extensions and do not identify a real user on the host system.

NOTE: If you configure a CIM extension to use a non-default username and password, you must specify those credentials rather than those for the host's "root" or "administrator" user when setting up data collection from the management server for that host .

Log Files

When you install, remove, or upgrade CIM extensions using the CIM Extensions Management Tool, the log files are saved to the following location:

```
<Install Directory>\logs\cedeploy.<CIME Host Name>.log
```

Status Icons

A status icon for each host is displayed in the column to the right of the host name. The following table lists all the status icons and their meanings:

Table 12 Status Icons

Icon	Status
?	The host has been added to the list, but no action has been selected.
ℹ	The action is waiting to begin or is in progress.
⚠	The last action completed with a warning.
✓	The last action completed successfully.
✖	The last action failed.

The HP SIM Plug-in

CIM extensions can be remotely managed with the use of the HP SIM Plug-in, which integrates the deployment options into the HP SIM menus.

NOTE: The HP SIM Plug-in is only supported on Windows management servers.

Each host being managed must be running a supported SSH daemon. See "About SSH" on page 182 for more information.

You must copy the CIM extensions to the Storage Essentials management server before you can use the HP SIM Plug-in. See "Copying the CIM Extensions to the Management Server" on page 182 for more information.

The HP SIM Plug-in supports deploying or managing CIM extensions on the following operating systems:

- AIX
- HP-UX
- Linux (i386, IA64, and x86_64)
- Tru64
- Solaris
- Windows

Installing the HP SIM Plug-in

To install the HP SIM Plug-in:

1. Verify that HP SIM is running.
2. Ensure that the CIM extension installation files will be accessible to HP SIM:

   Single server installations:

   If you installed Storage Essentials and HP SIM on the same server, when you are asked to select the directory that contains the CIM extensions, browse to the directory that was created while following the instructions in "Copying the CIM Extensions to the Management Server" on page 182.

   Dual server installations:

   If you installed Storage Essentials and HP SIM on separate servers, you must put a copy of the CIM extensions on the server running HP SIM:

   c. Copy the CIM extensions from the directory that was created while following the instructions in "Copying the CIM Extensions to the Management Server" on page 182.

   d. Put the CIM extensions in a directory on the HP SIM server (for example: `<SIM Install Directory>\Extensions`).

   e. During the HP SIM Plug-in installation, when you are asked to select the directory that contains the CIM extensions, point to the directory that you just created.

3. Insert the management server CD-ROM.
4. Double-click the `SEDeploy_SIM_Plugin.exe` file in the `HPtools` directory.
5. Close and restart the HP SIM browser for the new menu options to display.

Using the HP SIM Plug-in

The HP SIM Plug-in adds the following options to the **Deploy > Deploy Drivers, Firmware and Agents** menu in HP SIM:

- Install Storage Essentials Extensions
- Remove Storage Essentials Extensions
- Upgrade Storage Essentials Extensions

Installing the CIM Extension for HP Tru64 UNIX

Follow these additional steps if you are using the HP SIM Plug-in to install the CIM extension for HP Tru64 UNIX using only the HP SIM private key:

1. On the management server, open a command window and `cd` to `C:\Program Files\HP\Systems Insight Manager\config\sshtools`.
2. Run the following command:

   ```
   ssh-keygen -e -f .dtfSshKey.pub > <MANAGEMENT_SERVER_NAME>.pub
   ```

   where `<MANAGEMENT_SERVER_NAME>` is the hostname of the management server.
3. Copy `<MANAGEMENT_SERVER_NAME>.pub` to the `.ssh2` directory of the Tru64 root user's home directory.
4. Login to the Tru64 host as the root user, and run the following command:

   ```
   echo "Key <MANAGEMENT_SERVER_NAME>.pub" >> .ssh2/authorization
   ```

   Password-less deploy will now work correctly.

Log Files

When you install, remove, or upgrade CIM extensions using the HP SIM Plug-in, the log files are saved to the following location:

```
<SIM Install Directory>\plugin\sedeploy\logs\cedeploy.<CIME host IP>.log
```

About Upgrading Your CIM Extensions

You must upgrade your CIM extensions to obtain new functionality such as the following:

- QLogic failover on Linux hosts
- SecurePath support
- PowerPath support on Microsoft Windows
- Backup support - Backup information is not gathered from legacy CIM extensions. For backup information to be gathered by the management server, the CIM extension on the Backup Manager Host must be at the same software build as the management server. When you upgrade your management server, upgrade the CIM extensions on your Backup Manager Host to continue to see backup data.
- Cluster discovery

Keep in mind the following:

- After you upgrade a CIM extension on a Backup Manager Host, you must run HP SIM Discovery, and then Discovery Data Collection. The order of these steps is important. If you do Discovery Data Collection first, and then HP SIM Discovery, Backup Manager data becomes corrupted.
- The HP SIM Discovery and Discovery Data Collection is required for Backup Collections to work.

1. Upgrade the CIM extension as described in the *Installation Guide*.
2. Run HP SIM Discovery. See "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" on page 105 for more information.
3. Run Discovery Data Collection.See "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" on page 105 for more information.

IMPORTANT: After an upgrade, you need to specify again which hosts are Backup Manager Hosts by selecting **Include backup details** before you Discovery Data Collection.

7 Installing the CIM Extension for IBM AIX

HP Storage Essentials Standard Edition does not support IBM AIX hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 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.

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 HBA API.

For more information about the HBA API, 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 runtime 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 "Rolling Over the Log Files" on page 198.

IMPORTANT: The AIX CIM extension does not install on pSeries servers running the IBM Hardware Management Console.

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

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 388.

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. The hbatest program, which is accessible from the CIM Extension CD-ROM, lists the name and number for all HBAs 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.

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbatest:

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

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

IBM Adapters FCXXXX 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 the AIX System Management Interface Tool (SMIT). If you are unfamiliar with SMIT, refer to the documentation that accompanies the AIX host.

To upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.2 and later of the CIM extension are compatible with this build of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in "About Upgrading Your CIM Extensions" on page 189.

To install the CIM Extension for AIX:

IMPORTANT: You must install the CIM extension for IBM AIX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

1. Insert the CIM Extension 1 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 (**Esc+4**) and select the following:

   ```
   APPQcime
   ```

9. Press **Enter** to install.
10. If you see error messages when you install the CIM extension for AIX, see "Rolling Over the Log Files" on page 198.
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 194.
    - Start the CIM extension. See "Starting the CIM Extension Manually" on page 195.
    - *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 "Rolling Over the Log Files" on page 198.

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, enter 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 389.
- If you see the message “Fork Function Failed” 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 416.

When you enter the start command, the following message is displayed:

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

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 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

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where `1234` is the new port for the CIM extension
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings** and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

   NOTE: If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 196.

Additional Parameters

The following table describes the parameters that can be specified in the `cim.extension.parameters` file:

Table 13 Parameters for CIM Extensions

Parameter	**Description**
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 195.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 196.
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

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. Enter the following at the command prompt:

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

   The version number of the CIM extension and the date it was built are displayed, 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
   ```

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 Log Files

The logging information for the CIM extension is contained primarily in the cxws.log file, created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the cxws.out file and rolls it over.

Fulfilling the Prerequisites

If your installation fails, you may be missing the following prerequisites. Refer to the information in this section 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, such as switches, are not displayed. 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 HBA API. 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. In the **Refine Your Search Section,** select **Tools/Utilities** from the **Limit by Type** menu.
2. Select **AIX** from the **Limit by Platform or Operating System** menu.
3. Select **5.0** from the **Limit by Version** menu.
4. In the Limit by Adding Search Terms box, enter 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.

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 described in "Stopping the CIM Extension" on page 198.
2. Enter 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 Esc+4 and select:

   ```
   APPQcime
   ```

7. On the same page you selected `APPQcime`, select **No** for Preview by pressing the **Tab** key.
8. Press **Enter** to remove the software.

8 Installing the CIM Extension for SGI ProPack for Linux

HP Storage Essentials Standard Edition does not support SGI ProPack for Linux hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM Extension directly on the host. You can also install and manage CIM Extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 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 HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The CIM Extension authenticates using PAM (Pluggable Authentication Module) and supports the following password encryption mechanisms:

- Blowfish
- DES
- MD5

NOTE: All ProPacks require that pam-devel rpm is installed.

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 388.

Verifying SNIA HBA API Support

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

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

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

   If the host is SGI ProPack3, enter the following at the command prompt:

   ```
   ./hbatest_PP3.
   ```

   If the host is SGI ProPack 4 or later, enter the following at the command prompt:

   ```
   ./hbatest
   ```

On SGI ProPack 3, the SGI-branded HBA API library for QLogic and LSI HBAs is built into the operating system kernel.

On SGI ProPack 4 and later, contact your vendor for the vendor-specific HBA API library for LSI HBA. Discovery of ProPack4 hosts with QLogic HBA is not supported.

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 upgrade the CIM Extension, first remove the previous version before installing the latest version. Builds 4.2 and later of the CIM Extension are compatible with this build of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in "About Upgrading Your CIM Extensions" on page 189.

To install a CIM Extension on SGI ProPack for Linux:

1. Go to the `/Altix` directory on the CIM Extensions 2 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 enter `-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, and 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.

IMPORTANT: You must install the CIM extension for SGI ProPack for Linux to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

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 Manually" on page 204.

   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 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 389.

To start the CIM extension, enter 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, enter the following at the command prompt:

   ```
   # ./start
   ```

The following is displayed:

```
./start
```

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

A similar message is now displayed in the `cxws.out` file when the CIM extension has completed startup.

```
STATUS | wrapper  | 2006/07/10 15:44:26 | --> Wrapper Started as Daemon
STATUS | wrapper  | 2006/07/10 15:44:26 | Launching a JVM...
INFO   | jvm 1    | 2006/07/10 15:44:27 | Wrapper (Version 3.1.2)
http://wrapper.tanukisoftware.org
INFO   | jvm 1    | 2006/07/10 15:44:27 |
INFO   | jvm 1    | 2006/07/10 15:45:55 |
INFO   | jvm 1    | 2006/07/10 15:45:55 | Mon Jul 10 15:45:55 EDT 2006
INFO   | jvm 1    | 2006/07/10 15:45:55 | CXWS 5.1.0.169 on
/16.118.238.196:4673 now accepting connections
```

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
```

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 CIM extension is running when a message resembling the following is displayed:

```
CIM Extension Running
```

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where `1234` is the new port for the CIM extension.
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings**, and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

   NOTE: If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 206.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 14 Parameters for CIM Extensions

Parameter	**Description**
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 206.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 206.
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

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 Log Files

The logging information for the CIM extension is contained primarily in the cxws.log file, created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from SGI ProPack for Linux

To remove the CIM extension for SGI ProPack for Linux:

1. Change 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_APPQcime_CIM_Extensions
   ```

9 Installing the CIM Extension for HP-UX

HP Storage Essentials Standard Edition does not support HP-UX hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 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 HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

Refer to the HP tab of the support matrix for the prerequisites. If the installation fails, see "Fulfilling the Prerequisites" on page 216.

FC SNIA HBA API software is bundled with the driver and is installed at the same time the driver is installed.

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 388.

Verifying SNIA HBA API Support

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

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbatest:

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

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

HP SNIA adapters AXXXXA come from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during the installation of 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 opposed 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 following the instructions in this section, and then performing 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 upgrade the CIM extension, first remove the previous version before installing the latest version. Builds 4.2 and later of the CIM extension are compatible with this build of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in "About Upgrading Your CIM Extensions" on page 189.
- You must install the CIM extension for HP-UX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Login as root.
2. Insert the CIM Extension 1 CD-ROM into the CD-ROM drive on the HP-UX server.
3. Create the `/cdrom` directory on the 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 the c, t, and d numbers correspond to CD-ROM device numbers.

   To find out `c#t#d#` for your CD-ROM, run the `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 the following message is displayed: `analysis and execution succeeded`
6. Eject/unload the CD-ROM by unmounting the CD-ROM with the following command and pressing eject 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. Enter 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 389.

To start the CIM extension, enter 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...
```

Keep in mind the following:

- 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. Access information about these topics by typing the following:

  ```
  ./start -help
  ```

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 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.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Restricting the Users Who Can Discover the Host

The `-users` parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the `-users` parameter.

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 fewer privileges, for example jsmythe. First, you would add the user to the parameters file. You would then log on to the management server, access the Discovery page, and 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.

Follow these steps to add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -users myname
   ```

   where myname is a valid HP-UX user name.

   NOTE: You can enter multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

   NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already is use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where 1234 is the new port for the CIM extension
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

   NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings,** and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

> **NOTE:** If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

> **NOTE:** The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 213.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 15 Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 213.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 213.

Table 15 Parameters for CIM Extensions (continued)

Parameter	Description
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	Restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

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

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

   The version number of the CIM extension and the date it was built are displayed, 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 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

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 Log Files

The logging information for the CIM extension is contained primarily in the cxws.log file, created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the cxws.out file and rolls it over.

Fulfilling the Prerequisites

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

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

```
# fcmsutil /dev/td1
```

The 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 216.
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
   ```

10 Installing the CIM Extension for SGI IRIX

HP Storage Essentials Standard Edition does not support SGI IRIX hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 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 HBA API. For more information about the HBA API, see the following Web page at the SNIA Web Site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The installation requires the SGI Origin system, and 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 388.

Verifying SNIA HBA API Support

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

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

1. Go to the `Irix/tools` directory on the CIM Extension CD-ROM2.
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 in 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

IMPORTANT: To upgrade the CIM extension, first remove the previous version before installing the latest version. Builds 4.2 and later of the CIM extension are compatible with this build of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in "About Upgrading Your CIM Extensions" on page 189.

To install the CIM extension for IRIX:

1. Insert the CIM Extension 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.

   > **IMPORTANT:** You must install the CIM extension for SGI IRIX to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

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 Manually" on page 221.

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 389.

To start the CIM extension, enter the following in the `/opt/APPQcime/tools` directory:

```
# ./start
```

The following is displayed:

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

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 CIM extension is running when a message resembling the following is displayed:

```
CIM Extension Running
```

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:
   ```
   -port 1234
   ```
   where `1234` is the new port for the CIM extension.
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See ”Discovering Applications, Backup Hosts and Hosts” on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings**, and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:
   ```
   -on 127.0.0.1,192.168.0.1
   ```

NOTE: If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 222.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 16 Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 222.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 222.
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.

Table 16 Parameters for CIM Extensions (continued)

Parameter	Description
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

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 appcime 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. Enter the following at the command prompt:

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

   The version number of the CIM extension and the date it was built are displayed, 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

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

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, created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the cxws.out file and rolls it over.

Removing the CIM Extension from SGI IRIX

To remove the CIM extension for SGI IRIX:

1. Stop the CIM extension as described in "Stopping the CIM Extension" on page 225.
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
```

11 Installing the CIM Extension for SUSE and Red Hat Linux

IMPORTANT: Do not install the CIM extension onto the management server.

This chapter contains the following topics:

Keep in mind the following:

- This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.
- Make sure you have reviewed Table 2 on page 2 to ensure you are at the correct step.
- The 6.0 management server requires that any managed Tru64 or OpenVMS hosts be running at least version 5.1.0 SP4 (5.1.4) of the CIM Extensions. If the Tru64 and OpenVMS CIM Extensions are not at the minimum levels, the 6.0.0 management server will be unable to gather information from those hosts, and there will be various replication errors in the management server logs. It is preferable to upgrade all CIM Extensions to the same version as the management server, as some functionality may be unavailable when earlier CIM Extensions are used.

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 HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site:

http://www.snia.org/tech_activities/hba_api/

Prerequisites

During the installation, a “requires” rpm is run first to check for dependencies. You will be notified if you are missing any required packages.

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 388.

Verifying SNIA HBA API Support

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

To run hbatest:

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

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

Driver Information for Verifying Emulex SNIA Adapters

The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and the HBATool can detect the Emulex host bus adapter.

After you install the HBAnywhere software, you can find the location of the libraries as follows in the `/etc/hba.conf` file.

For the 64-bit hosts running the Linux operating system, following is displayed in hba.conf file:

To view the hba.conf file, enter the following:

```
# cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

```
com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
```

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

For 32-bit hosts running the Linux operating system, the following is displayed in hba.conf file:

To view the hba.conf file, enter the following:

```
cat /etc/hba.conf
```

The library name is listed first and then the path, as shown in the following example:

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

Driver Information for Verifying QLogic SNIA Adapters

QLogic SNIA adapters come from a separate package, qlapi-vX.XXX-rel.tgz, found in the QLogic driver. The adapters are installed separately after the 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/libqlsdm.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 opposed 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 following the instructions in this section, and then performing 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 upgrade the CIM extension, first remove the previous version before installing the latest version. Builds 4.2 and later of the CIM extension are compatible with this build of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in ″About Upgrading Your CIM Extensions″ on page 189.
- The installation is a two-step process where a “requires” rpm is run first to check for dependencies, and then the full rpm is installed.
- You must install the CIM extension for SUSE and Red Hat Linux to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Login as root.

2. Go to the `Linux/requires_rpm` directory on the CIM ExtensionCD1 CD-ROM by entering the following at the command prompt:

   ```
   # cd /cdrom/linux/requires_rpm
   ```

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

3. Use the appropriate "requires" rpm from the list below for the version of the OS you are installing.

   NOTE: The version and release number of the "requires" rpm will change based on the version and release.

   Redhat EL/AS 3

   - 32 bit on x86:
     `RHEL3/APPQcime-Requires-<Version> <Release>.i386.rpm`
   - 32 bit / 64 bit on x86_64:
     `RHEL3/APPQcime-Requires-<Version>-<Release>.x86_64.rpm`

   Redhat EL/AS 4

   - 32 bit on x86:
     `RHEL4/APPQcime-Requires-<Version>-<Release>.i386.rpm`
   - 2 bit / 64 bit on x86_64:
     `RHEL4/APPQcime-Requires-<Version>-<Release>.x86_64.rpm`
   - IA64:
     `RHEL4/APPQcime-Requires-<Version>-<Release>.ia64.rpm`

   Redhat EL/AS 5

   - 32 bit on x86:
     `RHEL5/APPQcime-Requires-<Version>-<Release>.i386.rpm`
   - 32 bit / 64 bit on x86_64:
     `RHEL5/APPQcime-Requires-<Version>-<Release>.x86_64.rpm`
   - IA64:
     `RHEL5/APPQcime-Requires-<Version>-<Release>.ia64.rpm`

   SLES 9

   - 32 bit on x86:
     `SLES9/APPQcime-Requires-<Version>-<Release>.i386.rpm`
   - 32 bit on x86_64:
     `SLES9/APPQcime-Requires-<Version>-<Release>.x86_64.rpm`
   - IA64:
     `SLES9/APPQcime-Requires-<Version>-<Release>.ia64.rpm`

   SLES 10

   - 2 bit on x86:
     `SLES10/APPQcime-Requires-<Version>-<Release>.i386.rpm`
   - 32 bit on x86_64:
     `SLES10/APPQcime-Requires-<Version>-<Release>.x86_64.rpm`

- IA64:
  `SLES10/APPQcime-Requires-<Version>-<Release>.ia64.rpm`

After running this “requires” rpm you will get one or more dependency errors. A dependency on the rpm package APPQcime is expected. For example:

```
APPQcime is needed by APPQcime-Requires-6.0.0-224.i386.rpm
```

If you get an additional dependency error, you must install the required packages before continuing.

4. After running the "requires” rpm and getting just the one expected dependency error, enter one of the following commands:

   For 64-bit Linux Itanium servers:

   ```
   # rpm -idvh APPQcime--<Version>-<Release>-ia64.rpm
   ```

   For all other servers:

   ```
   # rpm -idvh APPQcime--<Version>-<Release>-i386.rpm
   ```

   The following output is displayed:

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

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

5. *Optional*: Rerun the “requires” rpm from step 3. You should no longer receive any errors.

Example of steps 3 - 5:

3. `rpm –idvh RHEL3/APPQcime-Requires-6.0.0-224.i386.rpm`

```
Error:  Failed dependencies:
APPQcime is needed by APPQcime-Requires-6.0.0-224.i386.rpm
```

This error is the expected result, but if there were more errors, they would need to be addressed.

If you only received one error (as in this example), it means the other dependant libraries are all installed, so the full APPQcime package should now be installed.

4. `rpm –idvh APPQcime-6.0.0-224-i386.rpm`

(Install APPQcime package)

5. `rpm –idvh RHEL3/APPQcime-Requires-6.0.0-224.i386.rpm`

(No failed dependencies, so no messages appear.)

Optionally, verify packages were installed:

```
rpm –qa | grep APPQcime-Requires
rpm –qa | grep APPQcime
```

To uninstall packages, uninstall the "requires" rpm first. For example:

```
rpm –e APPQcime-Requires-6.0.0-224
rpm –e APPQcime
```

(Verified packages were uninstalled. No error messages appear.)

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 389.

To start the CIM extension, enter 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...
```

Note that when you start the CIM extension, you can change the port number the CIM extension uses. See "Configuring CIM Extensions" on page 232 for more information.

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 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.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named `cim.extension.parameters` and is located in the `[Installation_Directory]/conf` directory on the host. This directory also contains a file named `cim.extension.parameters-sample`. This file contains samples of available parameters and can be copied into the `cim.extension.parameters` file and used as a template.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.

2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where `1234` is the new port for the CIM extension
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings,** and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

NOTE: If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 233.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 17 Parameters for CIM Extensions

Parameter	**Description**
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 232.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 233.
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to the `/opt/APPQcime/tools` directory.
2. Enter 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
```

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 Log Files

The logging information for the CIM extension is contained primarily in the cxws.log file, created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the cxws.out file and rolls it over.

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 235.
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.

12 Installing the CIM Extension for NonStop

This chapter describes the following:

About the CIM Extension for NonStop

The CIM extension for NonStop 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 that 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 supports communication only 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 requirements described in the next two sections:

NOTE: If the installation fails, see "Fulfilling the Prerequisites" on page 245.

NonStop G06.27 or later Software Requirements

- Ensure that the OSS subsystem is running on the NonStop host.
- Enter the `osh` command from the TACL prompt to access the OSS environment.
- Ensure that the process `$ZPMON` is running.

- Ensure that adequate swap space is available.

Network Port

By default, the CIM extension uses port 4673 to communicate with the management server.

To ensure that your network port is working properly:

- Verify that the network port is open. Refer to the documentation accompanying your NonStop 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 388.

Installing the CIM Extension

Use the following procedure to install the CIM extension for NonStop:

1. Navigate to the default directory.
2. Transfer the depots and install scripts to the host using FTP. NonStop hosts do not support CD drives.
3. Place the CIM extension CD-ROM into the CD-ROM drive on any local host. Select one of the following options:
   - **UNIX/Linux host:** Enter the following command at the command prompt to go to the NonStop directory:

     ```
     # cd /cdrom/nsk/NSR
     ```

   - **Windows:** Browse to your compact disk drive. Enter the following command:

     ```
     C:\>D:
     ```

     where D: is the drive where your compact disc resides.

     You can also get this information using Windows Explorer.
4. Navigate to the NSR folder of the CIM extension CD-ROM by entering the following command:

   ```
   D:\>cd/nsk/NSR
   ```

5. Enter the following command to FTP the NonStop depots and install scripts to the NonStop host:

   ```
   ftp <NonStop host name>
   ```

6. Enter the superuser's username and password when you are prompted. For example:

   ```
   User (XXX.YYY.hp.com:(none)): super.super
   331 Password required for SUPER.SUPER.
   Password: XXXXXXXX
   230 User SUPER.SUPER logged in.
   ```

7. Enter the OSS subsystem at the command prompt:

   ```
   ftp> quote oss
   257 OSS API enabled.
   ```

8. Enter the binary mode of the file transfer by entering the following at the command prompt:

   ```
   ftp > bin
   200 Type set to I.
   ```

9. Create a directory on the NonStop host to store the depots and scripts, and transfer the files to that directory by entering the following commands:

```
ftp> mkdir /tmp/NonStopdepots
ftp> cd /tmp/NonStopdepots
ftp> put APPQCIMENSR.pax
ftp> put APPQJAVANSR.pax
ftp> put nsk_local_install.sh
ftp> put nsk_local_uninstall.sh
```

NOTE: Ensure that the directory on the NonStop host is part of the OSS layer. Do not transfer the depots to a Guardian volume or subvolume. For example, do not transfer the depots to a directory or subdirectory of `/G` directory when accessed from OSS. The Guardian layer imposes a filename length limit of eight characters.

10. Log in to the NonStop host (where you have transferred the depot files), as superuser. Select one of the following options:
    - If OSS is enabled during Telnet, choose that option.
    - Enter the `osh` command from the TACL prompt to access the OSS subsystem.
11. Go to the directory where you have transferred the depot files by running:

    ```
    /home/super: cd /tmp/NonStopdepots
    ```
12. Enter the following at the command prompt to install the JRE on NonStop:

    ```
    /tmp/NonStopdepots:./nsk_local_install.sh APPQJAVA
    ```

    When the installation is complete, the following message appears:

    ```
    Installation of APPQJAVANSR was successful. Package is installed under
    /opt/APPQcime directory. Install log can be found at /tmp/
    nsk_local_install.log
    ```

    IMPORTANT: You must install the CIM extension for NonStop to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.
13. Enter the following at the command prompt to install the APPQCIME agent:

    ```
    /tmp/NonStopdepots:./nsk_local_install.sh APPQCIME
    ```

    When the installation is complete, the following message appears:

    ```
    Installation of APPQCIMENSR was successful
    Package is installed under /opt/APPQcime directory
    Starting HP NSK CIM Extensions on current node
    Install log can be found at /tmp/nsk_local_install.log
    ```

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program lists the name and number for all HBAs 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.

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbatest:

1. Verify that you have installed the CIM extension.
2. Go to the `/opt/APPQcime/tools/hbatest` directory on the host where you installed the CIM extension.
3. Enter the following at the command prompt:

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

Starting the CIM Extension Manually

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

Keep in mind the following:

1. You must have superuser 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 superuser has enough privileges to provide the information the management server needs.
2. To configure UNIX CIM extensions to run behind a firewall, see "Configuring UNIX CIM Extensions to Run Behind Firewalls" on page 389.

To start the CIM extension, enter `./start` in the `/opt/APPQcime/tools` directory.

NOTE: Ensure that you have installed the CIM extension in the `/opt` directory.

The following message is displayed:

```
Starting CIM extension for NonStop..........
```

The CIM extension is ready to be contacted by the management server when a message similar to the following example appears:

```
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5:4673 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
- `4673` is the port used by the CIM extension

Keep in mind the following:

- Depending on your terminal type and processor speed, the message `CXWS x.x.x.x on /192.168.1.5:4673 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 are allowed to 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 entering:

  ```
  /start -help
  ```

Restricting the Users Who Can Discover the Host

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

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

The variable `myname` is a valid NonStop username that must be used to discover this NonStop host. For example, assume you want to use the management server to discover a NonStop host, but you do not want to provide the password to the superuser account. You can provide the password to another valid NonStop user account that has fewer privileges, for example `jsmythe`. You would log in to the NonStop host as superuser and start the CIM extension by using the following command:

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

The variable `jsmythe` is a valid NonStop username.

Log in to the management server, access the Discovery page (**Discovery > Setup**), and click **Add Address**. In the Add Address for Discovery page, provide the username and password for `jsmythe`. Only the username and password for `jsmythe` can be used to discover the NonStop 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 NonStop host (**Discovery > Setup**) on the management server. Other usernames 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, enter the `./start -port port_number` command to change the port that the CIM extension will access.

IMPORTANT: The steps in this section provide information about temporarily changing the port of the CIM extension. If you want to make the change permanent, see ”Permanently Changing the Port a CIM Extension Uses (UNIX Only)” on page 388.

To change the port, enter the following:

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

The variable `1234` is the port the CIM extension will listen on for all available network cards

The management server assumes the CIM extension is running on port `4673`. The management server also listens on port `17000` for CIM extensions from build 4.0.

If you change the port number, you must make the management server aware of the new port number in the Add Address for Discovery page (**Discovery > Setup > Add Address**). In the IP Address/DNS Name box, 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
```

The designation `192.168.1.2` is the IP address of the host and `1234` is the new port number.

If you have already added the host to the discovery list (**Discovery > Setup**) on the management server, you must remove it and then add it again. 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 NonStop server.

Specifying the CIM Extension to Listen on a Specific Network Card

You can specify the CIM extension to listen 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 `192.168.2.2.`

Specifying a NIC requires some changes to the NonStop host configuration also.

All NonStop nodes can be configured to have multiple IPs. Each IP has its corresponding TCP/IP process. This means that any TCP/IP operation for a particular IP is handled by its corresponding TCP/IP process. To start the agent with a particular IP, ensure that the corresponding TCP/IP process is set to default. Otherwise, the agent fails to start, and the following message is displayed:

```
Can't assign requested address: Unable to accept connections on specifiedIP
port portNo
```

The following table lists the commands that are used to display and set the default TCP/IP process.

Table 18 TCP/IP Process Display Commands

Command or Argument	Definitions and Output Examples
`info_define all`	Displays the default TCP/IP process
`scf info subnet $*.*`	Uses GTACL commands to check and set the TCP/IP process for the IP address.
`alter define`	Displays multiple IP addresses on a host, along with their TCP/IP processes. alter define= `TCPIP^PROCESS^NAME,FILE $ZTC4` **NOTE:** `ZTC4` is the TCP/IP process of an IP.

The following table lists port arguments.

Table 19 Port Arguments

Argument	Definition and Output Examples
`-on`	Can specify a port specification. For example: `./start -on 192.168.2.2:3456` Instead of listening on the default port, the CIM extension listens on IP address `192.168.2.2` and the indicated port `3456` of the designated NIC.
`-port`	Can be used in conjunction with the `-on` command option. Any `-on` arguments that do not specify a port number use the `-port` argument as the port number. For example: `./start -on 192.168.1.1 -port 1170` The CIM extension listens on Port `1170` of the designated NIC with the IP address of `192.168.1.1`.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

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

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

The CIM extension and build date are displayed, as shown in the following example:

```
CXWS for mof/cxws/cxws-nsk.mof
CXWS version x.x.x.x, built on Mon 19-March-xxxx 17:28:30 by Administrator
```

where `X.X.X.X` represents the version of the CIM extension and the letters `XXXX` represent the year of the build.

Combining Start Commands

You can also combine the `-users` and `-port` commands. Select from one of the following options:

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

where `myname` is the username that must be used to discover this Tru64 UNIX host. The new port number is `1234.`

Finding the Status of the CIM Extension

You can check the status of the CIM extension by entering `./status` in the `/opt/APPQcime/tools` directory.

The CIM extension is running when the following message appears:

```
CIM extension Running: Process ID: 93
```

Stopping the CIM Extension

To stop the CIM extension, enter the`./stop` at the command prompt in the `/opt/APPQcime/tools` directory.

Keep in mind the following:

- You must have superuser 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 when the files become larger than the configured size, for example 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.

The maximum size and the number of old logs that can be stored are configured in the `log4j.appender.File.MaxFileSize` and `log4j.appender.File.MaxBackupIndex` properties in the `/opt/APPQcime/conf/cxlog4j.properties` file.

The `cxws.out` file contains logging information, such as starting the CIM extension, 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.

The cxws_native.log contains logging information for NonStop system calls. The configuration information for cxws_native.log is maintained in /opt/APPQcime/conf/cxws_native.cfg. When the log file size exceeds the LOG_SIZE specified in the configuration file, the cxws_native.log file rolls over. The information in cxws_native.log is moved to cxws_native.log.old. If cxws_native.log.old already exists, it is deleted.

Increasing the native logging level

The cxws_native.log contains logging information for NonStop system calls. The configuration information for cxws_native.log is maintained in /opt/APPQcime/conf/cxws_native.cfg. Detailed logging information can be obtained by increasing the log level. To increase the log level, set LOG_LEVEL to 3 in cxws_native.cfg and restart the CIM extension.

Fulfilling the Prerequisites

Use the commands mentioned in this section to determine if you have the required software. To test whether OSS environment is running, enter the following command from the TACL prompt:

```
$SYSTEM SYSTEM 1> osh
```

The prompt switches to a UNIX style. For example:

```
/home/super:
```

Removing the CIM Extension from NonStop

To remove the CIM extension:

1. Log in as superuser.
2. Go to the /opt/APPQcime/scripts directory.
3. Execute the script nsk_local_uninstall.sh APPQCIME to remove the CIM extension.

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

   ```
   Uninstallation of package APPQCIME was successful.
   Uninstall log can be found at tmp/nsk_local_uninstall.log
   ```
4. Execute the script nsk_local_uninstall.sh APPQJAVA to remove the NonStop JAVA packaged with the extension.

   When you see the following message, NonStop JAVA has been removed:

   ```
   Uninstallation of package APPQJAVA was successful.
   Uninstall log can be found at tmp/nsk_local_uninstall.log
   ```
5. Go to the /opt directory and enter the following at the command prompt to remove the APPQcime directory:

   ```
   # rm -r APPQcime
   ```

Handling Daylight Savings Time Changes for the NonStop CIM Extension

The NonStop JDK packaged together with the NonStop CIM extension for S series does not contain daylight savings time (DST) changes. In order to obtain the DST changes, you must install conversion tool TZUPdater 1.1 which can be downloaded from www.hp.com/go/javaDSTtool.

This tool allows installed HP NonStop servers for Java (NSJ) JDK/JRE images to be updated with time zone data. TZupdater 1.1 accommodates the U.S. 2007 DST changes originating with the U.S. Energy Policy Act of 2005. This tool also incorporates changes to the 2007-2008 New Zealand's DST, which starts at 2:00 A.M. on September 30, 2007, and ends at 3:00 A.M. on April 6, 2008.

To execute TZupdater1.1:

1. Download and unzip `TZupdater-1.1-2007f.zip` from www.hp.com/go/javaDSTtool onto a local windows host.
2. FTP the `tzupdater.jar` from the unzipped folder to the NonStop host where the CIM extension is installed.
3. Use the binary mode of file transfer and FTP to the OSS subsystem.
4. Place `tzupdater.jar` in the `/opt/APPQcime/modjava` directory. The following is an example of this procedure:

   ```
   ftp>quote oss
   OSS API enabled.
   ftp> bin
   Type set to I.
   ftp> cd /opt/APPQcime/modjava
   ftp> put tzupdater.jar
   ```

5. Stop the CIM extension by entering:

   ```
   ../tools/stop
   ```

6. Point `JAVA_HOME` and `JREHOME` variables to the instance of the NSJ JDK to be operated upon.

   ```
   export JAVA_HOME=/opt/APPQcime/Java
   export JREHOME=$JAVA_HOME/jre.
   ```

7. Run `tzupdater` by entering:

   ```
   ./java -jar tzupdater.jar -u -v
   ```

   The following output is displayed:

   ```
   /opt/APPQcime/modjava: ./java -jar ../tzupdater.jar -u -v
   java.home: /opt/APPQcime/java/jre
   java.vendor: Hewlett-Packard Company
   java.version: 1.4.2_04
   JRE time zone data version: tzdata2003a
   Embedded time zone data version: tzdata2007f
   Extracting files... done.
   Renaming directories... done.
   Validating the new time zone data... done.
   Time zone data update is complete.
   ```

8. Restart the NonStop CIM extension:

```
../tools/start
```

13 Installing the CIM Extension for OpenVMS

HP Storage Essentials Standard Edition does not support OpenVMS hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM extension directly on the host.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 to ensure you are at the correct step.

About the CIM Extension for OpenVMS

The CIM extension for OpenVMS is compatible with OpenVMS for Alpha. The CIM extension for OpenVMS 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 HBA API. For more information about the HBA API, see the following Web page on the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

Prerequisites

The prerequisites are as follows:

Supported OpenVMS (Alpha) versions and required ECOs

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

```
$ PRODUCT SHOW PRODUCT/FULL
```

- **OpenVMS Alpha 7.3-2**

  The following patches must be installed in the order specified:
  - DEC-AXPVMS-VMS732_PCSI-V0300 or later
  - DEC-AXPVMS-VMS732_UPDATE-V0600 or later
  - DEC-AXPVMS-VMS732_SYS-V1000 or later
  - DEC-AXPVMS-VMS732_FIBRE_SCSI-V0900 or later
- **OpenVMS Alpha 8.2**
  - DEC-AXPVMS-VMS82A_PCSI-V0100 or later
  - DEC-AXPVMS-VMS82A_UPDATE-V0300 or later
  - DEC-AXPVMS-VMS82A_SYS-V0400 or later
  - DEC-AXPVMS-VMS82A_FIBRE_SCSI-V0200 or later
- **OpenVMS Alpha 8.3** - The OpenVMS Alpha 8.3 comes with the required ECOs and patches.

Supported OpenVMS Itanium versions and required ECOs

- **OpenVMS IA64 8.2-1**
  - HP-I64VMS-VMS821I_PCSI-V0100 or later
  - HP-I64VMS-VMS821I_UPDATE-V0300 or later
  - HP-I64VMS-VMS821I_SYS-V0200 or later
  - HP-I64VMS-VMS821I_FIBRE_SCSI-V0200 or later
- **OpenVMS IA64 operating systems** - The OpenVMS IA64 operating system comes with the required ECOs and patches.

Required Disk Space

The CIM extension for OpenVMS Alpha host requires 170 MB.

The CIM extension for OpenVMS IA64 host requires 400 MB.

Network Port Must Be Open

By default, the CIM extension uses port 4673 to communicate with the management server. Verify the network port is open. If you need to use a different port, see "Changing the Port Number" on page 254.

Installing the CIM Extension

This section covers the following CIM extension installations for OpenVMS:

- "Installing the CIM Extension on a Standalone Host" on page 251
- "Installing the CIM Extension on a Cluster" on page 252

Installing the CIM Extension on a Standalone Host

Keep in mind the following:

- The CIM extension on OpenVMS needs to be installed locally on each of the required hosts.
- You must be logged in using the "SYSTEM" account on each host to install the CIM extension for OpenVMS.

Follow these steps:

1. Log in as system.
2. Verify that the required ECOs and patches are installed; enter the following at the system prompt:

   ```
   $ PRODUCT SHOW  PRODUT/FULL
   ```

   See "Prerequisites" on page 250 if needed.
3. The management server is only compatible with host bus adapters (HBAs) that support the SNIA HBA API. The SNIA HBA API support for OpenVMS (Alpha) 7.3-2 and 8.2 and OpenVMS IA64 8.2-1 is part o the following FIBRE_SCSI ECO kits:
   - **OpenVMS Alpha 7.3-2** - DEC-AXPVMS-VMS732_FIBRE_SCSI-V0900 or later
   - **OpenVMS Alpha 8.2** - DEC-AXPVMS-VMS82A_FIBRE_SCSI-V0900 or later
   - **OpenVMS IA64 8.2-1** - HP-I64VMS-VMS8211_FIBRE_SCSI-V0200 or later for OpenVMS (IA64) 8.2-1.

   NOTE: The SNIA HBA API library is shipped along with the operating system for OpenVMS Alpha 8.3 and OpenVMS IA64 8.3.

   To verify the HBA supports the SNIA HBA API, check the OpenVMS host for the following files in the path specified:

   ```
   $ DIRECTORY SYS$COMMON:[SYSLIB]HBA_VMS.EXE
   $ DIRECTORY SYS$COMMON:[SYSLIB]HBA.CONF
   ```
4. Verify that the PIPE driver is installed by running the following command:

   ```
   $ MCR SYSMAN IO SHOW DEVICE
   ```

Check for an entry similar to the following:

```
-------------------------------------------------------
SYS$PIPEDRIVER
MPA 814D9F80 814DA000 814DA080
0  814D8F40
--------------------------------------------------------
```

If `SYS$PIPEDRIVER` is not listed, then the PIPE driver is not loaded. Run the following command to load the driver:

```
$ MCR SYSMAN IO CONNECT MPA0:/DRIVER=SYS$PIPEDRIVER/NOADAPTER
```

5. If the CD is already mounted, dismount it by entering:

```
$ DISMOUNT <CD-ROM device name>
```

6. Insert the CIM Extension CD-ROM in the CD-ROM drive.
7. Mount the CIM Extension CD-ROM by entering the following at the command prompt:

```
$ MOUNT /MEDIA=CDROM /UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION
DQB0 (or whichever is the CD-ROM device)
```

8. Change directory to the location of the OpenVMS Extension:

Alpha platforms	`$ SET DEF DQB0:[OVMS.ALPHA]`
Itanium platforms	`$ SET DEF DQB0:[OVMS.IA64]`

1. Run the installation script by entering the following command:

```
$ @OVMSINST
```

2. Verify that the CIM extension process starts properly. You should see the following message:

```
CXWS now accepting connections
```

3. Verify that the APPQCIME process is running by typing:

```
$ @SYS$COMMON:[OPT.APPQCIME.TOOLS]STATUS
```

4. Dismount the CD-ROM by typing:

```
$ DISMOUNT <CD-ROM device name>
```

5. Remove the CD. Press the eject button on the CD-ROM drive to take the CD out of the CD-ROM drive.

NOTE: The CIM extension starts during the local installation.

Installing the CIM Extension on a Cluster

Follow the steps in "Installing the CIM Extension on a Standalone Host" on page 251 to install the CIM extension for OpenVMS on a Cluster system. The CIM extension for OpenVMS must be installed on all nodes of the cluster.

Starting the CIM Extension Manually

The management server can only obtain information from a host when the CIM extension is running on the host. You must be a superuser for the host system in order to start the CIM extension.

The CIM extension provides information within the privileges of the user account that started the CIM extension. Only the system account has enough privileges to provide the information the management server needs.

To manually start the CIM extension:

1. Log in as system on the OpenVMS host on which you want to start the CIM extension.
2. Enter the following command to start the CIM extension.

   ```
   $ @SYS$COMMON:[OPT.APPQCIME.TOOLS]START
   ```

   The following message is displayed:

   ```
   STARTING OpenVMS CIME...
   %RUN-S-PROC_ID, identification of created process is 00002976
   -----------------------------------------------------------

   Sun Oct 28 11:54:26 IST 2007
   CXWS 6.0.0.269 on /127.0.0.1:4673 now accepting connections

   Sun Oct 28 11:54:26 IST 2007
   CXWS 6.0.0.269 on /15.154.53.91:4673 now accepting connections
   ```

How to Determine if the CIM Extension is Running

You can determine if the CIM extension is running by entering the following in the SYS$COMMON:[OPT.APPQCIME.TOOLS] directory.

```
$ @STATUS
```

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

```
CIM Extension is running. Process id :001B0AEE
```

where 001B0AEE is the process ID running the CIM extension.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named CIMEXTENSION.PARAMETERS and is located in the SYS$SPECIFIC:[OPT.APPQCIME.CONF] directory on the host. This directory also contains a file named CIMEXTENSION.PARAMETERS-SAMPLE. The CIMEXTENSION.PARAMETERS-SAMPLE file contains samples of available parameters which can be used as a template to create the CIMEXTENSION.PARAMETERS file.

Restricting the Users Who Can Discover the Host

The -USERS parameter provides increased security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the -USERS parameter.

For example, assume you want to use the management server to discover a OpenVMS host, but you do not want to provide the password to the root account. You can provide the password to another valid OpenVMS user account that has fewer privileges, for example jsmythe. First, you would add the user to the parameters file. You would then log on to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the OpenVMS host.

Follow these steps to add a user to the parameters file:

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:

   ```
   SET DEF SYS$SPECIFIC:[OPT.APPQCIME.CONF]
   ```

2. Open the CIMEXTENSION.PARAMETERS file in a text editor, and enter the following line:

   ```
   -users jsmythe
   ```

   where `jsmythe` is a valid OpenVMS user name.

   NOTE: You can enter multiple users by separating them with a colon, as shown in the following example:

   ```
   -users jsmythe:myname
   ```

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the CIMEXTENSION.PARAMETERS file whenever it is started manually or when the host is rebooted.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already is use, follow these steps to change the port the CIM extension will access:

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:

   ```
   SET DEF SYS$SPECIFIC:[OPT.APPQCIME.CONF]
   ```

2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where 1234 is the new port for the CIM extension
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

Adding a Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Step 1 — Discovering Your Hosts and Backup Manager Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** >

System Protocol Settings, and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to `SYS$SPECIFIC:[OPT.APPQCIME.CONF]` by entering the following command:

   ```
   SET DEFAULT SYS$SPECIFIC:[OPT.APPQCIME.CONF]
   ```

2. Open the `CIMEXTENSION.PARAMETERS` file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

   NOTE: If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

   NOTE: The CIM extension looks for parameters in the `CIMEXTENSION.PARAMETERS` file whenever it is started manually or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a Port Number to Discovery" on page 254.

Additional Parameters

The following table describes additional parameters that can be specified in the `CIMEXTENSION.PARAMETERS` file:

Table 20 Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 254.

Table 20 Parameters for CIM Extensions (continued)

Parameter	Description
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 255.
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority but the user must have the following system and process privileges: CMKRNL, SYSPRV and SYSLCK. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	Restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

1. Go to `SYS$COMMON:[OPT.APPQCIME.tools]` by entering the following command:

   ```
   SET DEF SYS$COMMON:[OPT.APPQCIME.tools]
   ```

2. Enter the following at the command prompt:

   ```
   $ @start -version
   ```

   The version number is displayed.

Combining Start Commands

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

```
SYS$COMMON:[OPT.APPQCIME.TOOLS]START -users myname -port 1234
```

or

```
SYS$COMMON:[OPT.APPQCIME.TOOLS]START -port 1234 -users myname
```

where

- `myname` is the user name that must be used to discover this OpenVMS host
- `1234` is the new port.

Modifying the Boot Time Start Script (Optional)

When you install the CIM extension, its start script is put in the SYS$COMMON:[OPT.APPQCIME.TOOLS] directory with the file name START.COM. Optionally, this script can be used to start the CIM extension at boot time.

The following command must be included as the last line in the START.COM file:

```
$ @ SYS$COMMON:[OPT.APPQCIME.TOOLS]START
```

Parameters you can add when you manually start the CIM extension, such as -port and -users, can be enabled using the above command.

To modify the SYS$STARTUP:SYSTARTUP_VMS.COM file:

1. Open SYS$STARTUP:SYSTARTUP_VMS.COM in a text editor.
2. Find the following line of code:
   ```
   $ EXIT
   ```
3. Add the following line before the line containing $ EXIT
   ```
   $ @ SYS$COMMON:[OPT.APPQCIME.TOOLS]START
   ```
4. Save the file.

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

Stopping the CIM Extension

To stop the CIM extension:

1. Log in to the system as a superuser.
2. Navigate to the following directory:
   ```
   SYS$COMMON:[OPT.APPQCIME.TOOLS]
   ```
   Where SYS$COMMON:[OPT] is the directory in which you installed the CIM extension.
3. Enter: $ @STOP to stop the CIM extension.

NOTE: Once the CIM extension is stopped on the host, the management server will not be able to gather information about this host.

Rolling Over the Log Files

The logging information for the CIM extension is contained primarily in the CXWS_LOG file, created by default in the SYS$COMMON:[OPT.APPQCIME.TOOLS] directory. The CXWS_LOG file rolls over once it becomes more than 30 MB. The information in CXWS_LOG is moved to CXWS_LOG.1. When the logs roll over again, CXWS_LOG.1 is renamed to CXWS_LOG.2 and the information that is in CXWS_LOG is moved to CXWS_LOG.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- CXWS_LOG - contains the latest logging information
- CXWS_LOG.1 - contains logging information that was previously in cxws.log
- CXWS_LOG.2 - contains logging information that was previously in cxws.log.1

- CXWS_LOG.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the CXWS.OUT file and rolls it over.

The CXWS_NATIVE.LOG contains logging information relative to OpenVMS native operations. The configuration information for CXWS_NATIVE.LOG is maintained in SYS$SPECIFIC:[OPT.APPQCIME.CONF], where SYS$SPECIFIC:[OPT] is the directory in which the node-specific files of the CIM extension are present. When the log file size exceeds the LOG_SIZE parameter specified in the configuration file for the CXWS_NATIVE.LOG, the file rolls over. The information in CXWS_NATIVE.LOG is moved to CXWS_NATIVE.LOG.OLD. If CXWS_NATIVE.LOG.OLD already exists, it is deleted.

Increasing the Native Logging Level

The configuration information for CXWS_NATIVE.LOG is maintained in SYS$SPECIFIC:[OPT.APPQCIME.CONFIG]CXWS_NATIVE.CFG. In order to increase the logging level, specify the desired log level in this file.

For example, Set LOG_LEVEL to 3 in CXWS_NATIVE.CFG and restart the CIM extension to increase the log level to 3.

Removing the CIM Extension from OpenVMS

This section includes information on removing the CIM extension. It covers the following topics:

- "Uninstalling the OpenVMS CIM Extension on a Standalone Host" on page 258
- "Uninstalling the OpenVMS CIM Extension on a Cluster Host" on page 259

Uninstalling the OpenVMS CIM Extension on a Standalone Host

To remove the CIM extension for OpenVMS on a standalone host:

1. Log in as system.
2. Enter the following at the command prompt:

```
$ @SYS$COMMON:[OPT.APPQCIME.SCRIPTS]APPIQ_LOCAL_UNINSTALL.COM
```

3. Press **Enter** to proceed with the uninstall, as shown in the example below:

   CIM Extension is Stopped...

   The following product has been selected:

```
HP AXPVMS APPQCIME V6.0                Layered Product
The following product will be removed from destination:
HP AXPVMS APPQCIME V6.0                DISK$VMS_7_3_2:[VMS$COMMON.]
Portion done:
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
The following product has been removed:
 HP AXPVMS APPQCIME V6.0                Layered Product
```

Uninstalling the OpenVMS CIM Extension on a Cluster Host

The OpenVMS CIM extension must be uninstalled from all nodes on the cluster. Follow the steps in ”Uninstalling the OpenVMS CIM Extension on a Standalone Host” on page 258 for each node on the cluster.

14 Installing the CIM Extension for HP Tru64 UNIX

HP Storage Essentials Standard Edition does not support HP Tru64 UNIX hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

Keep in mind the following:

- This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.
- Make sure you have reviewed Table 2 on page 2 to ensure you are at the correct step.
- The 6.0 management server requires that any managed Tru64 or OpenVMS hosts be running at least version 5.1.0 SP4 (5.1.4) of the CIM Extensions. If the Tru64 and OpenVMS CIM Extensions are not at the minimum levels, the 6.0.0 management server will be unable to gather information from those hosts, and there will be various replication errors in the management server logs. It is preferable to upgrade all CIM Extensions to the same version as the management server, as some functionality may be unavailable when earlier CIM Extensions are used.

About the CIM Extension for Tru64 UNIX

The CIM extension for HP Tru64 UNIX 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 HBA API. For more information about the HBA API, see the following Web page at the SNIA Web site: http://www.snia.org/tech_activities/hba_api/

Prerequisites

The installation for the CIM extension verifies that the host is running at least Tru64 5.1B. If the installation fails, see "Fulfilling the Prerequisites" on page 269.

Also, verify the following before you install the CIM extension:

Software Requirements

NOTE: You do not need to install the FC-HBA shared libraries if you are running Tru64 UNIX version 5.1B-4.

If you are running Tru64 UNIX version 5.1B-3 or version 5.1B-2, you must install one of the following SNIA patches to obtain the FC-HBA shared libraries.

- For Tru64 UNIX version 5.1B-2 - Install T64KIT1000413-V51BB25-E-20060222.
- For Tru64 UNIX version 5.1B-3 - Install T64KIT1000414-V51BB26-E-20060222.

To obtain the patch:

1. Go to the IT Resource Center Web site at the following URL: http://www1.itrc.hp.com/.
2. Use the Search box at the Web site to find the patch number. When you search for the patch, make sure IT Resource Center (Compaq) is selected.

   NOTE: To save time, copy the patch number from the PDF or HTML Installation Guide and paste it into the Search box.

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 Tru64 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 388.

Installing the CIM Extension

IMPORTANT: You must install the CIM extension for Tru64 in the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

You can install the CIM extension for Tru64 in either of two ways:

- **On a Standalone Host** - See "Installing the CIM Extension on a Standalone Host" on page 263.

- **On a Cluster** - See "Installing the CIM Extension on a Cluster" on page 263.

Installing the CIM Extension on a Standalone Host

To install the CIM extension using CLI:

1. Login as root.
2. Place the CIM Extension CD-ROM into the CD-ROM drive on the Tru64 server.
3. Create the /cdrom directory on Tru64 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/disk/cdromxx  /cdrom
   ```
   where xx corresponds to the CD-ROM device number.

   You can find the cdrom device number by entering the following at the command prompt:

   ```
   # hwmgr -view devices
   ```
5. To install the CIM extension:
   a. Go to the /cdrom/tru64/ directory, as shown in the following example:

   ```
   # cd /cdrom/tru64/
   ```
   b. Run the script /tru64_local_install.sh at the command prompt:

   ```
   #./tru64_local_install.sh
   ```
   The installation is complete when you are told the following:

   ```
   Installation of AppStorM Tru64 CIM Extensions was successful.
   ```

   NOTE: The tru64_local_install.sh command starts the CIM extension.
6. Eject the CD-ROM by doing the following:
   a. 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.

   b. Press the eject/unload button on the CD-ROM drive.
7. Press the **Eject** button on the CD-ROM drive to take the CD out of the CD-ROM drive.

   The CIM extension for Tru64 starts automatically at boot time by using /sbin/rc3.d scripts. The CIM extension uses port 4673 when it starts automatically after a reboot.
8. Enter the following at the command prompt to find the status of the CIM extension:

   ```
   /opt/APPQcime/tools/status
   ```

Installing the CIM Extension on a Cluster

The installation of the CIM extension on a cluster is similar to the installation of the CIM extension on a standalone node. However, on a cluster it is required to run the install script on only one node of the cluster. By default the install script (tru64_local_install.sh) starts the CIM extension automatically on all nodes of the cluster after an installation. To install the CIM extension on all nodes of the cluster, repeat the steps found in "Installing the CIM Extension on a Standalone Host" on page 263.

To install the CIM extension on just the current node:

1. Go to the `/cdrom/tru64/` directory, as shown in the following example:

   ```
   # cd /cdrom/tru64/
   ```

2. Run the following command at the command prompt:

   ```
   #./tru64_local_install.sh -curnode
   ```

3. You must start the CIM extension manually as described in "Starting the CIM Extension Manually" on page 264.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program lists the name and number for all HBAs 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.

IMPORTANT: The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbatest:

1. Verify that you have installed the CIM extension.
2. Go to the `/opt/APPQcime/tools/hbatest` directory on the host where you installed the CIM extension.
3. Enter the following at the command prompt:

   ```
   ./hbatest
   ```

   The program runs its diagnostics.

Starting the CIM Extension Manually

The management server can only obtain information from this host when the CIM extension is running. 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 "Configuring CIM Extensions" on page 265 for more information. You can also access information about these topics by typing the following:

```
/start -help
```

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 389.

To start the CIM extension, enter 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 Tru64...
```

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 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.

Configuring CIM Extensions

Configuration information is stored in a configuration text file that is read by the CIM extension on start-up. The file is named cim.extension.parameters and is located in the [Installation_Directory]/conf directory on the host. This directory also contains a file named cim.extension.parameters-sample. This file contains samples of available parameters and can be copied into the cim.extension.parameters file and used as a template.

Restricting the Users Who Can Discover the Host

The -users parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the -users parameter.

For example, assume you want to use the management server to discover a Tru64 host, but you do not want to provide the password to the root account. You can provide the password to another valid Tru64 user account that has fewer privileges, for example jsmythe. First, you would add the user to the parameters file. You would then log on to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the Tru64 host.

Follow these steps to add a user to the parameters file:

1. Go to the [Installation_Directory]/conf directory.
2. Open the cim.extension.parameters file in a text editor, and enter the following line:

   ```
   -users myname
   ```

   where myname is a valid Tru64 user name.

NOTE: You can enter multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where `1234` is the new port for the CIM extension
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings,** and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

NOTE: If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.

4. Restart the CIM extension for your changes to take effect.

NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually, or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 266.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 21 Parameters for CIM Extensions

Parameter	Description
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 266.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 266.
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

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. Enter the following at the command prompt:

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

The version number of the CIM extension and the date it was built are displayed, as shown in the following example:

```
Starting CIM Extension for Tru64
Thu Sep 21 14:46:47 EDT xxxx
CXWS x.x.x.x on /192.168.1.5:4673 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
- `4673` is the port used by the CIM extension

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, created by default in the `<Installation_directory>/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in `cxws.log` is moved to `cxws.log.1`. When the logs roll over again, `cxws.log.1` is renamed to `cxws.log.2` and the information that is in `cxws.log` is moved to `cxws.log.1`. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- `cxws.log` - contains the latest logging information
- `cxws.log.1` - contains logging information that was previously in `cxws.log`
- `cxws.log.2` - contains logging information that was previously in `cxws.log.1`

`cxws.log.3` - contains logging information that was previously in `cxws.log.2`

The cxws_native.log file contains logging information relative to Tru64 native operations. The configuration information for cxws_native.log is maintained in /opt/APPQcime/conf/cxws_native.cfg. When the log file size exceeds the LOG_SIZE parameter specified in the configuration file for the cxws_native.log, the file rolls over. The information in cxws_native.log is moved to cxws_native.log.old. If cxws_native.log.old already exists, it is deleted.

Increasing the Native Logging Level

The cxws_native.log contains logging information relative to Tru64 system calls used. The configuration information for cxws_native.log is maintained in /opt/APPQcime/config/cxws_native.cfg, where /opt is the directory into which you installed the CIM extension. More detailed logging information can be obtained by increasing the log level. Set LOG_LEVEL to 3 in cxws_native.cfg, and restart the CIM extension to increase the log level.

Fulfilling the Prerequisites

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

```
# setld -i
```

Ensure that the required patches listed in the prerequisites are present

Removing the CIM Extension from Tru64

This section describes the following:

- Removing the CIM Extension from a Standalone Host, page 269
- Removing the CIM Extension from a Cluster, page 269

Removing the CIM Extension from a Standalone Host

To remove the CIM extension for Tru64:

1. Login as root.
2. Go to the /opt/APPQcime/scripts directory, where /opt is the directory into which you installed the CIM extension.
3. Execute the following script:

```
tru64_local_uninstall.sh
```

4. When you see the following message, the CIM extension has been removed:

```
"UnInstallation of AppStorM Tru64 CIM Extensions was successful".
```

5. To remove the APPQcime directory, go to the /opt and /cluster/member/{memb}/opt directories, and enter the following at the command prompt:

```
    # rm -rf APPQcime
```

Removing the CIM Extension from a Cluster

The uninstall procedure from ”Removing the CIM Extension from a Standalone Host” on page 269 needs to be executed on one node of the cluster only. The script ensures that the agent process is stopped on all nodes and the product is considered removed from all the nodes.

The node specific directory `/cluster/member/{memb}/opt/APPQcime` needs to be cleaned up on each node explicitly.

15 Installing the CIM Extension for Sun Solaris

HP Storage Essentials Standard Edition does not support Sun Solaris hosts. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 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/

Prerequisites

The management server requires certain packages and patches. The installation checks for the required packages listed in the following section and verifies that the Solaris operating system has been installed.

You need the core set SUNWCreq. If you have only the core environment packages installed, install the following manually in the order listed:

1. SUNWlibC - Sun Workshop Compilers Bundled libC
2. SUNWlibCf - SunSoft WorkShop Bundled libC (cfront version)
3. SUNWlibCx - Sun Workshop Bundled 64-bit libC

Keep in mind the following:

- Solaris does not support the upgrading of the CIM extension. Before loading a new CIM extension, see "Removing the CIM Extension from Solaris" on page 279 to verify no agent exists.
- 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:

- **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.
- **Backup Manager** - Make sure you have at least 500 MB if you are using the host as a master backup server in a large environment, for example 300 clients, 25,000 jobs and 500,000 images.

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 388.

Verifying SNIA HBA API Support

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

Keep in mind the following:

- *QLogic host bus adapters only*: For Solaris SAN Foundation Suite, the firmware version reported on the HBA is not the same as what is reported using luxadm. The management server uses the result of the HBAAPI, while luxadm displays different values.

- The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

To run hbatest:

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

Depending on the driver and version of the operating system, the SNIA API library may be installed with the driver or its utility program provided by the vendor. You can find the API library by entering the following at the command prompt:

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

The following are examples of the library names and its path:

Emulex

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

QLogic

```
qla2x00         /usr/lib/libqlsdm.so
```

JNI

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so
JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so
```

SUN Branded

```
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:

- Solaris does not support the upgrading of the CIM extension. Before loading a new CIM extension, see "Removing the CIM Extension from Solaris" on page 279 to verify no agent exists.
- The instructions in this section apply if you are doing a local installation of the CIM extension, as opposed 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 following the instructions in this section, and then performing 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 upgrade the CIM extension, first remove the previous version before installing the latest version. Builds 4.2 and later of the CIM extension are compatible with this build of the management server. You must upgrade your CIM extension if you want the latest functionality, as described in "About Upgrading Your CIM Extensions" on page 189.
- You must install the CIM extension for Sun Solaris to the default directory. If there are space issues, such as large CIM extension binary files, create a symbolic link to a folder with more space.

To install the CIM extension:

1. Login as root.
2. Go to the Solaris directory on the CIM Extension 1 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 APPQcime.pkg APPQcime
   ```

   The APPQcime package is added.
4. When you are asked for an installation directory, enter the path to the default directory (`/opt`), and press **Enter**.
5. When you are asked if you want to continue the installation, enter **y**.

   The CIM extension is installed.
6. When you are asked if you want to add another package, enter **q** to quit the installation.
7. If you see error messages when you install the CIM extension, see "Removing the CIM Extension from Solaris" on page 279.
8. 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
9. Start the CIM extension. See "Starting the CIM Extension Manually" on page 274.

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 389.

To start the CIM extension, enter 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...
```

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 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

Configuring CIM Extensions

Configuration information is stored in a configureable text file that is read by the CIM extension at startup. The unconfigured file is named cim.extension.parameters-sample and is located in the [Installation_Directory]/conf directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file:

1. Open the cim.extension.parameters-sample file and save a copy renamed as cim.extension.parameters to the same directory.
2. Edit the cim.extension.parameters file with the desired settings. See Table 22 on page 277.
3. Save and close the cim.extension.parameters file and then restart the service for the CIM extension by doing the following:
   a. Enter the following to go to the tools directory:
      - `cd /<Installation Directory>/tools directory`
   b. Enter the following to stop the service:
      - `./stop`
   c. Enter the following to start the service:
      - `./start`

Restricting the Users Who Can Discover the Host

The -users parameter provides greater security by restricting access. When you use the management server to discover the host, provide a user name that was specified in the -users parameter.

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 fewer privileges, for example jsmythe. First, you would add the user to the parameters file. You would then log on to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the Solaris host.

Follow these steps to add a user to the parameters file:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -users myname
   ```

   where myname is a valid Solaris user name.

   NOTE: You can enter multiple users by separating them with a colon. For example `-users myname:jsymthe`.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

   NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where `1234` is the new port for the CIM extension
3. Save the file.
4. Restart the CIM extension for your changes to take effect.

   NOTE: The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See ”Discovering Applications, Backup Hosts and Hosts” on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings**, and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM Extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]/conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -on 127.0.0.1,192.168.0.1
   ```

   > **NOTE:** If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

> **NOTE:** The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The -on parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 276.

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 22 Parameters for CIM Extensions

Parameter	**Description**
`-port <new port>`	The CIM extension uses port 4673 by default. Use this command to change the port the CIM extension will access. See "Changing the Port Number" on page 276.
`-on <ip address of NIC card>`	Use this command to configure the CIM extension to listen on a specific network card (NIC). You can also specify the port you used. See "Configuring the CIM Extension to Listen on a Specific Network Card" on page 276.

Table 22 Parameters for CIM Extensions (continued)

Parameter	Description
-user	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
-credentials <username from the management server> :<password>	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
-mgmtServerIP <ip address>	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Finding the Version of a CIM Extension

To find the version number of a CIM extension:

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

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

The version number of the CIM extension and the date it was built are displayed, 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 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

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 Log Files

The logging information for the CIM extension is contained primarily in the cxws.log file, created by default in the <Installation_directory>/tools directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in cxws.log is moved to cxws.log.1. When the logs roll over again, cxws.log.1 is renamed to cxws.log.2 and the information that is in cxws.log is moved to cxws.log.1. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- cxws.log - contains the latest logging information
- cxws.log.1 - contains logging information that was previously in cxws.log
- cxws.log.2 - contains logging information that was previously in cxws.log.1
- cxws.log.3 - contains logging information that was previously in cxws.log.2

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 CIM extension appends the cxws.out file and rolls it over.

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 278.
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.
   ```

16 Installing the CIM Extension for Microsoft Windows

IMPORTANT: Do not install the CIM extension onto the management server.

This chapter contains the following topics:

NOTE: This chapter describes how to install and manage the CIM extension directly on the host. You can also install and manage CIM extensions remotely. See "Deploying and Managing CIM Extensions" on page 181.

IMPORTANT: Make sure you have reviewed Table 2 on page 2 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, devices and host bus adapters. It then makes the information available to the management server.

The CIM extension communicates with a host bus adapter (HBA) by one of two methods:

- The Microsoft HBAAPI.DLL
  - The Microsoft HBAAPI.DLL is available with Microsoft Windows 2003 SP1 and later. This is default method that the CIM extension uses.
  - The CIM Extension requires hbaapi.dll 5.2.3790.2753 which ships with Microsoft Windows 2003 SP2 or can be downloaded from Microsoft Knowledge Base KB922772 for earlier versions of Windows.
  - If you are running Windows 2000 or a version of the hbaapi.dll before version 5.2.3790.2753, the SNIA HBA API will be used.
- The SNIA HBA API (appiq_hbaapi.dll)
  - The Host Bus Adapter Application Programming Interface (HBA API) created by the Storage Network Industry Association (SNIA).

- The management server supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the following Web page at the SNIA website:
  http://www.snia.org/tech_activities/hba_api/
- The appiq_hbaapi.dll file is installed as part of the CIM extension to provide access to the SNIA HBA API and it can be found in `<Installation_Directory>\CimExtensions\lib\`.
- The SNIA compliant HBA API provided by the HBA Vendor can be verified by checking the Windows registry for the following:
  - **For 32-bit operating systems** - `\\HKEY_LOCAL_MACHINE\Software\SNIA\HBA`
  - **For 64-bit operating systems** - `\\HKEY_LOCAL_MACHINE\Software\WoW6432Node\SNIA\HBA`

To use the SNIA HBAAPI (appiq_hbaapi.dll):

1. Set the following registry setting:

   `HKEY_LOCAL_MACHINE\SOFTWARE\AppIQ`
2. Create a String Value named HbaApiPath with Value Data `<Installation Directory>\CimExtensions\lib\appiq_hbaapi.dll`.
3. In the `<Installation_Directory>\CimExtensions\tools` directory on the host, the program hbatest.exe is available for testing if the HBA configuration is able to provide information.

Verifying SNIA HBA API Support

The management server can only talk to host bus adapters (HBAs) that support the SNIA HBA API. The hbatest program, which is accessible from the `<Installation_Directory>\CimExtensions\tools`, lists the name and number for all HBAs 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. Open a command window and change the directory to `<Installation_Directory>\CimExtensions\tools`.
2. Enter the following at the command prompt:

   ```
   hbatest.exe
   ```

   The `hbaapi.dll` must be upgraded or the SNIA HBA API must be used if the following configuration is used:
   - You are using Emulex HBA's.
   - The host has a version of `hbaapi.dll` that is earlier than version 5.2.3790.2753.
   - The host is running HP MPIO multipathing.

When using Emulex HBA's and the SNIA library, remember that previous versions of HBAnyware provide the SNIA library; however, several later versions of HBAnyware do not ship with the SNIA library and rely upon the Microsoft SNIA library. Your configuration may require you to run the

Emulex setupelxhbaapi program, which modifies the registry so that SNIA libraries can be detected by the CIM extension. To install the setupelxhbaapi program, download it from the Emulex website:

http://www.emulex.com

The `setupelxhbaapi` program installs the `hbaapi.dll` and Emulex `emulexhbaapi.dll` files into the `program files\emulex\hbaapi` folder and creates a registry key with the absolute path to the `emulexhbaapi.dll` file.

Installing the CIM Extension

Keep in mind the following:

- You must have administrator privileges to install this software.
- 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 disable the "Explorer Enhanced Security Settings."

Perform the following steps:

1. Insert the CD-ROM for the CIM extensions, go to the Windows directory, and 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 **Choose**. You can always display the default directory by clicking **Restore Default Folder**. When you are done, click **Next**.
5. Check the preinstallation summary. You are shown the following:
   - Product Name
   - Installation Folder
   - Version
   - Disk Space Information
6. Do one of the following:
   - Click **Install** if you agree with the pre-installation summary.
   - Click **Previous** if you want to modify your selections.
   - Click **Cancel** to exit the installer.

   The CIM extension is installed.
7. When you have been told the installation is 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 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 extension.
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.

Upgrading a Host with the Latest CIM Extension

When upgrading the CIM extension for Windows, the following issues may occur:

- The Host CIM Extension Version Report in Reporter still displays the previous version.
- The management server does not display the host bus adapter data for Windows hosts.
- File System Viewer scans are not possible.

To prevent these issues from occurring, perform the following steps:

1. Upgrade the management server, as described in the following chapters:
   - **Microsoft Windows** - See "Installing the Management Server on Microsoft Windows" on page 7.
   - **Linux** - See "Installing the Management Server on Linux" on page 59.
2. Upgrade the CIM extension on the Windows hosts. Install CIM extension over a previous version by following the installation steps as described in "Installing the CIM Extension" on page 283.

NOTE: You do not need to upgrade the CIM extensions all at once. Keep in mind, however, that CIM extensions from earlier versions do not return all information; for example they don't return FSRM data. It is strongly recommended you upgrade your CIM extensions on Windows as soon as possible.

3. Perform a discovery in HP SIM (**Options** > **Discovery**) for a re-discovery of the upgraded hosts. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information about discovering hosts.
4. Run Discovery Data Collection in HP SIM (**Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**).
5. Refresh reports to update report data.

Configuring CIM Extensions

Configuration information is stored in a configureable text file that is read by the CIM extension at start-up. The unconfigured file is named `cim.extension.parameters-sample` and is located in the `[Installation_Directory]\CimExtensions\conf` directory on the host. This file contains samples of available parameters that will modify the behavior of the CIM extension and can be used as a template.

To manage the CIM extension using the parameters file, do the following:

1. Open the `cim.extension.parameters-sample` file and save a copy renamed as `cim.extension.parameters` to the same directory.
2. Edit the `cim.extension.parameters` file with the desired settings. See Table 23 on page 288.
3. Save and close the `cim.extension.parameters` file and then stop and restart the CIM service by rebooting the host or restarting the AppStorWin32Agent service from the Services window.

This section contains the following topics:

- Changing the Port Number, page 285
- Configuring the CIM Extension to Listen on a Specific Network Card, page 286
- Defining UNC Volumes, page 286
- Additional Parameters, page 287

Changing the Port Number

The CIM extension uses port 4673 by default. If this port is already in use, follow these steps to change the port the CIM extension will access:

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

   ```
   -port 1234
   ```

   where `1234` is the new port for the CIM extension.
3. Save the file.

4. Restart the CIM extension for your changes to take effect.

> **NOTE:** The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

Adding a New Port Number to Discovery

If you change the port number, you must include the new port number in your discovery. If you have not already done so, discover the host. See "Discovering Applications, Backup Hosts and Hosts" on page 297 for more information, and then select **Options** > **Protocol Settings** > **System Protocol Settings**, and select the host you discovered as a target. On the System Protocol Settings page, enter the port number for the host under the WBEM section.

Configuring the CIM Extension to Listen on a Specific Network Card

Follow these steps to configure the CIM extension to listen on a specific network card (NIC):

1. Go to the `[Installation_Directory]\CimExtensions\conf` directory.
2. Open the `cim.extension.parameters` file in a text editor, and enter the following line:

```
-on 127.0.0.1,192.168.0.1
```

> **NOTE:** If you want to configure the CIM extension to listen on multiple NICs, use a comma to separate multiple addresses.

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

> **NOTE:** The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

The "-on" parameter 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:

```
-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 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. See "Adding a New Port Number to Discovery" on page 286.

Defining UNC Volumes

You can use UNC shares to discover file system data from a server. If you want to scan UNC volumes, you must define them in a `UncShares.xml` file. To create the `UncShares.xml` file on a Windows host:

1. Confirm that a CIM extension is installed on the Windows host.

2. Go to the `<Installation_Directory>\CimExtensions\conf` directory.
3. Open the `UncShares.xml-sample` file in a text editor.
4. Identify the host through which the UNC shares' scan is planned. This is the host through which you will be scanning UNC shares from a different/remote host.
5. Add the host name and shared directory to the following line:

   ```
   <!-- <UNC_SHARE PATH=""/> -->
   ```

   For example:

   ```
   <UNC_SHARE PATH="\\RemoteSystem\MyShare1"/>
   ```

   Where `RemoteSystem` is the name of the host and `MyShare` is the name of the shared directory.

   Repeat it for all of your shares, as shown in the following example:

   ```
   <UNC_SHARE PATH="\\RemoteSystem\MyShare1"/>
   <UNC_SHARE PATH="\\RemoteSystem\MyShare2"/>
   <UNC_SHARE PATH="\\RemoteSystem\MyShare3"/>
   ```
6. Save the file as `UncShares.xml`.
7. Restart the CIM Extension service on the managed host.
8. Update the element details for the host from the management server by running a Discovery Data Collection.
9. Edit the File System Viewer configuration page for the host selecting the desired UNC shares to scan.

   The username and password combination you used for discovering the host should have at least read only permissions on the file shares which need to be scanned. So in most cases this would be a service account which you can have created in the active directory. This service account should be an admin on the “proxy FSV host” and should have read only (at least) access to the UNC share

   NOTE: You can use the IP address of the host instead of the name.

   If you want to discover multiple UNC shares which have different credentials, use different “proxy FSV hosts” as you can currently use only use one login / password pair [each UNC share has its own associated login / password in this release].

Additional Parameters

The following table describes additional parameters that can be specified in the `cim.extension.parameters` file:

Table 23 Parameters for CIM Extensions

Parameter	Description
`-user`	The user defined in this parameter must be a valid existing user for the host. Only the user needs to be defined. The user name and password are provided from the management server during discovery. The user does not need to have root authority. A colon-separated list can be used to specify multiple users.
`-credentials <username from the management server> :<password>`	The credentials defined by this parameter must match the values entered from the management server during discovery. They are not used as authentication on the host itself.
`-mgmtServerIP <ip address>`	This parameter restricts the CIM extension to listen only to a specific management server IP address.

Rolling Over the Log Files

The logging information for the CIM extension is contained primarily in the cxws.log file, created by default in the `<Installation_Directory>/CimExtensions/tools` directory. The cxws.log file rolls over once it becomes more than 100 MB. The information in `cxws.log` is moved to `cxws.log.1`. When the logs roll over again, `cxws.log.1` is renamed to `cxws.log.2` and the information that is in `cxws.log` is moved to `cxws.log.1`. The numbering for the files continues sequentially, with there being a maximum of three backup logs, as follows:

- `cxws.log` - contains the latest logging information
- `cxws.log.1` - contains logging information that was previously in `cxws.log`
- `cxws.log.2` - contains logging information that was previously in `cxws.log.1`
- `cxws.log.3` - contains logging information that was previously in `cxws.log.2`

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 CIM extension appends starting, stopping, and unexpected error conditions to the existing `cxws.out` file.

Removing the CIM Extension from Windows

IMPORTANT: If you remove a CIM extension from a Windows host where there is a service that is using WMI (such as Microsoft Exchange), you are shown a message saying that the WMI service could not be stopped. Continue with the removal of the CIM extension. Reboot after the uninstall process completes.

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 **Change/Remove**.
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.

17 Installing and Discovering the Windows Proxy

This chapter describes the following:

The Windows Proxy is required when the management server is on Linux and you want to obtain information from Microsoft Windows hosts that do not have a CIM extension installed. First, install the Windows Proxy as described in "Installing the Windows Proxy" on page 291. Then, discover the Windows Proxy as described in "Discovering the Windows Proxy" on page 292.

Keep in mind the following:

- File System Viewer will not work if the hosts behind the Windows proxy are on a private network. If you want to use File System Viewer and your license lets you use this functionality, the Windows hosts cannot be on a private network.
- File System Viewer will also not work if the Windows proxy and the management server do not have network connectivity.
- The management server is unable to discover a database 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 the database.
- If you run into problems with starting the Windows proxy, decrease the maximum Java heap size, as described in "Decreasing the Maximum Java Heap Size" on page 294.
- When the Windows proxy is installed on a new server, the Windows hosts must be re-discovered.

Installing the Windows Proxy

IMPORTANT: If you are upgrading the Windows proxy, you can install the latest version of the Windows Proxy over the previous version.

To install the Windows proxy:

1. Insert the Utilities CD-ROM, go to the Windows directory and then double-click **InstallWindowsProxy.exe**.
2. When you see the introduction screen, click **Next**.
3. 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**.

4. Read the important notes. Then, click **Next**.
5. Check the pre-installation summary. You are shown the following:
   - Product Name
   - Installation Folder
   - Disk Space Required
   - Disk Space Available
6. 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 Windows Proxy is installed.
7. When you have been told the installation has been successful, click **Done** to quit the installation.

   IMPORTANT: Keep in mind that the Windows Proxy automatically starts when the system is restarted. The management server can only obtain information from the Windows hosts when the Windows Proxy (AppStorWinProxy service) is running.

8. If the Windows host running the Windows proxy has a private and a public network interface, you must modify the winproxy.conf file.
9. Discover the Windows proxy as described in the topic, "Discovering the Windows Proxy" on page 292.

Discovering the Windows Proxy

IMPORTANT: Install the Windows proxy before you try the following steps.

Keep in mind the following:

- Install the Windows proxy before you try the following steps.
- The recommended workaround for entering an IP address into the discovery list as well as the Windows Proxy list is to use IP address in one user interface and DNS name in the other.

To discover a Windows proxy:

1. Select **Discovery** > **Setup** on the management server.
2. Click the **Windows Proxy** tab.
3. Enter the following information for the Windows proxy:

IMPORTANT: A primary key violation error is displayed when you have the same IP address or DNS name listed in both the Discovery list (**Discovery** > **Setup**) and in the Windows Proxy list. If you have already entered the IP address for a host into the discovery list (**Discovery** > **Setup**), provide its DNS name in the Windows Proxy list. Likewise, if the DNS name for a host is listed in the Discovery list, provide its IP address in the Windows Proxy list.

- **IP Address/DNS Name** - The IP address or DNS name used to access the host running the Windows proxy.
- **User Name** - The user name of an account used to access the host running the Windows proxy.
- **Password** - The password of an account used to access the host running the Windows proxy.
- **Verify Password**

4. Click **OK**.
5. Click the **IP Addresses** tab.
6. Add the hosts and applications as described in the topic, "Discovering Applications, Backup Hosts and Hosts" on page 297.
7. Click **Start Discovery** if you have already added your hosts and applications for discovery.

Configuring Windows Proxy Authentication

To discover the Windows proxy, the management server requires by default the password and user name of the administrator's account of the host. If you do not want to use the administrator's password for discovery, you can modify the `winproxy.conf` file so that another user name and password can be used. The following options are available to you:

- **Create another Windows account for the host** - You can provide a user name and password other than the administrator's for discovery. Just create a Windows account for the host. You must then set the following properties in the `[install_directory]\WindowsProxy\winproxy.conf` file to true: `winproxy.allowAllWindowsUsers` and `winproxy.authenticateWindowsUsers`. After you modify the `winproxy.conf` file, you must restart the AppStorWinProxy service, which is the service for the Windows proxy. Refer to the following example:

  ```
  wrapper.java.additional.7=-Dwinproxy.authenticateWindowsUsers=true
  wrapper.java.additional.#=-Dwinproxy.allowAllWindowsUsers=true
  ```

  where # is the next consecutive number in the list of properties, for example `wrapper.java.additional.7`. This number can change based on the number of properties under `# Java Additional Parameters` in the `winproxy.conf` file.
- **Create a user name and password in the winproxy.conf file** - If you do not want to use Windows authentication to create another user account, you can set a user name and password in the `winproxy.conf` file. Although this user name and password can be used to discover the Windows proxy, it cannot be used to log into the host running the Windows proxy.

See the following steps for more information on how to set a user name and password in the `winproxy.conf` file.

To set a user name and password in the `winproxy.conf` file:

1. Open the `[install_directory]\WindowsProxy\winproxy.conf` file in a text editor, such as Notepad.
2. Add the following underlined examples after the last line in put in the application parameters as follows:

   ```
   # Application parameters. Add parameters as needed starting from 1
   wrapper.app.parameter.1=com.appiq.cxws.main.WmiMain
   wrapper.app.parameter.2=-reloading
   wrapper.app.parameter.3=-u
   wrapper.app.parameter.4=username
   wrapper.app.parameter.5=-p
   wrapper.app.parameter.6=password
   ```

   where

   - `username` is the name of the user account
   - `password` is the password for the user account

   The numbering must be consecutive. For example, if the last line in `# Application Parameters` ends at 2 you must number the code as follows:

   ```
   wrapper.app.parameter.3=-u
   wrapper.app.parameter.4=username
   wrapper.app.parameter.5=-p
   wrapper.app.parameter.6=password
   ```

   where

   - `username` is the name of the user account
   - `password` is the password for the user account
3. Restart the AppStorWinProxy service, which is the service for the Windows proxy.

Decreasing the Maximum Java Heap Size

If you run into problems with starting the Windows proxy on Windows XP, decrease the maximum Java heap size for the Windows proxy as follows:

1. Open the `[install_directory]\WindowsProxy\winproxy.conf` in a text editor, such as Notepad.
2. Change the value of the `wrapper.java.maxmemory` property from 1024 to 512 MB, as shown in the following example:

   ```
   wrapper.java.maxmemory=512
   ```
3. Save the `winproxy.conf` file.
4. Restart the AppStorWinProxy service, which is the service for the Windows proxy.

Removing the Windows Proxy

To remove the Windows proxy:

1. Go to the Control Panel in Microsoft Windows.
2. Double-click **Add or Remove Programs**.
3. From the Currently installed programs list, select **HP Windows Proxy**.
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.

18 Discovering Applications, Backup Hosts and Hosts

HP Storage Essentials Standard Edition supports a subset of the devices supported by Enterprise Edition. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter describes the following:

Step 1 — Discovering Your Hosts and Backup Manager 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 a CIM extension on the host if you want to obtain detailed information about the host and its applications, including those applications for backup. See the support matrix for your edition for information about which backup applications the management server supports.

For information about discovering clustered hosts, see "Host and Application Clustering" on page 341.

The management server also detects the backup applications its supports, such as Veritas™ NetBackup™ or HP Data Protector. If you are licensed for Backup Manager and you want to manage and monitor your backup applications, select **Include backup details** when you run Discovery Data Collection, as described in "Step B — Discovery Data Collection" on page 301.

Keep in mind the following:

- Make sure you have reviewed the table, Table 2 on page 2 to make sure you are at the correct step.
- Elements discovered through SMI-S and hosts discovered with CIM extensions from Build 5.1 and later of HP Storage Essentials cannot be added to discovery groups. These elements are listed separately and can be placed independently into scheduled Discovery Data Collection tasks without being part of a discovery group. This allows you greater flexibility when gathering discovery data. (For more information, see "Creating Custom Discovery Lists" on page 163).

  If you are upgrading from a previous build of the product, and you rediscover your hosts, they will be moved out of their existing discovery groups. Each rediscovered host would be placed in its own discovry group. If the original discovery groups containing these hosts were included in scheduled Discovery Data Collection tasks, the schedules would be modified to contain the new discovery groups for rediscovered hosts.

- After installing the CIM extension on a DataProtector system on Windows, check the Logon account for the DataProtector CRS service and verify that it matches the AppStorWin32Agent service. To determine the Logon account for the DataProtector CRS service, go to **Control Panel > Administrative Tools > Services**, select the DataProtector CRS service, access its Properties page, and select the **Logon** tab. To determine the Logon account for the AppStorWin32Agent service, go to **Control Panel > Administrative Tools > Services**, select the AppStorWin32Agent service, access its Properties page, and select the **Logon** tab.
- If you change the password of a host after you discover it, stop and restart the CIM extension running on the host, and change the host password in the WBEM Settings section of the System Protocol Settings page.
- If you update the system protocol settings for a host in HP SIM, the updated information is sent to HP Storage Essentials when an identification step occurs in HP SIM.
- 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.
- If you want to receive status reports about Discovery Data Collection, see "Configuring E-mail Notification for Discovery Data Collection" on page 398 for information about how to configure this option.
- Depending on your license, you may not be able to access Backup Manager, File System Viewer and/or monitor certain applications may not be available. See the List of Features to determine if you have access to Backup Manager, 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, see 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 413.
- Discovery Data Collection can hang if obtaining information from an AIX host where SAN storage was previously available is no longer visible to the operating system. You may need to reboot the management server to resolve this issue.
- When discovering a Linux host from the management server, the operating system/server type is not available.
- If you started a CIM extension on a Sun Solaris host by using the `cim.extension.parameters` config file or with the `./start -users` command, the user name provided in the command must be used to discover the host. For example, if you use ./start -users myname:yourname (where myname and yourname are valid UNIX accounts) to start the CIM extension, myname or yourname and its password must be used to discover the host.
- If you try to discover a Solaris host with multiple IP address, the management server picks only one IP address for discovery.

- You can configure the management server to obtain information about your backup manager hosts at a set interval. See the topic, “Scheduling Backup Collection for Backup Managers” in the HP SE User Guide for more information about collectors.

Discovery of hosts consists of these steps:

- ”Step A — Set Up Discovery for Hosts” on page 299.
- ”Step B — Discovery Data Collection” on page 301

Step A — Set Up Discovery for Hosts

HP recommends a phased discovery process. You can discover your elements in phases by creating separate tasks for groups of elements. Before you discover applications, backup servers, and hosts, you should have discovered your switches, storage systems, NAS devices and tape libraries. See ”Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 105 for more information.

Use the following procedure for each discovery task:

1. Decide if you will use global or system credentials for the discovery task. See ”Using Credentials” on page 108 for tips on how to choose the credential type that best suits your environment.
2. If you decide to use global credentials, enter them now:
   a. Select **Options** > **Protocol Settings** > **Global Protocol Settings**.
   b. Enter the global user name, and password in the Default WBEM settings section.
   c. Click **OK**.

   IMPORTANT: For best results, enter only global credentials that apply to the set of hosts for the current discovery task. When this discovery task is complete, you can delete the element specific global credentials and enter global credentials for the next set of hosts you want to discover.

3. Select **Options** > **Discovery**.
4. Click **New** on the HP SIM Discovery page Automatic tab.
5. Name the task based on the hosts being discovered. For example, *Windows hosts*.
6. Clear the Automatically execute discovery every check box.
7. Enter the IP addresses of the hosts to discover in the Ping inclusion ranges, system (hosts) names, templates, and/or hosts files box.

NOTE: To use a hosts file to specify systems for an automatic discovery, add the hosts file name to the Ping inclusion ranges, templates and/or hosts files section on the Discovery page, Automatic tab, Configure general settings section. Use the following statement: `$Hosts_filename` where *Hosts_filename* is the name of the hosts file that you want to use.

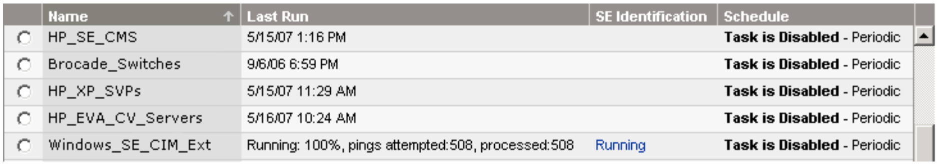
NOTE: Refer to *Creating a new discovery task* in the HP SIM online help for more information.

8. Select the discovery task and click **Run Now**. HP SIM pings each host. If the ping is successful, the host is added to HP SIM's All Systems collection.
9. If you did not enter global credentials, enter system credentials for your hosts.
   a. Click **All Systems** in the System and Event Collections pane.
   b. Click the element name or IP address in the System Name column of the system table view page.
   c. Click the **Tools & Links** tab.
   d. Click the **System Protocol Settings** link.
   e. Enter the host's user name and password in the WBEM settings section.
   f. Click **OK**.

NOTE: You can update the system protocol settings for multiple systems by clicking **Options > Protocol Settings > System Protocol Settings**.

10. Select **Options > Discovery**.
11. Select the discovery task created in step 1 and click **Run Now**.

    When complete, the task shows 100%. Within two minutes HP Storage Essentials Discovery automatically begins. At this time, the status in the SE Identification column changes from Pending to Running. You can click the **Running** link to view the HP Storage Essentials Discovery progress.

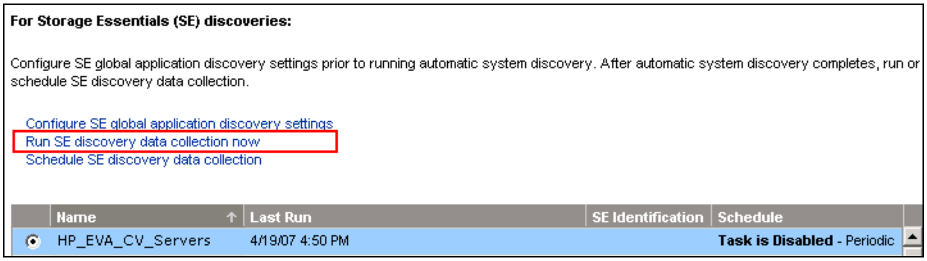


	Name	Last Run	SE Identification	Schedule
○	HP_SE_CMS	5/15/07 1:16 PM		**Task is Disabled** - Periodic
○	Brocade_Switches	9/6/06 6:59 PM		**Task is Disabled** - Periodic
○	HP_XP_SVPs	5/15/07 11:29 AM		**Task is Disabled** - Periodic
○	HP_EVA_CV_Servers	5/16/07 10:24 AM		**Task is Disabled** - Periodic
○	Windows_SE_CIM_Ext	Running: 100%, pings attempted:508, processed:508	Running	**Task is Disabled** - Periodic

Figure 13 Discovery progress

NOTE: SE discovery processing might finish before the SE Identification column shows the Running status. From HP SIM, select **Tasks & Logs > View Storage Essentials Logs** to see the HP Storage Essentials discovery progress.

12. To obtain details about your discovered elements, click the **Run SE Discovery Data Collection Now** link in the For Storage Essentials (SE) discoveries section above the list of tasks.



For Storage Essentials (SE) discoveries:

Configure SE global application discovery settings prior to running automatic system discovery. After automatic system discovery completes, run or schedule SE discovery data collection.

Configure SE global application discovery settings
Run SE discovery data collection now
Schedule SE discovery data collection

	Name	Last Run	SE Identification	Schedule
●	HP_EVA_CV_Servers	4/19/07 4:50 PM		**Task is Disabled** - Periodic

Figure 14 Run SE Discovery Data Collection Now link

NOTE: You can also click **Options > Storage Essentials > Discovery > Run Discovery Data Collection** to access this functionality. You must run Discovery Data Collection to obtain information about your elements. Run Discovery Data Collection when the network is not busy because this step takes some time to finish. See "Step B — Discovery Data Collection" on page 301 for more information.

13. Verify the **Include backup details** option is selected if you want to monitor and manage backup applications in Backup Manager.
14. Verify the **Include infrastructure details** option is selected. This option is required to manage and monitor your elements not related to the backup infrastructure.
15. Click **Get Details**.

To verify that discovery was successful, click **Tools > Storage Essentials > System Manager**. The Topology page appears and shows your discovered elements.

Step B — Discovery Data Collection

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. Clusters won't be recognized until Discovery Data Collection is completed. Discovery Data Collection must be run on all of the participating nodes of application clusters.

Keep in mind the following:

- Running Discovery Data Collection takes time. You might want to perform this process when the network and the managed elements are not busy.
- Reports show data from the last successful Discovery Data Collection and report cache update. When a scheduled Discovery Data Collection finishes, the report cache refreshes automatically. If you run Discovery Data Collection manually, the report cache updates every 6 hours. For information about refreshing the report cache, see the User Guide.

- During Discovery Data Collection the data you see in the user interface is not updated until the data collection is finished.
- During Discovery Data Collection, the topology in System Manager is recalculated. While the topology is being recalculated, the loading of the user interface in Storage Essentials may be slow.
- You can use discovery groups to break up Discovery Data Collection. For example, instead of running Discovery Data Collection for all elements, you could specify only the elements in Discovery Group 1. For more information, see "Using Discovery Groups" on page 162.
- When an element in a discovery group is updated, its dependent elements are also updated.
- If you want to monitor and manage backup servers, select **Include backup details**. If you also want to manage and monitor the host itself, select **Include infrastructure details**; otherwise, the host appears as a generic element in the topology in System Manager.
- If Discovery Data Collection includes an AIX host, three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port are displayed in the system log. You can ignore these errors.
- You can quarantine elements to exclude them from Discovery Data Collection. For example, if you want to get information about all the elements in a discovery group except for one, you can quarantine that element. For more information, see "Placing an Element in Quarantine" on page 167.
- If a problem occurs with a host or SMI-S element during Discovery Data Collection, the host or element is automatically quarantined. To remove the element from quarantine, see "Removing an Element from Quarantine" on page 167.
- If you want to receive status reports about Discovery Data Collection, see "Configuring E-mail Notification for Discovery Data Collection" on page 398 for information about how to configure this option.

To obtain details:

Getting details is included in "Step A — Set Up Discovery for Hosts" on page 299.

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 and Backup Manager Hosts" on page 297.

You can configure the management server to monitor hosts and applications, such as Oracle, Microsoft Exchange server, Caché, 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 installation guide.

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 and Backup Manager Hosts" on page 297, 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 run Discovery Data Collection. Discovery Data Collection 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 304
- "Monitoring Microsoft SQL Server" on page 312
- "Monitoring Sybase Adaptive Server Enterprise" on page 320
- "Monitoring Microsoft Exchange" on page 323
- "Monitoring Caché" on page 325

Creating Custom Passwords on Managed Database Instances

Depending on the password policy, SQL Server 2005 may require that passwords be alphanumeric. For this reason, a managed SQL Server 2005 database instance might not accept the default managed database password (`password`) during APPIQ_USER creation. A script is provided to input an alphanumeric password for SQL Server 2005. For all other applications, this script is optional.

Because the management server uses a single password for managing all types of databases, the script for specifying a custom password is provided for each managed database type (SQLServer, Oracle, Sybase, and Caché). If the password is changed on any managed database instance, you should run the respective custom password scripts for each of the other managed database instances, and specify the same password.

The script names for each database type are as follows:

Table 24 Script Names for Managed Databases

Database Type	**With Default Password**	**With Custom Password**
Oracle	CreateOracleAct.sh (or .bat) or CRACCT.COM (for OpenVMS)	CreateOracleActWithCustomPwd.sh (or .bat) or CUSTACCT.COM (for OpenVMS)
SQL Server	CreateSQLServerAct.bat	CreateSQLServerActCustomPwd.bat
Sybase	CreateSybaseAct.bat	CreateSybaseActCustomPwd.bat
Caché 5.0.20	createCacheDB50User.sh (or .bat)	createCacheDB50UserCustomPwd.sh (or .bat)
Caché 5.2 and 2007.1	createCacheDBUser.sh (or .bat) or CRUSER.COM (for OpenVMS)	createCacheDBUserCustomPwd.sh (or .bat) or CUSTUSER.COM (for OpenVMS)

After changing the password on all managed database instances, the password must be changed on the Storage Essentials management server. To change the password on the Storage Essentials management server:

1. Select **Discovery > Setup**.
2. Click the **Applications** tab.
3. Click **Change Password** in the Change Password for Managed Database Account section.
4. Enter the password that was used for creating APPIQ_USER on the managed database instances.

Monitoring Oracle

To monitor and manage Oracle, you must do the following:

- "Step A — Create the APPIQ_USER Account for Oracle" on page 304
- "Step B — Provide the TNS Listener Port" on page 307
- "Step C — Set up Discovery for Oracle 10g" on page 308

After you complete these steps, you must discover Oracle, and perform Discovery Data Collection. See "Step 3 — Discovering Applications" on page 335.

Keep in mind the following:

- 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.
- By default discovery of Oracle is not supported through autoscan. To enable autoscan, add the line - "`oracleautoscan=true`" in the Custom Properties window from the Advanced page in **Options** > **Storage Essentials** > **Manage Product Health**. Then, click **Advanced** in the Disk Space tree. Auto scans are only supported for Oracle 9i. To discover Oracle 10g instances, you must enter the application information described "Step C — Set up Discovery for Oracle 10g" on page 308.

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 platforms) or `CRACCT.COM` (on OpenVMS) 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.

NOTE: To create the APPIQ_USER with a custom password, run `CreateOracleActWithCustomPwd.bat` (on Microsoft Windows) or `CreateOracleActWithCustomPwd.sh` (on UNIX platforms) or `CUSTACCT.COM` (on OpenVMS). For more information, see "Creating Custom Passwords on Managed Database Instances" on page 303.

Keep in mind the following:

- The `CreateOracleAct.bat` script must run under SYS user.

- Create the APPIQ_USER account on the 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. See 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.
- When creating the APPIQ_USER account on an Oracle Real Application Cluster (RAC) Database, this script should be run only once, on any one of the instances of the Oracle RAC Database. Since all the instances of an Oracle RAC access the same Database, it is sufficient to create the APPIQ_USER account on any one of the instances.
- 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 the management server:

1. Do one of the following:
   - **To run the script on IBM AIX, SGI IRIX, HP-UX, Linux or Sun Solaris**, log into an account that has administrative privileges, mount the CIM extensions CD-ROM (if not auto-mounted), and go to the `/DBIQ/oracle/unix` directory by typing the following:

     ```
     # cd /cdrom/DBIQ/oracle/unix
     ```

     where `/cdrom` is the name of the directory where you mounted the CD-ROM.
   - **To run the script on Microsoft Windows**, go to the `DBIQ\oracle\win` directory on the CIM extensions CD-ROM.
   - **To run the script on OpenVMS**:

     Log into an account that has administrative privileges.

     Mount the CIM Extensions CD-ROM (if not auto-mounted) using the following command.

     ```
     $ MOUNT /MEDIA=CDROM
      /UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION
     DQB0
     ```

     where `DQB0` is the CD-ROM drive.

     Go to the directory containing the Oracle agent creation script using the following command.

     ```
     $ SET DEF DQB0:[OVMS.DBIQ.ORACLE]
     ```
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 UNIX platforms) or `CRACCT.COM` (on OpenVMS) on the computer with the Oracle database. On OpenVMS, run `CRACCT.COM` on the host using the following command.

```
$ @CRACCT.COM
```

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 the 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.
   - Grants create session and select on dictionary tables privileges to APPIQ_USER, enabling the 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 UNIX platforms) or `RMACCT.COM` (on OpenVMS).

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.
- 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.
- When removing the APPIQ_USER account from an Oracle RAC Database, this script should be run only once, on any one of the instances of the Oracle RAC Database. Since all the instances of an Oracle RAC access the same Database, it is sufficient to remove the APPIQ_USER account from any one of the instances.

To remove the APPIQ_USER account for that Oracle instance:

1. If you plan to remove the management software for Oracle from a UNIX platform, do the following:

   a. Log into an account that has administrative privileges.

   b. Mount the CIM Extensions CD-ROM (if not auto-mounted).

c. Go to the `/DBIQ/oracle/unix` directory by typing the following:

```
# cd /cdrom/DBIQ/oracle/unix
```

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

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. If you plan to remove the management software for Oracle from a computer running OpenVMS do the following:

   a. Mount the CIM Extensions CD-ROM (if not auto-mounted) using the following command:

   ```
   $ MOUNT /MEDIA=CDROM
   UNDEFINED_FAT=STREAM:32767/OVERRIDE=IDENTIFICATION

   DQB0
   ```

   where `DQB0` is the CD-ROM drive.

   b. Go to the directory containing the Oracle agent creation script using the following command:

   ```
   $ SET DEF DQB0:[OVMS.DBIQ.ORACLE]
   ```

4. 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.
5. Run `UninstallOracleAct.bat` (on Windows) or `UninstallOracleAct.sh` or `RMACCT.COM` (on OpenVMS).
6. This script removes the management software for the specified Oracle instance.

   NOTE: You can use a remote Oracle client to run this script.

7. 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.
8. 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. Enter the new port number and click **OK.**
4. If necessary, click the 🗑 button to remove the old port number.

IMPORTANT: Monitoring Oracle 10g or Oracle clusters requires an additional step. If you are not monitoring Oracle 10g or Oracle clusters, go to ”Step 3 — Discovering Applications” on page 335.

Step C — Set up Discovery for Oracle 10g

NOTE: If you are discovering an Oracle cluster, see ”Discovering Oracle Real Application Clusters (RAC)” on page 309.

NOTE: By default discovery of Oracle is not supported through auto scan. To enable autoscan, add the line - "`oracleautoscan=true`" in the Custom Properties window from the Advanced page in **Options** > **Storage Essentials** > **Manage Product Health**. Then, click **Advanced** in the Disk Space tree. Autoscans are only supported for Oracle 9i. To discover Oracle 10g instances, you must enter the application information described in the following procedure.

To monitor Oracle 10g, provide additional information as described in the following steps:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **System Application Discovery Settings**, select a target, and click **Run Now**.

   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.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Oracle.

   The **Management IP/DNS Name** box is optional.
4. In the **Server Name** box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
5. In the **Port Number** box, enter 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))
      )
    )
  )
```

6. Select **ORACLE** from the Database Type menu.
7. Click **OK**.

Discovering Oracle Real Application Clusters (RAC)

Since Oracle RAC is an active-active application cluster, one RAC instance can provide information for the whole RAC. Regardless of the instance through which the database is accessed, the same sets of tables are accessed. This includes the data dictionary tables that are used to understand the logical and physical storage organization of the Oracle RAC application.

Discovery of Oracle RAC Instances Using One Instance

Because one RAC instance can provide information for the whole RAC, it is possible to identify and discover all the instances in the Oracle RAC cluster from any one of its instances. This means that the you can enter the application setup information for one instance of the Oracle RAC, and the management server will automatically discover the other instances, subject to certain conditions. The conditions to be satisfied for discovering all the instances of Oracle RAC using application setup information from one of its instances are as follows:

- Only the Oracle RAC instances running on hosts already discovered and identified as part of the same cluster will be discovered as part of the Oracle RAC on the management server.
- The management server is able to contact the hosts running Oracle RAC instances using the short host name. The management server can be configured to access the hosts running Oracle RAC instances using the short name in the following ways:
  - On the management server, add entries for each host running an Oracle RAC instance in `/etc/hosts` (on UNIX platforms) or `%WINDIR%\system32\drivers\etc\hosts` (on Windows).
  - Add the domain of the host in the domain search list of the management server under the search option of `/etc/resolv.conf` (on UNIX platforms) or Append these DNS suffixes (in order) on the **Advanced TCP/IP Settings > DNS** tab (on Windows).
- The listener is configured on the same IP address that is used to discover the host. For example, on the Application Setup page, the management IP address for the application should be the same as the host IP address.
- Typically, all the instances of Oracle RAC will be listening on the same TNS port number. If this is not the case, the port numbers for the other instances should be specified in the default port list in the Application Setup page. For example, if SID1 is listening on TNS port LP1, and SID2

is listening on TNS port LP2, then it is possible to automatically discover SID2, provided that TNS port LP2 is part of the default port list in the Application Setup page.

To discover Oracle RAC:

1. Install the CIM extension on each node in the cluster.
2. If the cluster is not automatically discovered by the management server, create the cluster using Cluster Manager. For more information about Cluster Manager, see "Host and Application Clustering" on page 341.
3. Create the APPIQ_USER account on any one node in the cluster. See "Step A — Create the APPIQ_USER Account for Oracle" on page 304.
4. Discover the host for the first node in HP SIM. See "Step A — Set Up Discovery for Hosts" on page 299.
5. Discover the first Oracle node as follows:
   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. Select a target, and click **Run Now**.

   2. Click the **Create** button for the Database Information table.
   3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Oracle.

      In the **Management IP/DNS Name** box, enter 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` (on Windows)

      `$ORACLE_HOME/network/admin/listener.ora` (on UNIX platforms)

   4. In the **Server Name** box, enter the Oracle System Identifier (SID) of the Oracle database you want to monitor.
   5. In the **Port Number** box, enter 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.

      Microsoft Windows:

```
%ORA_HOME%\network\admin\listener.ora
```

      Unix Platforms:

```
$ORACLE_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))
      )
    )
  )
```

f. Select **ORACLE** from the Database Type menu.

g. Click **OK**.

6. If the conditions described in the "Discovery of Oracle RAC Instances Using One Instance" section are satisfied, then all the other instances in the Oracle RAC will also be discovered, and the Oracle RAC application cluster will also be constructed by the management server.
7. If the other instances of the Oracle RAC are not discovered in the previous step, repeat steps 4 and 5 for each node in the cluster.

About Discovery of an Oracle RAC Application Cluster on a Host Cluster Discovered Using Cluster Manager

When the underlying host cluster is not discovered, the management server will be "Oracle RAC safe," but not fully "Oracle RAC aware." Each instance will show up as a standalone Oracle application, and data will be collected for each instance separately (even though both instances will return identical capacity data). However, the management server does not explicitly identify and construct the Oracle RAC application cluster. Also, when the underlying host cluster is not discovered, other instances of the Oracle RAC cannot be discovered automatically as described in the Discovery of Oracle RAC Instances Using One Instance section.

However, if you create the host cluster at a later point in time, subsequent discovery of any instance in Oracle RAC will identify and construct the Oracle RAC application cluster. The management server will shift to "Oracle RAC aware" mode on top of the host cluster that you created.

Deleting Oracle Application Information

If you do not want the management server to monitor an Oracle 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. See the documentation for HP Systems Insight Manager. Select a target, and then, click **Run Now**.

2. In the Database Information table, click the 🗑 button, corresponding to the Oracle Application instance you do not want the management server to monitor.
3. Perform Discovery Data Collection to make the management server aware of your changes.

Monitoring Microsoft SQL Server

NOTE: If you are planning to monitor Microsoft SQL Server clusters, see "Monitoring Microsoft SQL Server Clusters" on page 318

To manage and monitor Microsoft SQL Servers, you must do the following:

- "Step A — Create the appiq_user Account for the Microsoft SQL Server" on page 313
- "Step B — Provide the Microsoft SQL Server Name and Port Number" on page 316

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 312.

Switching to Mixed Mode Authentication

IMPORTANT: Do not make security changes to your Microsoft SQL Server installation unless you are familiar with the security requirements of your site.

Microsoft SQL Server must be running in Mixed Mode Authentication. You can switch to Mixed Mode Authentication as follows:

Microsoft SQL Server 2000:

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 and select **Properties**.

   The SQL Server Properties (Configure) window appears.
4. Click the **Security** tab.
5. For "Authentication," select **SQL Server and Windows**.
6. If the SQL instance is a clustered instance, make sure that the Startup Service Account is that of a Domain Administrator account. If the SQL instance is not clustered, make sure that the Startup Service Account is that of System Account.

Microsoft SQL Server 2005:

1. Open SQL Server Management Studio (**Start Menu > Programs > Microsoft SQL Server 2005 > SQLServer Management Studio**).
2. Connect to the Microsoft SQL Server 2005 instance.
3. Right-click the server name and select **Properties**. The SQL Server Properties (Configure) window is displayed.
4. Select **Security**.

5. For “Server Authentication,” select **SQL Server and Windows Authentication Mode**, and then click **OK**. You may be prompted to restart the SQL server.
6. Open SQL Server Configuration Manager (**Start Menu > Programs > Microsoft SQL Server 2005 > SQLServer Configuration Manager**). Make sure that the SQL instance is logged on with a Domain Administrator account if it is a clustered instance and System Account if it is a non-clustered instance.

Step A — Create the appiq_user Account for the Microsoft SQL Server

Microsoft SQL Server 2000:

The management server accesses Microsoft SQL Server through the appiq_user account. This account is created when you run the `CreateSQLServerAct.bat` or `CreateSQLServerActCustom.bat` script on the computer running the Microsoft SQL Server database you want to monitor. This account has create session and select dictionary privileges, which allow the management server to view statistics for the Microsoft SQL Server.

NOTE: For more information about creating the appiq_user account with a custom password, see ”Creating Custom Passwords on Managed Database Instances” on page 303.

Keep in mind the following:

- The script must run under the SA user account. To verify that the SA account is enabled, launch SQL Server’s Query Analyzer tool and attempt to connect to the database as SA with the SA user’s password.
- Obtain the SQL Server name before you run the script
- 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 Microsoft SQL Server:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions 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. In a new command window, run the `CreateSQLServerAct.bat` script on the computer with the SQL Server database.

   NOTE: You can use a remote SQL Server isql to run this script.

4. The script prompts you for the name of the Microsoft SQL Server on which to create the appiq_user account. If you are creating the account on a default instance, enter the host name

if the instance is non-clustered and the SQLNetwork Name if the instance is clustered. If you are creating the account on a named instance, enter the host name and the instance name as follows:

For a non-clustered instance:

<Host Name>\<Instance Name>

For a clustered instance:

<SQL Network Name>\<Instance Name>

5. If you are running the `CreateSQLServerActCustom.bat` script, you will be prompted for a password for the appiq_user account. Provide a password that meets the password policy criteria described in "Creating Custom Passwords on Managed Database Instances" on page 303. If you are running the `CreateSQLServerAct.bat` script, the default password (`password`) is automatically used.
6. The script prompts you for the SA user password. Enter the password.

   The appiq_user account is created.
7. To determine if the appiq_user account was added correctly to your Microsoft SQL server:
   a. Open SQL Server Enterprise Manager.
   b. Expand the user interface for SQL Server Enterprise Manager, then expand the specific SQL Server and select **Security**.
   c. Double-click **Logins** and view the list of users authorized to access the SQL Server.
   d. Click the refresh button in SQL Server Enterprise Manager. If the appiq_user is not listed, the management server is not able to discover the database.
8. To determine if the SQL Server is ready to accept connections from the management server:
   a. Connect to the SQL Server installation through Query Analyzer using the account `appiq_user` and the password `password`.
   b. Create a sample ODBC datasource for the SQL Server installation using the appiq_user account.
   c. Click the **Test** button to test the datasource.
9. Repeat these steps for each Microsoft SQL Server 2000 instance you want to manage.

Microsoft SQL Server 2005:

The management server accesses Microsoft SQL Server through the appiq_user account. To create this account, run the `CreateSQLServerActCustomPwd.bat` script on the computer running the Microsoft SQL Server database you want to monitor. This account has create session and select dictionary privileges, which allow the management server to view statistics for the Microsoft SQL Server.

Keep in mind the following:

- The script must run under the SA user account. To verify that the SA account is enabled, launch SQL Server's Query Analyzer tool and attempt to connect to the database as SA with the SA user's password.
- Obtain the SQL Server name before you run the script
- 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 Microsoft SQL Server:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions 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. In a new command window, run the `CreateSQLServerActCustomPwd.bat` script on the computer with the SQL Server database.

   > **NOTE:** You can use a remote SQL Server isql to run this script.

4. The script prompts you for the name of the SQL Server on which to create the appiq_user account. If you are creating the account on a default instance, enter the host name if the instance is non-clustered and the SQLNetwork Name if the instance is clustered. If you are creating the account on a named instance, enter the host name and the instance name as follows:

   For a non-clustered instance:

   <Host Name>\<Instance Name>

   For a clustered instance:

   <SQL Network Name>\<Instance Name>
5. The script prompts you for the password for the appiq_user account. Provide a password that meets the password policy criteria described in "Creating Custom Passwords on Managed Database Instances" on page 303.
6. The script prompts you for the SA user password. Enter the password.

   The appiq_user account is created.
7. To determine if appiq_user was added correctly to your SQL server:
   - **a.** Open SQL Server Management Studio.
   - **b.** Expand the user interface for SQL Server Management Studio, and then expand the specific SQL Server and select **Security**.
   - **c.** Double-click **Logins** and view the list of users authorized to access the SQL Server.
   - **d.** Click the Refresh button in SQL Server Management Studio. If the appiq_user is not listed, the management server is not able to discover the database.
8. To determine if the SQL Server is ready to accept connections from the management server:
   - **a.** Connect to the SQL Server installation through SQL Server Management Studio using the appiq_user account and the password specified earlier.

b. Create a sample ODBC datasource for the SQL Server installation using the appiq_user account.

c. Click the **Test** button to test the datasource.

9. Repeat these steps for each Microsoft SQL Server 2005 instance you want to manage.

Step B — Provide the Microsoft SQL Server Name and Port Number

The server name for the Microsoft SQL Server and port number for managing a SQL database must be provided in the following steps:

IMPORTANT: If you have name resolutions issues, your server may be discovered; however, your applications will not be discovered. You can address the name resolution issues by adding entries within the hosts file on the management server for the systems in question.

When configuring the System Application Discovery Settings for SQL servers, the following needs to be specified as described in the steps within this section:

- **Host IP/DNS Name**: <IP Address>
- **Database Server**: <SQL Server Name>
- **Port Number**: <SQL Port #>
- **Database Type**: SQLSERVER

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. See the documentation for HP Systems Insight Manager. Select a target, and then, click **Run Now**.

2. Click the **Create** button for the Database Information table.

3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Microsoft SQL Server. You must provide the host name. You cannot use localhost or parenthesis.

4. You can leave the **Management IP/DNS Name** box blank. This box is for Oracle clusters. When you leave the **Management IP/DNS Name** box 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.

5. In the Database Server box, enter the SQL database server name you want to monitor.

   The SQL Server name is either the Windows system name (default) or the name specified when the SQL server was installed. It is one of the following:

   - The name specified at the time the SQL server was installed
   - The Windows system name (Windows 2000)
   - The local name (Windows 2003)

   For example, if a Windows 2003 server called SQLTEST has an IP address of 192.168.2.10 with the default SQL port (1433) and shows the name of (local) within SQL Enterprise

Manager/SQL Server Management Studio, the correct system application discovery settings on the management server would be the following:

- **Host IP/DNS Name**: 192.168.2.10
- **Database Server**: SQLTEST
- **Port Number**: 1433
- **Database Type**: SQLSERVER

6. In the **Port Number** box, enter the port that SQL is using.

   To determine the correct SQL Port Number that the SQL Server is using, follow these steps:

   Microsoft SQL Server 2000

   a. Open SQL Server Enterprise Manager.

   b. Expand the user interface for SQL Server Enterprise Manager, and then select the specific SQL server. Right-click and then select **Properties** from the menu.

   c. Click the **Network Configurations** button. On the General Tab, select the TCP/IP entry under the Enabled Protocols section, then click the **Properties** button.

   d. The resulting window shows you the TCP/IP port your SQL server uses. Provide this port number in the **Port Number** box on the management server.

   Microsoft SQL Server 2005

   a. Open SQL Server Configuration Manager.

   b. Select the specific SQL Server 2005 Network Configuration entry for the SQL Server 2005 instance.

   c. Select the TCP/IP entry on the right pane, and then click the Properties right click menu.

   d. From the IP Addresses tab, obtain the Port Number configured for the instance. Provide this port number in the Port Number box on the management server.

7. Select **SQLSERVER** from the Database Type menu.
8. Click **OK**.

IMPORTANT: Perform Discovery Data Collection for your inputs to take effect. See "Step 3 — Discovering Applications" on page 335.

Removing the appiq_user Account for Microsoft 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 from the Microsoft SQL Server databases on a host:

1. To run the script on Microsoft Windows, go to the `DBIQ\sqlserver\win` directory on the CIM Extensions CD-ROM.

IMPORTANT: You must complete the following steps.

2. Verify you have the password to the server administrator user account.

   You are prompted for the password for this user account when you run the script.
3. Run the `DropSQLServerAct.bat` script on Microsoft Windows on the computer with the SQL Server database.
4. Enter the name of the SQL Server server.
5. Enter the password for the server administrator account.

   The account for appiq_user is removed. The management server can no longer monitor the SQL Server databases on this host.

Deleting Microsoft SQL Server Information

If you do not want the management server to monitor a Microsoft 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. See the documentation for HP Systems Insight Manager. Select a target, and then, click **Run Now**.
2. In the Database Information table, click the 🗑 button, corresponding to the SQL Server instance you do not want the management server to monitor.
3. Perform Discovery Data Collection to make the management server aware of your changes.

Monitoring Microsoft SQL Server Clusters

IMPORTANT: Make sure the Microsoft SQL Server cluster database is in “Mixed Mode authentication.” To switch to mixed mode authentication, see ”Switching to Mixed Mode Authentication” on page 312.

To monitor and manage Microsoft SQL Server clusters:

1. Install CIM Extensions on each of the participating nodes.
2. Create the appiq_user account as described in ”Step A — Create the appiq_user Account for the Microsoft SQL Server” on page 313.

   NOTE: This step needs to be run on any one of the participating host nodes of the Microsoft SQL Server cluster.
3. Enter the server name and port number as described in ”Provide the Microsoft SQL Server Name and Port Number for a Cluster” on page 319.

Provide the Microsoft SQL Server Name and Port Number for a Cluster

The server name for the Microsoft SQL Server and port number for managing a Microsoft SQL Server cluster database must be provided in the following steps:

IMPORTANT: If you have name resolutions issues, your server may be discovered; however, your applications will not be discovered. You can address the name resolution issues by adding entries within the hosts file on the management server for the systems in question.

When configuring the System Application Discovery Settings for SQL servers, the following needs to be specified as described in the steps within this section:

- **Host IP/DNS Name**: <IP Address>
- **Database Server**: <SQL Server Name>
- **Port Number**: <SQL Port #>
- **Database Type**: SQLSERVER

To add information for discovering a Microsoft SQL Server cluster:

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. See the documentation for HP Systems Insight Manager. Select a target, and then, click **Run Now**.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of at least one of the participating host nodes running Microsoft SQL Server cluster. You must provide the host name. You cannot use localhost or parenthesis.
4. You can leave the Management IP/DNS Name box blank. When you leave the Management IP/DNS Name box 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.
5. In the Database Server box, enter the SQL database server name you want to monitor.

   The SQL Server name would be one of the following:

   - The name specified at the time the SQL server was installed
   - The Microsoft SQL Network Name (the default instance)

   For example, if a Microsoft SQL Server cluster instance called SQLCLUSTER is running on a 2 node Windows 2003 cluster (individual host node IP address being 192.168.2.10 and 192.168.2.11) at the default SQL port (1433) and shows the name of Microsoft SQL Network Name within SQL Enterprise Manager / SQL Server Management Studio, the correct system application discovery settings on the management server would be either of the following:

   - **Host IP/DNS Name**: 192.168.2.10
   - **Database Server**: SQLCLUSTER
   - **Port Number**: 1433

- **Database Type**: SQLSERVER

Or

- **Host IP/DNS Name**: 192.168.2.11
- **Database Server**: SQLCLUSTER
- **Port Number**: 1433
- **Database Type**: SQLSERVER

6. In the **Port Number** box, enter the port that SQL is using.

   To determine the correct SQL Port Number that the SQL Server is using, follow these steps:

   Microsoft SQL Server 2000 Cluster

   a. Open SQL Server Enterprise Manager.
   b. Expand the user interface for SQL Server Enterprise Manager, and then select the specific SQL server. Right-click and then select **Properties** from the menu.
   c. Click the **Network Configurations** button. On the General Tab, select the TCP/IP entry under the Enabled Protocols section, then click the **Properties** button.
   d. The resulting window shows you the TCP/IP port your SQL server uses. Provide this port number in the **Port Number** box on the management server.

   Microsoft SQL Server 2005 Cluster

   a. Open SQL Server Configuration Manager.
   b. Select the specific SQL Server 2005 Network Configuration entry for the SQL Server 2005 instance.
   c. Select the TCP/IP entry on the right pane, and then click the Properties right click menu.
   d. From the IP Addresses tab, obtain the Port Number configured for the instance. Provide this port number in the Port Number box on the management server. If Dynamic Ports are used, the Port Number is located under IPAll > TCP Dynamic Ports.
7. Select **SQLSERVER** from the Database Type menu.
8. Click **OK**.

IMPORTANT: Perform Discovery Data Collection for your inputs to take effect. See "Step 3 — Discovering Applications" on page 335.

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 Sybase IQ, which is 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 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.

NOTE: To create the APPIQ_USER with a custom password, run `CreateSybaseActCustomPwd.bat`. For more information, see "Creating Custom Passwords on Managed Database Instances" on page 303.

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 CIM Extensions 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 CIM Extensions 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 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. Enter 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 the computer with the Sybase database.
4. Enter the name of the Sybase server.
5. Enter 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. See the documentation for HP Systems Insight Manager. Select a target, and then, click **Run Now**.
2. Click the **Create** button for the Database Information table.
3. In the **Host IP/DNS Name** box, enter the IP address or DNS name of the host running Sybase.
4. You can leave the **Management IP/DNS Name** box blank. This box is for Oracle clusters. When you leave the **Management IP/DNS Name** box 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.
5. In the **Server Name** box, enter the Sybase database you want to monitor.
6. In the **Port Number** box, enter the port that Sybase is using.
7. Select **SYBASE** from the Database Type menu.
8. Click **OK**.

IMPORTANT: Perform Discovery Data Collection for your inputs to take effect. See "Step 3 — Discovering Applications" on page 335.

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. See the documentation for HP Systems Insight Manager. Select a target, and then, click **Run Now**.
2. In the Database Information table, click the 🗑 button, corresponding to the Sybase instance you do not want the management server to monitor.
3. Perform Discovery Data Collection to make the management server aware of your changes.

Monitoring Microsoft Exchange

NOTE: If you are planning to monitor Microsoft Exchange Clusters, see "Monitoring Microsoft Exchange Failover Clusters" on page 325.

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 ("Step 3 — Discovering Applications" on page 335).

Adding Microsoft Exchange Domain Controller Access

Before adding a domain controller, note the following:

- The hosts should recognize the management server by name, because a reverse look-up is required by both operating system security and Microsoft Exchange. Make sure the domain controller, Exchange server host, and management server are accessible to one other using the host name and the fully-qualified domain name.
- The user name you provide must be the Common Name (CN) of the Active Directory User for accessing the Microsoft Exchange server. If you enter the Windows user name and it is different from the CN, the management server will not discover the Exchange instance.

  To find the CN for a user on a domain controller server:

  a. Install the ADSIEdit MMC snap-in if it is not installed.

  b. Select **Start > Run** and enter `adsiedit.msc`.

  c. When the snap-in opens, expand the DOMAIN directory and navigate to the **CN=Users** folder to see the CN for each user in the Active Directory.

To provide information about your domain controllers:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **Global Application Discovery Settings**.
2. In the Exchange Information section, click **Create**.
3. Click the **Add New Domain Controller** link.

   a. In the Domain box, enter the domain name.

   b. In the Domain Controller Name box, enter the fully qualified DNS name for the domain controller.

   c. In the User Common Name box, enter the Common Name (CN) of the Active Directory User for accessing the Microsoft Exchange server.

   d. In the Domain Password box, enter the corresponding password for accessing the Microsoft Exchange server.

   e. In the Verify Password box, re-enter the password for verification.
4. Click **Add**.

   The domain controller is added to the table.
5. Click **OK**.
6. Repeat these steps for each domain controller.
7. When all of your domain controllers are added, run `wmiadap /f` on the Exchange Server to refresh the Exchange data.

IMPORTANT: You must discover the host running Microsoft Exchange. See "Step 3 — Discovering Applications" on page 335.

Editing a Microsoft Exchange Domain Controller

To provide information about your domain controllers:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **Global Application Discovery Settings**.
2. Click the **Edit** button next to the Exchange domain controller you want to edit.
3. Enter a new User Common Name or Domain Password.
4. Click **Edit**.

   The domain controller updates are added to the table.

   Click **OK**.

Deleting a Microsoft Exchange Domain Controller

To delete all of the domain controllers of a particular domain:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **Global Application Discovery Settings**.
2. Click the **Delete** (🗑) button corresponding to the domain you want to remove.
3. Run Discovery Data Collection for your changes to take effect.

To delete a particular domain controller in a domain:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **Global Application Discovery Settings**.
2. Identify the domain for the domain controller you want to remove, and click the **Edit** (📝) button corresponding to that domain.
3. In the Edit window, click the **Delete** (🗑) button corresponding to the domain controller you want to remove.
4. Run Discovery Data Collection for your changes to take effect.

Monitoring Microsoft Exchange Failover Clusters

To monitor and manage Microsoft Exchange Failover Clusters:

1. Install CIM Extensions on each of the participating nodes of Microsoft Exchange Failover Cluster.
2. Add information for Microsoft Exchange Domain Controller Access. See "Adding Microsoft Exchange Domain Controller Access" on page 324.
3. Perform Discovery Data Collection on each of the participating nodes of the Exchange Cluster.

Monitoring Caché

To monitor Caché, you must do the following:

- "Step A — Import the Wrapper Class Definitions into the Caché Instance" on page 326
- "Step B — Create APPIQ_USER Account on the Caché Instance" on page 330

- ”Step C — Provide the Caché Instance Name and Port Number” on page 334

After you complete these steps, you must discover Caché. See ”Step 3 — Discovering Applications” on page 335.

NOTE: The required drivers for Caché were automatically installed along with the management server.

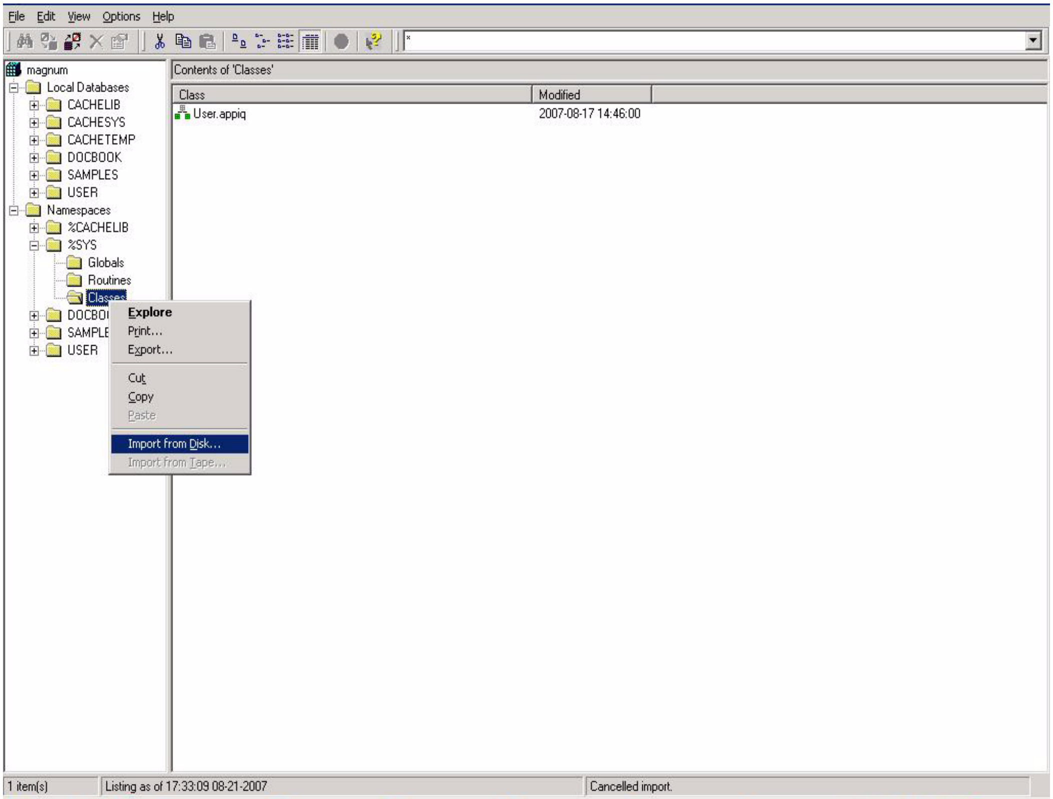
IMPORTANT: Before you begin these steps, make sure you purchased Caché IQ, which is the module that lets you monitor Caché. Contact your customer support if you are unsure if you purchased this module.

Step A — Import the Wrapper Class Definitions into the Caché Instance

To import the wrapper classes:

For Caché 5.0 (5.0.20 onwards)

1. Launch the Caché Explorer by right-clicking the Caché Cube icon in the system tray area of the Windows toolbar and selecting **Explorer**.
2. Right click the **Classes** folder located at **Namespaces > “%SYS” > Classes**.
3. Select **Import from disk**.



Class	Modified
User.appiq	2007-08-17 14:46:00

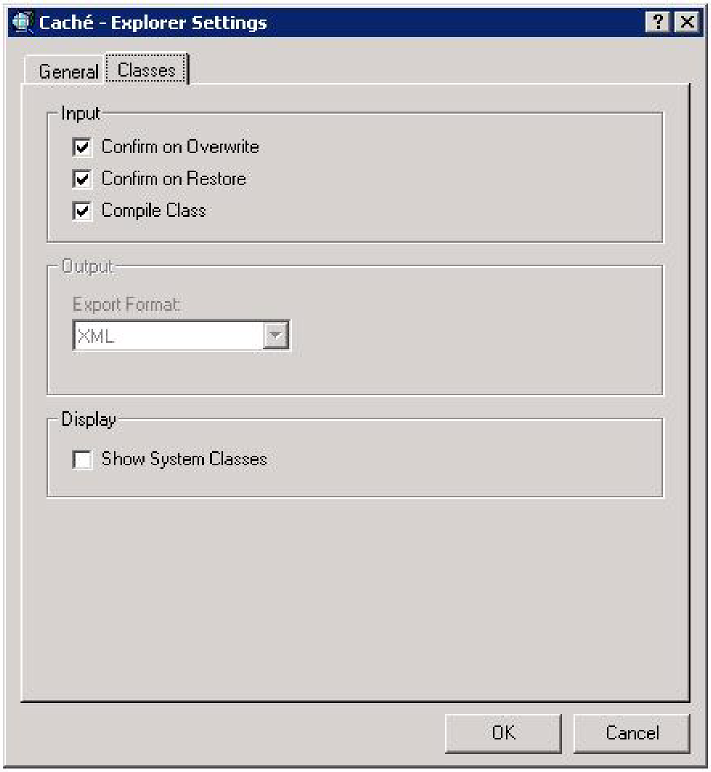
1 item(s) | Listing as of 17:33:09 08-21-2007 | Cancelled import.

Figure 15 Selecting Import from Disk

4. Browse the CIM Extension CD, select the wrapper xml file, and click **Open**.

- On IBM AIX, Linux, or HP-UX, log into an account that has administrative privileges, and mount the CIM Extensions CD-ROM (if not auto-mounted). The wrapper file is `/cdrom/DBIQ/cachedb/unix/cachedb50_sqlprojs.xml`

  where `/cdrom` is the name of the directory where you mounted the CD-ROM
- On Microsoft Windows, the wrapper file on the CIM Extensions CD-ROM is `\DBIQ\cachedb\win\cachedb50_sqlprojs.xml`.
- When the Import Classes windows is displayed, click **Options**.
- Select the **Classes** tab, enable the **Compile Class** checkbox, and click **OK**.



Caché - Explorer Settings

Input

☑ Confirm on Overwrite

☑ Confirm on Restore

☑ Compile Class

Output

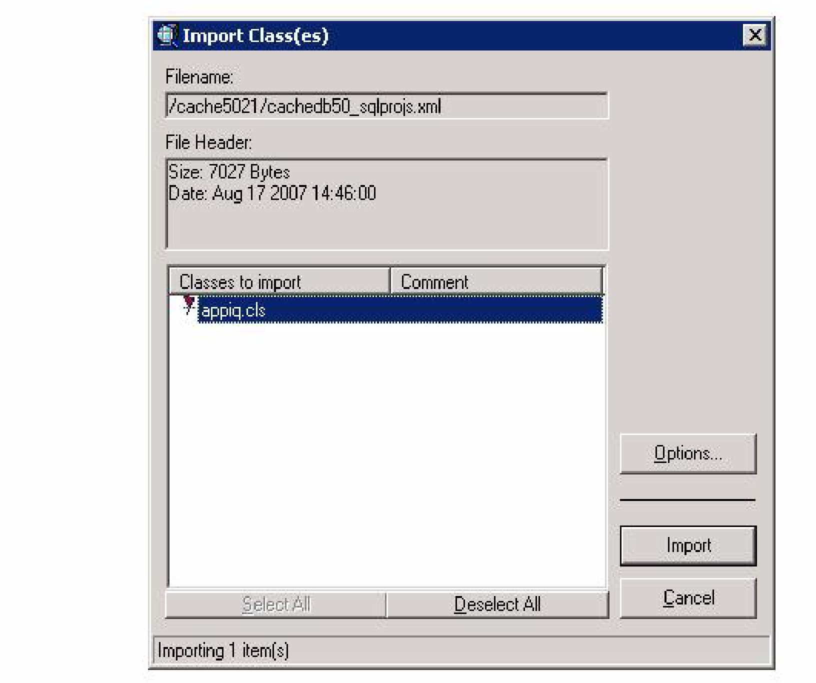
Export Format: XML

Display

□ Show System Classes

Figure 16 Enabling Compile Class

5. In the Import Classes pop-up window, select `appiq.cls`, and click **Import**.



Import Class(es)

Filename:
/cache5021/cachedb50_sqlprojs.xml

File Header:
Size: 7027 Bytes
Date: Aug 17 2007 14:46:00

Classes to import	Comment
appiq.cls	

Importing 1 item(s)

Figure 17 Selecting appiq.cls

For Caché 5.2 and Caché 2007.1

1. Launch the Caché System Management Portal by right-clicking the Caché Cube icon in the system tray area of the Windows toolbar and selecting **System Management Portal**.
2. Click the **Classes** link under Data Management.
3. On the Classes page, select the **Namespaces** radio button, and then select **%SYS**.
4. Click **Import**.
5. Browse the CIM Extension CD, select the wrapper xml file, and click **Open**.
   - On IBM AIX, Linux, or HP-UX, log into an account that has administrative privileges, and mount the CIM Extensions CD-ROM (if not auto-mounted). The wrapper file is `/cdrom/DBIQ/cachedb/unix/cachedb_sqlprojs.xml`

     where `/cdrom` is the name of the directory where you mounted the CD-ROM
   - On Microsoft Windows, the wrapper file on the CIM Extensions CD-ROM is `\DBIQ\cachedb\win\`cachedb_sqlprojs.xml.
   - On OpenVMS:

   a. Log in as system and mount the CIM Extensions CD-ROM.

   b. Copy the wrapper file (for example: `DQB0:[OVMS.DBIQ.CACHE] SQLPROJS.XML`), where `DQB0` is the CD-ROM drive, to any internal location on the OpenVMS host.

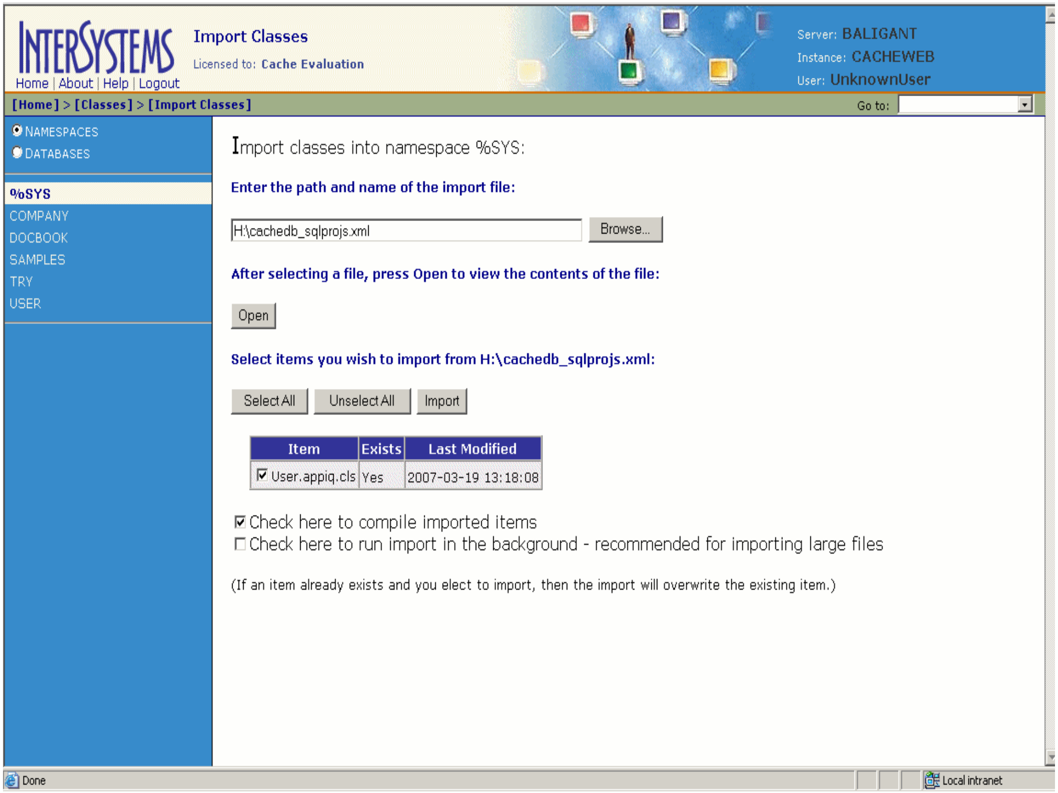
   For example, copy `$DQB0:[OVMS.DBIQ.CACHE]SQLPROJS.XML $DKA0:[000000]SQLPROJS.XML` where DKA0 is a local drive on the OpenVMS host.

c. Browse to $DKA0 and specify SQLPROJS.XML within $DKA0 as the import file.

6. After the file is opened, click **Select All**.
7. Select **Check here to compile imported items**, and click **Import**.

   The wrapper class definitions are imported into the Caché %SYS namespace.

   The following image shows an example of importing the wrapper class definitions:



Licensed to: Cache Evaluation

Server: BALIGANT
Instance: CACHEWEB
User: UnknownUser

Import classes into namespace %SYS:

Enter the path and name of the import file:

H:\cachedb_sqlprojs.xml

After selecting a file, press Open to view the contents of the file:

Select items you wish to import from H:\cachedb_sqlprojs.xml:

Item	Exists	Last Modified
☑ User.appiq.cls	Yes	2007-03-19 13:18:08

☑ Check here to compile imported items
☐ Check here to run import in the background - recommended for importing large files

(If an item already exists and you elect to import, then the import will overwrite the existing item.)

Figure 18 Importing Wrapper Class Definitions

Step B — Create APPIQ_USER Account on the Caché Instance

The management server accesses Caché through the APPIQ_USER account. This account is created when you run the appropriate script (described below) on the computer running the Caché database you want to monitor. You can execute these scripts from the management server also.

This script creates APPIQROLE with execute permissions for the SQL projections imported into the Caché managed instance, creates an APPIQ_USER account, and assigns APPIQROLE to APPIQ_USER.

The script must run as the _SYSTEM user. You should enter the Caché server name, the Super Server port number, and the password of the _SYSTEM user account as arguments for the script.

NOTE: If you are running Caché 5.2 or later, and the Caché instance was installed using "Locked Down" security mode, see "Locked Down Security Mode" on page 332 before creating the APPIQ_USER account.

To create APPIQ_USER for the Caché instance:

1. Do one of the following:

   To create APPIQ_USER on the host:

   - To run the script on IBM AIX, HP_UX, or Linux, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the `/DBIQ/cachedb/unix` directory by entering the following:

     ```
     # cd /cdrom/DBIQ/cachedb/unix
     ```

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

   - To run the script on Microsoft Windows, go to the `DBIQ\cachedb\win` directory on the CD-ROM.
   - To run the script on OpenVMS, log in as system, mount the CD-ROM drive, and go to the `[OVMS.DBIQ.CACHE]` directory by entering the following:

     ```
     SET DEF DQB0:[OVMS.DBIQ.CACHE]
     ```

     Where `DQB0` is the name of the CD-ROM drive.

   To remotely create APPIQ_USER on the Caché instance from the management server:

   - To run the script on Linux, go to the `/opt/<product name>/install/cachedb/unix` directory by entering the following:

     ```
     # cd opt/<product name>/install/cachedb/unix
     ```

   - To run the script on Windows, go to the `%MGR_DIST%\install\cachedb\win` directory

2. Verify you have the password to the _SYSTEM user account.
3. For Caché 5.0: run `createCacheDB50User.bat` (on Windows) or `createCacheDB50User.sh` (on UNIX platforms) on the computer with the CacheDatabase. To specify a custom password for the APPIQ_USER account, run `createCacheDB50UserCustomPwd.bat` (on Windows) or `createCacheDB50UserCustomPwd.sh` (on UNIX platforms) on the computer with the CacheDatabase.

   For later versions of Caché: run `createCacheDBUser.bat` (on Windows) or `createCacheDBUser.sh` (on UNIX platforms) or `CRUSER.COM` (on OpenVMS) on the computer with the CacheDatabase. To specify a custom password for the APPIQ_USER account, run `createCacheDBUserCustomPwd.bat` (on Windows) or `createCacheDBUserCustomPwd.sh` (on UNIX platforms) or `CUSTUSER.COM` (on OpenVMS) on the computer with the CacheDatabase.
4. Enter the Caché server name, the Super Server port number and the password of the _SYSTEM user account as arguments for the script. If you are running the custom password creation script,

enter the custom password as the fourth argument.

When invoking the scripts on OpenVMS, enclose the arguments in double quotes:

```
$ @CRUSER.COM "<host name>" "<super server port>" "<password for _SYSTEM
user>"
```

5. Repeat the previous step for each Caché instance you want to manage.

Locked Down Security Mode

For Caché 5.2 and later versions, if the Caché instance was installed using “Locked Down” security mode, the following steps must be carried out before creating the APPIQ_USER account:

1. Launch the System Management Portal.
2. Click the **Security Management** link under System Administration.
3. On the Security Management page, click **Services**.
4. Click **%Service_Bindings** on the Services page.
5. On the Edit definition for Service %Service_Bindings page:
   a. Under Allowed Incoming Connections, click **Add** and enter the IP address of the management server in the Explorer User Prompt window.
   b. If the create APPIQ_USER scripts are being executed from the host on which Caché instance is running, add the IP address of the host.
   c. Click the **Service Enabled** checkbox on the Edit definition for Service %Service_Bindings page.
   d. Click **Save**.
6. Click the **Security Management** link under System Administration in the System Management portal.
7. On the Security Management page, click the **Users** link .
8. Click the **Edit** link for _SYSTEM user.
9. On the Edit Definition for User _SYSTEM page, click the **User Enabled** checkbox and enter a password for the _SYSTEM user in the Password and Confirm Password boxes.
10. Click the **Save** button.

    Once the APPIQ_USER has been created, the _SYSTEM user can be disabled from the System Management portal.

Removing the APPIQ_USER Account from the Caché Instance

If you no longer want the management server to monitor a Caché instance, you can remove the APPIQ_USER account and APPIQROLE for that Caché instance by running `dropCacheDBUser.bat` (on Windows) or `dropCacheDBUser.sh` (on UNIX platforms) or `DROPUSER.COM` (on OpenVMS).

Before you remove the APPIQ_USER account from the Caché instances on a host, make sure no processes are running APPIQ_USER for that Caché instance. The management server uses APPIQ_USER to obtain information about a Caché instance.

For Caché 5.2 and later versions, if the Caché instance was installed using "Locked Down" security mode, ensure that the _SYSTEM user has been enabled before trying to remove the APPIQ_USER account. To ensure that the _SYSTEM user has been enabled:

1. Launch the System Management Portal
2. Click the **Security Management** link under System Administration.
3. On the Security Management page, click the **Users** link.
4. Click the **Edit** link for _SYSTEM user.
5. On the Edit Definition for User _SYSTEM page, click the **User Enabled** checkbox and enter a password for the _SYSTEM user in the Password and Confirm Password fields.
6. Click **Save**.

   Once the APPIQ_USER has been removed, the _SYSTEM user can be disabled from the System Management portal. The %Service_Bindings service that was enabled before creating the APPIQ_USER can also be disabled.

To remove the APPIQ_USER account:

1. Do one of the following:

   To remove the APPIQ_USER account from the host:

   - To run the script on IBM AIX, HP_UX, or Linux, log into an account that has administrative privileges, mount the CD-ROM (if not auto-mounted), and go to the `/DBIQ/cachedb/unix` directory by entering the following:

     ```
     # cd /cdrom/DBIQ/cachedb/unix
     ```

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

   - To run the script on Microsoft Windows, go to the `DBIQ\cachedb\win` directory on the CD-ROM.
   - To run the script on OpenVMS, log in as system, mount the CD-ROM drive, and go to the `[OVMS.DBIQ.CACHE]` directory by entering the following :

     ```
     SET DEF DQB0:[OVMS.DBIQ.CACHE]
     ```

     Where `DQB0` is the name of the CD-ROM drive.

   To remotely remove the APPIQ_USER account from the Caché instance from the management server:

   - To run the script on Linux, go to the `/opt/<product name>/install/cachedb/unix` directory by entering the following:

     ```
     # cd opt/<product name>/install/cachedb/unix
     ```

   - To run the script on Windows, go to the `%MGR_DIST%\install\cachedb\win` directory
2. Verify you have the password to the _SYSTEM user account.
3. For Caché 5.0, run `dropCacheDB50User.bat` (on Windows) or `dropCacheDB50User.sh` (on UNIX platforms) on the computer with the CacheDatabase. For later versions of Caché, run `dropCacheDBUser.bat` (on Windows) or `dropCacheDBUser.sh` (on UNIX platforms), or `DROPUSER.COM` (on OpenVMS) on the computer with the CacheDatabase.

4. Enter the Caché server name, the Super Server port number and the password of the _SYSTEM user account as arguments for the script.

   When invoking the scripts on OpenVMS, enclose the arguments in double quotes:

   ```
   $ @DROPUSER.COM "<host name>" "<super server port>" "<password for _SYSTEM
   user>
   ```
5. Repeat the previous step for each Caché instance you want to manage.

After deleting the APPIQ_USER account from the Caché instance, you can also delete the wrapper class definitions.

For Caché 5.0 (5.0.20 onwards)

1. Launch the Caché Explorer.
2. Click the Classes folder located at **Namespaces > "%SYS" > Classes**. Right-click the `User.appiq` class, and select **Delete**.
3. The Confirm Deletion window displays. Click **Yes**.

For Caché 5.2 and Caché 2007.1

1. Launch the Caché System Management Portal.
2. Click the **Classes** link under Data Management.
3. On the Classes page, select the Namespaces radio button, and then click **%SYS**.
4. Click **Delete**.
5. Enter `User.appiq.cls` in the Enter search mask box, and click **Search**.
6. Select `User.appiq.cls`, and click **Delete**.

Step C — Provide the Caché Instance Name and Port Number

To provide the Caché instance name and SuperServer port number for managing the Caché instance:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **System Application Discovery Settings**, select a target, and click **Run Now**.

   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. See the documentation for HP Systems Insight Manager.
2. Click the **Create** button for the Database Information table.
3. In the Host IP/DNS Name box, enter the IP address or DNS name of the host running Caché.
4. You can leave the Management IP/DNS Name box blank. This box is for clusters. When you leave the Management IP/DNS Name box 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.
5. In the Database Server box, enter the Caché instance name you want to monitor.
6. In the Port Number box, enter the SuperServer port that Caché is using.
7. Select **Cache** from the Database Type menu.

8. Click **OK**.

IMPORTANT: Perform Discovery Data Collection for your inputs to take effect. See "Step 3 — Discovering Applications" on page 335.

Deleting Caché Information

If you do not want the management server to monitor a Caché 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. See the documentation for HP Systems Insight Manager. Select a target, and click **Run Now**.
2. In the Database Information table, click the 🗑 button corresponding to the Caché instance you do not want the management server to monitor.
3. Perform Discovery Data Collection to make the management server aware of your changes.

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 Your Applications" on page 335)
- Perform Discovery Data Collection ("Step C — Run Discovery Data Collection" on page 337)

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 302.
- If you used a custom password for the APPIQ_USER account, you must change the password on the Storage Essentials management server before performing Discovery Data Collection. See "Creating Custom Passwords on Managed Database Instances" on page 303.
- Make sure you have reviewed the table, Table 2 on page 2 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.

Step A — Detect Your Applications

If you have not already done so, use HP Systems Insight Manager to discover the hosts running the applications you want to discover. See "Step A — Set Up Discovery for Hosts" on page 299.

To make the software aware of the applications on the network:

1. Click **Tools** > **Storage Essentials** > **Home** > **Discovery** > **Setup**.
2. To start discovering elements on the network, click the **Start Discovery** button on the IP Addresses tab.

   The software discovers the IP addresses selected.

   During discovery, the following occurs:

   - The software changes the status light from green to orange.
   - The Log Messages page is displayed. To view the status of discovery, click **Discovery** > **View Logs**.

   The DISCOVERY COMPLETED message is displayed in the Log Messages box when Discovery is complete.

   Keep in mind the following:

   - 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.
   - If you are having problems discovering an element, see "Troubleshooting Discovery and Discovery Data Collection" on page 395.

Step B — Obtain the Topology

The user interface may load slowly while the topology is being recalculated. It may also take more time to log into the management server during a topology recalculation.

To obtain the topology:

1. Click **Discovery** > **Topology**.

   The discovered elements are selected.
2. Click the **Get Topology** button.

   The management server obtains the topology for selected elements.
3. Select the discovery group from which you want to obtain the topology. If you are obtaining the topology for hosts for the first time, make sure **All Discovery Groups** is selected.

   You can use discovery groups to break up getting the topology or getting details. For example, instead of obtaining the topology for all of the elements, you could specify that the management server gets the topology 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 102.
4. If you see errors in the topology, look at the log messages, which can provide an indication of what went wrong. Look at Event Manager for additional information. Access Event Manager by clicking the Event Manager button in the left pane. To obtain troubleshooting information, see the "Troubleshooting Topology Issues" on page 403.

   If the topology for an element in your network changes, select the element and click **Get Topology** in **Discovery** > **Topology** to updated the information.

The software obtains just enough information about where the element is connected in the topology, for example a switch connected to a host.

Step C — Run Discovery Data Collection

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.
- During Discovery Data Collection the topology is recalculated. While the topology is being recalculated, the loading of the user interface may be slow. It may also take more time to log into the management server during a topology recalculation.
- When you do Discovery Data Collection that includes an AIX host, three SCSI errors (2 FSCSI error and 1 FCS error) per IBM adapter port are displayed in the system log. You can ignore these errors.
- You can quarantine elements to exclude them from Discovery Data Collection. See "Placing an Element in Quarantine" on page 167 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 is unable to obtain information from an element during Discovery Data Collection as a result of a CIM extension failure, 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 167 for information on how to remove an element from quarantine.

To obtain details:

1. Select **Options** > **Storage Essentials** > **Discovery** > **Run Discovery Data Collection**.
2. Select **All Discovery Groups** or click **Select Custom Discovery Groups** to specify a customized list. If you are running Discovery Data Collection for the first time, select **All Discovery Groups**.

   NOTE: For information on selecting a custom discovery list, see "Creating Custom Discovery Lists" on page 163.

3. Click **Get Details**.

   You can view the progress of gathering details by clicking **Tasks & Logs** > **View Storage Essentials Logs**.

   The DISCOVERY COMPLETED message is displayed in the Log Messages box when Discovery is complete.

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.

4. See 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 379.

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** button for the **Oracle Information** table.
3. Enter 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 395 for more information.

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** boxes.

To change the password:

1. Select **Options** > **Protocol Settings** > **Storage Essentials** > **Global Application Discovery Settings**.
2. Click the **Change Password** button.
3. Verify you have already changed the password of the databases listed on this page.

4. Enter a new password in the **Password** box.

   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 (_)

5. Re–enter the password in the **Verify Password** box.
6. Click **OK**.

19 Host and Application Clustering

Some of the features described in this chapter are not included in HP Storage Essentials Standard Edition. To determine which features apply to your product, see the List of Features, which is accessible from the Documentation Center (**Help** > **Documentation Center** in HP Storage Essentials).

This chapter contains the following topics:

About Clustering

The management server provides full support for managing clusters. Cluster support includes the following features:

- Clusters are recognized as managed elements.
- System Manager supports clusters in all areas.
- The element topology shows which shared resources an application instance uses.
- Cluster capacity utilization is accurately reported.
- Capacity utilization trending is provided for applications running on clusters.

The management server supports automatic discovery of several popular cluster servers, and allows management of other clusters through Cluster Manager.

Discovering Clusters

The following cluster services support automatic discovery:

- Microsoft Cluster Services (MSCS) on Windows 2003
- Veritas Clusters on Solaris

Cluster services that don’t support automatic discovery can be discovered manually by using Cluster Manager. See ”Manual Discovery of Host Clusters” on page 342.

The following application clusters are supported:

- Oracle Real Application Clusters (RAC)
- Microsoft Exchange 2000/2003 FailOver Clusters and 2007 Single Copy Cluster (SCC)
- Microsoft SQL Server 2000 and 2005

For information about discovering application clusters, see ”Discovering Applications, Backup Hosts and Hosts” on page 297.

Refer to the support matrix for a complete list of supported configurations. The support matrix is accessible from the Documentation Center (**Help > Documentation Center** in HP Storage Essentials).

Automatic Discovery of Host Clusters

MSCS on Windows 2003 and Veritas Clusters on Solaris support automatic discovery. To discover hosts using either of these cluster services:

1. Discover your hosts and applications as described in "Discovering Applications, Backup Hosts and Hosts" on page 297. The clusters are automatically recognized by the management server.

> **NOTE:** The following optional steps describe how to select a preferred host from which shared resource capacity data will be collected.

2. *Optional*: Access Cluster Manager by right-clicking a cluster in System Manager and selecting Edit Cluster. The Cluster Manager Overview page is displayed. Click **Next**.
3. *Optional*: Cluster Manager Step 2 (Select Preferred Host for Cluster Shared Resources) is displayed. Select a preferred host for each of the cluster shared resources. Keeping the default selection of "None" will result in shared resource capacity data being collected from an available active host that shares the resource. Choosing a particular active host results in the specified host being used for data collection. If the specified host becomes unavailable, an available active host is used for data collection.

   Specify the preferred host for individual cluster shared resources. If a resource is not shared by the preferred host selection, the preferred host menu for that shared resource will continue to display the previous selection.

   When you have finished specifying preferred hosts, click **Finish**.

Manual Discovery of Host Clusters

If you are using a cluster service that doesn't support automatic discovery, you must manually create your clusters. For the list of cluster services that support automatic discovery, see "Discovering Clusters" on page 341.

> **NOTE:** In some environments, using Cluster Manager to manually create a cluster with NetApp hosts may result in unsuccessful or incomplete cluster creation.

To manually discover clusters:

1. Discover your hosts and applications as described in "Discovering Applications, Backup Hosts and Hosts" on page 297.
2. Access Cluster Manager by right-clicking a host in System Manager and selecting **Build Cluster**. The Cluster Manager Overview page is displayed. Click **Next**.
3. Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) is displayed. If you are discovering an HP Serviceguard cluster, this page may already be populated, and you can skip to the next step. If this page isn't already populated, follow these steps to specify the cluster properties and cluster members:
   a. In the Cluster Properties section, specify the cluster name, cluster server, and cluster virtual IP.

b. In the Available Hosts section, select the hosts to add to the Cluster Members table. If desired, use the filter to assist in the selection of hosts. For details about the filtering functionality, see "Filtering Hosts" on page 343.

   You may also use the Select Related Hosts button to facilitate the selection of hosts. Select a host in the table, and click **Select Related Hosts** to automatically select any related hosts.

c. After you have selected the hosts that you would like to add to the cluster, click **Add Selected Hosts to Cluster**. The selected hosts are added to the Cluster Members table.

d. Click **Next**.

4. Cluster Manager Step 3 (Specify Cluster Shared Resources) is displayed. Select **Automatic** or **Manual**. If you select Automatic, click **Display Cluster Shared Resources**, and the table at the bottom of the page is automatically populated.

   If you select Manual discovery, follow these steps:

   a. Enter a name in the Cluster Shared Resource Name box.

   b. Select a resource type from the Resource Type menu. The menu includes the following resource types:

      - **Logical Disk**
      - **Disk Partition**
      - **Volume Manager Volume**
      - **Disk Drive**

   c. Select the relevant resource for each cluster host, and click **Save Selections as Cluster Shared Resource**. The selections are added to the Cluster Shared Resources table.

   d. Repeat steps a through c for each shared resource in the cluster.

   e. Click **Next**.

5. Cluster Manager Step 4 (Select Preferred Hosts for Cluster Shared Resources) is displayed. Select a preferred host for each of the cluster shared resources. Shared resource capacity data will be collected from the specified node. Selecting "None" will result in no information being collected about the cluster shared resource.

   Specify the preferred host for individual cluster shared resources. If a resource is not shared by the preferred host selection, the preferred host menu for that shared resource will continue to display the previous selection.

   When you have finished specifying preferred hosts, click **Finish**.

Filtering Hosts

The Available Hosts table on Cluster Manager Step 2 (Specify Cluster Properties and Cluster Members) allows you to filter the list of hosts displayed. To filter the list of hosts:

1. Click the **+ Filter** link to display the filtering options.

   If the volume filter is already displayed, the **- Filter** link is shown instead, which will collapse the filtering options.

2. Enter all or part of a volume name in the Name Contains box.

3. Select an operating system from the Operating System menu.
4. Enter all or part of a vendor name in the Vendor Contains box.
5. Enter a number in the Processors (>=) box.

   Hosts with at least as many processors as specified will display in the table.
6. Enter a number in the HBAs (>=) box.

   Hosts with at least as many HBAs as specified will display in the table.
7. Enter a number in the Ports (>=) box.

   Hosts with at least as many ports as specified will display in the table.
8. Click **Filter**.

   The table is updated to display only the elements that meet the filter criteria.

NOTE: To reset the filter criteria, click **Reset**.

File Servers and Clusters

If you have marked a host as a file server and you move it into or out of a cluster, you must remove the file server data from the host and then re-mark it as a file server. To remove the file server data from the host and re-mark it as a file server:

1. Select **Reports** > **Storage Essentials** > **Data Collection** > **FileSystem Viewer Data** in HP Systems Insight Manager.
2. Verify that the **File Servers** tab is displayed.
3. Select the file servers you want to remove, and then click **Delete**.
4. Click **Add File Server**.
5. Click the check boxes for the hosts that you would like to mark as file servers.
6. Click **OK**.

   The hosts are marked as file servers, and you are returned to the **File Servers** tab.
7. After removing the file server data from the host and then re-marking it as a file server, you must rescan the cluster member nodes and the cluster nodes. If a rescan is not completed, incorrect data may be displayed.

Clustering in System Manager

System Manager has been enhanced to seamlessly support clusters in all areas. You can view connectivity information from all levels on a single canvas — from applications running on clusters, to the storage array spindles that share volumes for all the nodes of a cluster.

For detailed information about System Manager, see "Viewing Element Topology and Properties" on page 354.

The following figure shows how clusters are displayed in System Manager. Note that the tree nodes on the List tab reflect the structure of the clusters.

In this figure, the box on the left of the topology canvas shows a cluster with two hosts, and the box on the right shows a cluster with four hosts. Both clusters are in the expanded view mode, so all of the nodes are displayed. To minimize the view of a cluster, click the (-) button.

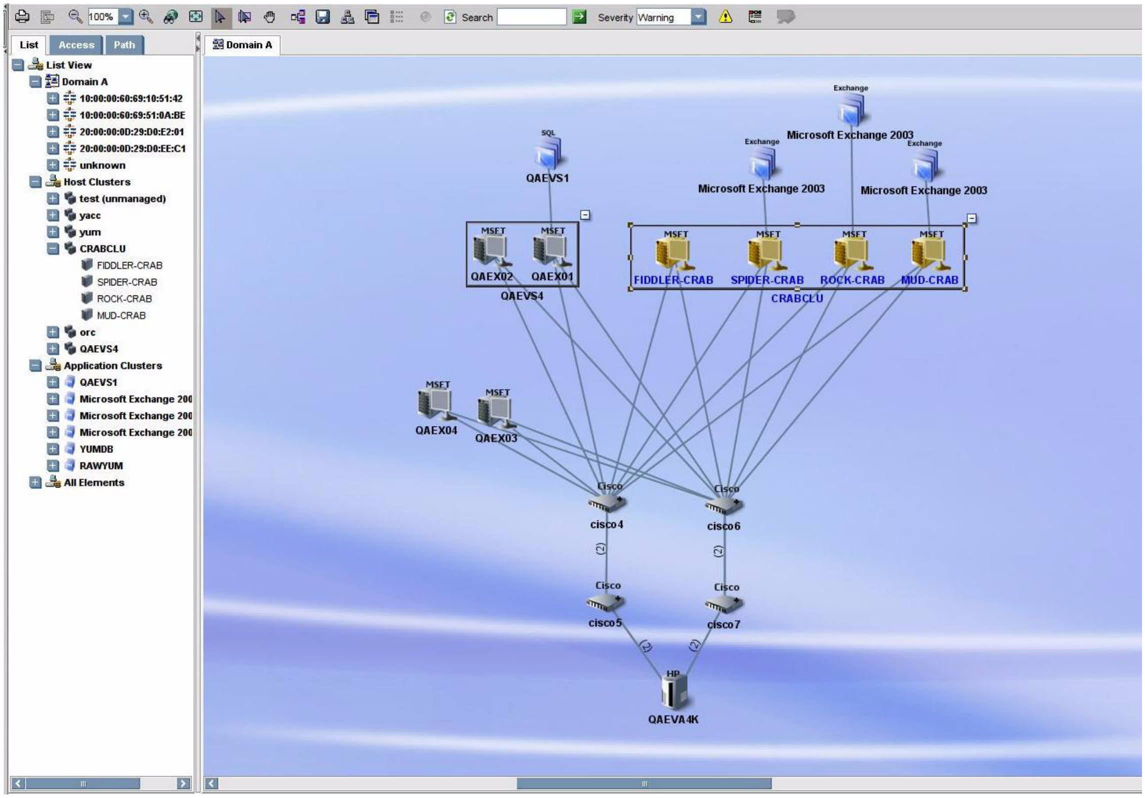


Figure 19 System Manager Cluster Representation

In the minimized view of a cluster, all of the nodes of the cluster are collapsed into a single box. To expand the display to show all of the nodes, click on the (+) button.

In the minimized view, a dotted line from an application to a cluster indicates that the application only runs on some of the clustered hosts. A solid line indicates that the application runs on all of the clustered hosts.

Double-click a cluster to open the Properties page for the cluster. Double-click an individual cluster node to open the Properties page for that node.

Clustering in Topology

Element topology expands System Manager’s view to show exactly which shared resources a particular application instance uses. Individual paths from application nodes are listed in the path tree as well.

For detailed information about viewing element topology, see ”Viewing Element Topology” on page 437.

In the following figure, individual instances of Microsoft Exchange Server 2003 share HP EVA virtual disk array group shared resources:

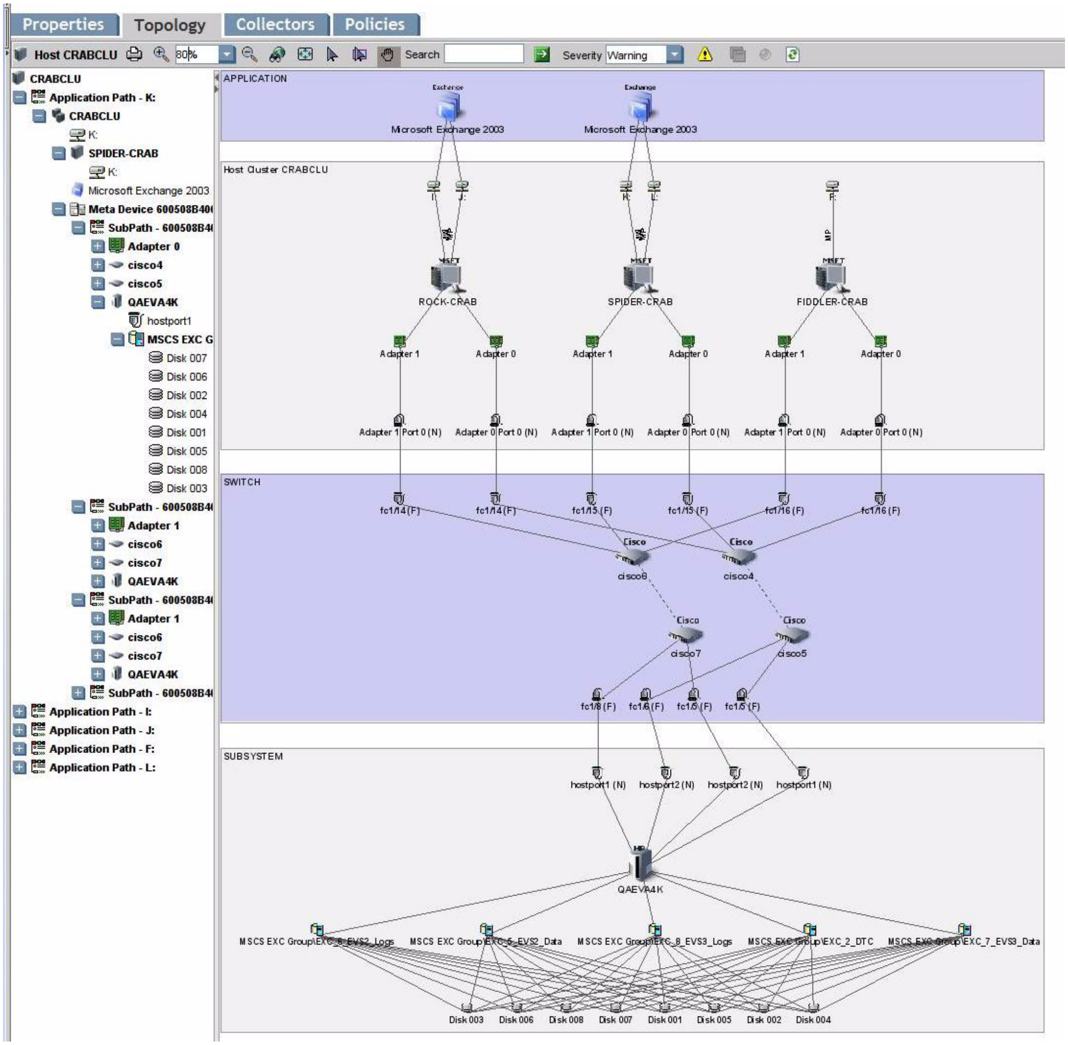


Figure 20 Cluster Element Topology Representation

Clustering in Capacity Manager

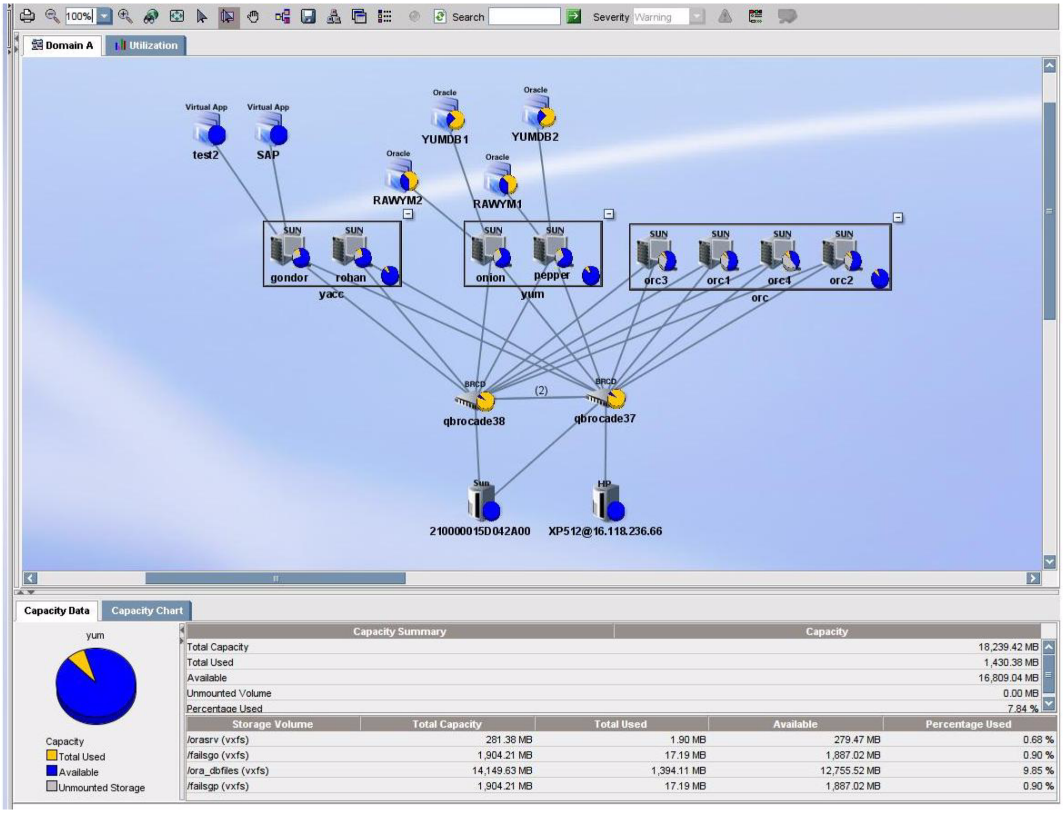
In Capacity Manager, it is possible to see the whole capacity utilization by the cluster. Clusters are represented as managed elements, and the capacity calculator intelligently avoids double counting of the capacity from individual nodes at the cluster level.

For detailed information about Capacity Manager, see "Finding an Element's Storage Capacity" on page 669.

You can drill down to various levels to see the following details of cluster capacity utilization:

- Whole cluster capacity
- Individual application instance capacity
- Individual cluster node capacity
- Capacity trending over a period of time
- Shared resources of individual nodes

The following figure shows an example of how clusters are represented in Capacity Manager:



Capacity Summary	Capacity
Total Capacity	18,239.42 MB
Total Used	1,430.38 MB
Available	16,809.04 MB
Unmounted Volume	0.00 MB
Percentage Used	7.84 %

Storage Volume	Total Capacity	Total Used	Available	Percentage Used
/orasrv (vxfs)	281.38 MB	1.90 MB	279.47 MB	0.68 %
/failsgo (vxfs)	1,904.21 MB	17.19 MB	1,887.02 MB	0.90 %
/ora_dbfiles (vxfs)	14,149.63 MB	1,394.11 MB	12,755.52 MB	9.85 %
/failsgp (vxfs)	1,904.21 MB	17.19 MB	1,887.02 MB	0.90 %

Figure 21 Capacity Manager Cluster Representation

20 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 contains the following topics:

About Security for the Management Server

The management server offers security based on the assignment of roles and organizations. Role-based security determines access to specific functionality depending on the user account assigned to a role. Organization-based security determines 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 349
- "About Organizations" on page 352
- "Planning Your Hierarchy" on page 355
- "Naming Organizations" on page 355

About Roles

The management server ships with several predefined roles, which 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 Manager, but not to System Manager, Provisioning Manager, Policy Manager, Backup Manager, and Reporter. Likewise, users assigned to the domain administrator role have access to all of the features, as shown in Table 25 on page 350.

IMPORTANT: These roles apply only to features and elements in HP Storage Essentials. For example, assume you assigned a user to the Help Desk role in Storage Essentials. For example, assigning a user to the Help Desk role in Storage Essentials will not give the user that role in any other product.

Table 25 Default Role Privileges

Feature	**Role**					
	CIO	**Domain Administrator**	**Storage Administrator**	**Server Administrator**	**Application Administrator**	**Help Desk**
Application Viewer	X	X			X	X
System Manager	X	X	X	X	X	
Event Manager		X	X	X	X	X
Backup Manager	X	X	X	X	X	
Provisioning Manager		X	X			
Provisioning Administration		X	X			
Capacity Manager	X	X	X	X	X	
Policy Manager		X	X			
Chargeback Manager	X	X	X			
Business Tools	X	X	X			
Reporter	X	X	X	X	X	
Global Reporter	X	X	X			
File System Viewer		X		X		
Performance Manager	X	X	X	X	X	
Access CLI		X	X			
Custom Commands		X	X			

Table 25 Default Role Privileges (continued)

Feature	Role					
	CIO	Domain Administrator	Storage Administrator	Server Administrator	Application Administrator	Help Desk
System Configuration		X				

SIMViewOnly

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 25 on page 350. See "Adding Users" on page 356 for more information.

Granting Global Reporter Access

Users with access to Global Reporter can view all 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.

Domain Administrator Role Privileges

Only users belonging to the Domain Administrators role can add, modify, and delete users, roles, and organizations. The Domain Administrator can only edit active organizations.

Domain Administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server. Domain administrators can also edit their full name, e-mail, phone, and other details, as well assign and un-assign any organization.

System Configuration Option

If the System Configuration option is selected for a role, all users assigned to that role will have the administration capabilities shown in the following list:

- 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 Manager, File System Viewer and Performance Manager
- Configure reports and traps
- Set up the management server to send e-mail

If you do not want users belonging to that role to have those capabilities, do not assign the System Configuration option.

Roles Used to Restrict Access

Roles also restrict access to element properties, element records, and Provisioning Manager, as shown in Table 26 on page 351.

Table 26 Default Role Privileges by Elements

Role	Element					
	Application	**Host**	**Switch**	**Storage System**	**Tape Library**	**Others**
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

Options for Restricting a Role

In addition, you can assign one of the following options within a role to further allow or restrict access for a specific element:

- **Full Control** — Lets you view and modify the record for the element on the Asset Management tab, and perform provisioning if applicable.
- **Element Control** — Lets you view and modify the record for the element on the Asset Management tab. You cannot perform provisioning.
- **View** — Lets you only view element properties.

For example, if users belong to a role that only lets them view the element properties on storage systems, those users 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 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 Reporter and modify servers.

About Organizations

IMPORTANT: Organizations only apply to elements in HP Storage Essentials. For example, a user assigned to an organization containing only hosts will only be able to view hosts in Storage Essentials; however, that user may be able to view all other elements in HP Systems Insight Manager.

You can use organizations to 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 assigned to an organization can see only the elements that belong to that 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. A user assigned to OnlyHosts and OnlySwitches 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. The figure below shows a parent-child hierarchy in which BostonWebHosts organization contains two child organizations, BostonWebHost_Windows and BostonWebHost_Solaris. BostonWebHosts is a parent because it contains two organizations.

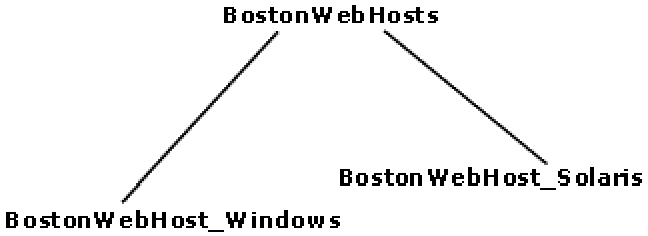


Figure 22 Parent-Child Hierarchy for Organizations

If a child contains organizations, it is also a parent. For example, if 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; for example, when you add a new element, you need to add it only once; the change ripples through the hierarchy. For example, if you add an element to BostonWebHost_Windows, not only users 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 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. For example, if you have a user that oversees all Web hosts in the company, you could assign that user 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. For example, if 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

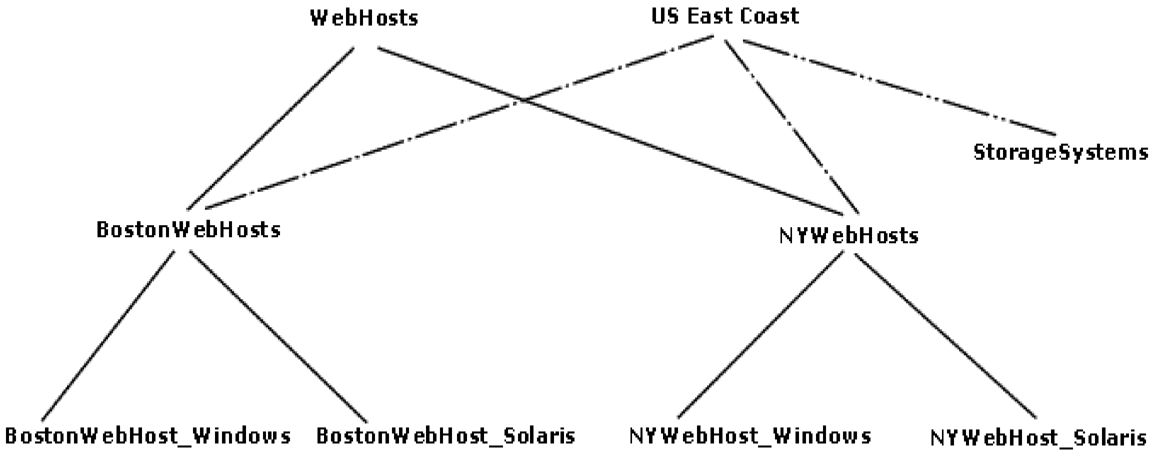


Figure 23 Children in Multiple Organizations

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 became 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.
- Users can view all elements only in the Discovery pages. In all other pages, only the members of the active organization are available. Discovery lists in HP SE (Discovery tab on the SE Home page) are not filtered. Users can see all elements in the discovery lists regardless of their affiliation with an organization.
- Events from all elements regardless of the user's organization are displayed by Event Manager.
- 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 when you email reports. If you do not have permission to access hosts, the reports you e-mail, including the host-specific reports, will not contain information about hosts. 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.

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? Or 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 a graphics illustration program, so you can keep track of which organizations are parents and children.

Create the child organizations first, then their parents. See "Adding an Organization" on page 363 for more information.

Naming Organizations

When you create an organization, give it a name that reflects its members. 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 which are children. When you name an organization, you might want to include a portion of the name of the dominant parent organization. For example, if 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 contains the following topics:

Adding Users

This section contains procedures for adding users and authorizing privileges. Only users belonging to the Domain Administrator role can add or modify users.

Keep in mind the following:

- On Windows systems — The user name and password must be alpha-numeric, and cannot exceed 256 characters. The user name cannot begin with a number.
- On Linux systems — The user name and password cannot exceed 256 characters.

To create an account:

1. In HP SIM, click **Options** > **Security** > **Users and Authorizations**.
2. Click the **User** tab.
3. Click **New**.
4. Enter the following information:
   - Enter a user name in the Login name box. The account must be valid on the operating system (includes Active Directory on Windows) on the central management server (CMS).
   - If you are running the management server on Microsoft Windows, enter the domain name of the server running Storage Essentials in the Domain box.

   You do not need to provide additional information. For more information about the other options displayed 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 not only view the features in the tool bar, but use them as well.

To authorize a user to use the features in Storage Essentials:

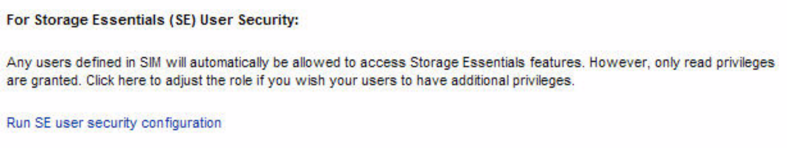
1. Click the **Authorizations** tab if the new user doesn't have All Tools or HP SE Tools associated. Click **New**.

2. In the New Authorizations table, select the user.
3. Select **Manually assign toolbox and system/system group authorizations**.
4. In the Selected Toolbox(es) section, select **HP SE Tools**.
5. In the Select Systems list box, select the systems you want the user to be able to manage.

> **IMPORTANT:** You must select CMS (Central Management Server) as one of the systems.

6. Click **OK**.

   The users you created in HP SIM are put in the SIMViewOnly Role. This role does not allow users to access any of the features listed in "Default Role Privileges" on page 350.
7. If you want to change the role from the default SIMViewOnly role, click the Run SE User Security Configuration link on the HP SIM Users tab.



For Storage Essentials (SE) User Security:

Any users defined in SIM will automatically be allowed to access Storage Essentials features. However, only read privileges are granted. Click here to adjust the role if you wish your users to have additional privileges.

Run SE user security configuration

Figure 24 Run SE user security configuration

8. Change the role as described in "Editing a User Account" on page 357.

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.
- See "Domain Administrator Role Privileges" on page 351.
- User modifications take 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, click **Security** > **Users**.
3. Click the **Edit** (✎) button for the user account you want to modify.
4. To change the account name, enter a new name for the user account in the **Name** box; for example: jsmith

   This name becomes the user name for the account.

5. To change the name assigned to the user account, enter a new name for the account in the Full Name box.

   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 menu.
7. To change the e-mail address listed, enter a new e-mail address in the **E-mail** box.
8. To change the phone number listed, enter the user's new phone number in the **Phone** box.
9. Change or remove information from the **Notes** box if necessary.
10. To change the organizations to which the user belongs, select or deselect the organizations from the table in the user interface.

    NOTE: The Everything organization is the default organization that lets users access all current and future elements.
11. Click **OK**. The user account is updated.

Deleting Users

Keep in mind the following:

- You cannot delete the admin account.
- Only users belonging to the Domain Administrator role can delete users.

To delete a user account:

1. In HP SIM, click **Options** > **Security** > **Users and Authorizations**.
2. Click the **User** tab.
3. Select the check box for the users you want to delete, and click **Delete**.

   The selected user accounts are 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, ask your Domain Administrator to make the changes.

To modify your user profile (other than name, role, and organization affiliation):

1. Click the name of your account in the upper-left corner in the HP SE Home page, (**Tools** > **Storage Essentials** > **Home in HP SIM**).

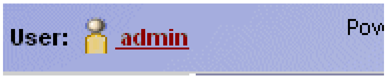


Figure 25 Clicking the Name of Your User Account

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 **Save Changes**.

Modifying Your User Preferences

Use the User Preference tab to modify your user preferences for System Manager and Element Topology. 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.
2. Click the **User Preferences** tab.

System, Capacity and Performance Manager Preferences

Select one of the following:

- **Load-on-Demand:** Does not populate the tree nodes or display elements in the topology when the page opens (Faster). Use this option for medium to large environments.
- **(Default) Automatic Loading:** Populate fabric tree nodes and display all elements in the topology when the page opens (Slower).

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 menu.

If you want events refreshed within a time period, select the **Refresh events automatically** box 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.

Warnings for Slow Systems Operations

By default, the management server warns you when it encounters issues occurring when 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 359 for information on how to access the User Preferences tab.

Viewing the Properties of a Role

If you are assigned the Domain Administrator role, you can 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, click **Security** > **Users**.
3. In the Role column, click the name of the role.

The following information for the selected role is displayed:

- 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 — How much access the user has to a type of element, such as hosts, storage systems, switches, and applications. See "About Security for the Management Server" on page 349 for more information.
- Access to the <product name> — Components in the management server the user can access, where `<product name>` is the name of your product.

To learn how to edit a role, see "Editing Roles" on page 361.

Viewing the Properties of an Organization

If you are assigned the Domain Administrator role, you can determine which elements a user can access by viewing the properties of the user's organization

To view the properties of 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, click **Security** > **Users**.
3. In the Organization column, click the name of a organization.
4. Take one of the following actions:
   - To determine which elements are in a child organization, click the link of the child organization.
   - To learn more about an element, click the element's link to display 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 Security for the Management Server" on page 349 for more information.

To learn how to edit an organization, see "Editing an Organization" on page 365.

Managing Roles

This section contains the following topics:

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 "About Security for the Management Server" on page 349 for more information about roles and organizations.

Keep in mind the following:

- The Role Name and Description boxes do not accept special characters, except spaces and the following characters: $, -, ^, ., and _
- Only users belonging to the Domain Administrator role can add roles.

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, click **Security** > **Roles**.
3. Click **New Role**.
4. In the Role Name box, enter 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 box, enter a description for the role; for example: Role for those in quality assurance.

   The description cannot be more than 1024 characters.
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.
     See "Options for Restricting a Role" on page 352.
7. Select the features you want a user to be able to access.
8. Click **OK**.

Editing Roles

The software lets you modify the default roles and/or the roles you have created. See "About Security for the Management Server" on page 349 for more information about roles and organizations.

Keep in mind the following:

- Only users belonging to the Domain Administrator role can modify roles.
- Domain administrators can change the user names and roles of other domain administrators, but they cannot modify their own user name and roles while logged into the management server.
- After you click **OK** 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 box does 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, click **Security** > **Roles**.
3. Click the **Edit** (✎) button.
4. Make the desired changes:
   - To edit the name of the role, change the name in the Role Name box. The name can contain spaces, but it cannot be longer than 256 characters.
   - To edit the description of the role, change the description in the Description box. The description cannot be more than 1024 characters.
   - 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.
       See "Options for Restricting a Role" on page 352.
5. Select the features you want a user to be able to access.

   See "Management Server Components" on page 9 for more information about these features.
6. Click **OK**.

Deleting Roles

Keep in mind the following:

- A role cannot be deleted if it contains a user.
- Only users belonging to the Domain Administrator role can delete roles.

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, click **Security** > **Roles**.
3. Select **Roles** from the menu.
4. Click the corresponding **Delete** button (🗑).

   The role is deleted.

Managing Organizations

This section contains the following topics:

Adding an Organization

You can create new organizations to restrict access to certain elements. For example, if 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 will only be able to access the elements you specified.

See "About Security for the Management Server" on page 349 for more information about roles and organizations.

Keep in mind the following:

- Create child organizations first, then their parents.
- Events from all elements regardless of the user's organization are displayed by Event Manager.
- Only users belonging to the Domain Administrator role can add organizations.
- Only active organizations can be edited.
- 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.
- Moving a cluster from one organization to another moves all of the cluster's nodes to the target organization.

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, click **Security** > **Roles**.

3. Click the **New Organizations** button.
4. In the **Name** box, enter a name for the organization.

   The name of an organization has the following requirements:

   - Can contain spaces.
   - Can add digits to the beginning of an organization's name.
   - Cannot be longer than 256 characters.
   - Cannot contain the caret (^) symbol—currently the system allows the caret symbol to be entered, but the caret symbol should not be included in an organization's name.
5. In the **Description** box, enter a description for the organization.

   The Description box cannot have more than 1024 characters.
6. Click **Add or Remove Members** to determine which elements the user will see.
7. To add elements:
   a. Expand the Element Types node in the tree, and select the element type that you would like to add.
   b. In the right-hand pane, select the elements you would like to add by clicking the appropriate check boxes.
   c. Click **Add**.
   d. The selected elements are added to the Organization Members pane. To add storage volumes to the organization, see "Adding Storage Volumes to an Organization" on page 364.
8. To add organizations:
   a. Click the **Organizations** node.
   b. In the right-hand pane, select the elements you would like to add by clicking the appropriate check boxes.
   c. Click **Add**. The selected organizations are added to 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 "About Security for the Management Server" on page 349 for more information.
9. Click **OK** when you are done adding the elements and organizations.

Adding Storage Volumes to an Organization

Only users belonging to the Domain Administrator role can add storage volumes to an organization.

To add storage volumes to an organization:

1. Click **Add or Remove Members**.
2. Expand the Element Types node in the tree and select the Storage Systems node.
3. In the right-hand pane, click the **Storage Volumes** tab and select a storage system from the Showing Volumes for Storage System menu.
4. If you want to filter the list of volumes for a storage system, click the **Show Volume Filter** link, select the appropriate filter criteria, and click **Submit Query**.

5. Select the storage volumes you want to add to the organization. Click the **+Ports** link in the Ports column to see a list of the ports associated with a particular volume.
6. When you are finished selecting volumes, click the **Add** button located at the top of the pane.
7. Click **OK**. The selected volumes are added to the Organization Members pane.

Viewing Organizations

The Setup Organizations page lists the organizations with their descriptions. The page also shows the number of top-level elements, users, and child organizations assigned to each organization.

Only users belonging to the Domain Administrator role can view organizations.

The No. of Top Level Elements column provides the total number of elements assigned directly to an organization. This number does not include those within the child organization. A zero (0) in the Elements column indicates that the organization contains only child organizations; however, users assigned to that organization would have access to the elements assigned to its child organizations.

Access the Setup Organizations page by clicking **Security** > **Organizations** in Storage Essentials.

To access information about a child organization, click its link in the Child Organization column.

Editing an Organization

When elements are removed from an organization, users belonging only to that organization are no longer able to access the removed elements.

See "About Security for the Management Server" on page 349 for more information about roles and organizations.

Keep in mind the following:

- Depending on your license, role-based security may not be available. See the List of Features accessible from the Documentation Center.
- Only users belonging to the Domain Administrator role can edit organizations.
- Only active organizations can be edited.
- You cannot edit the Everything organization.

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, click **Security** > **Roles**.
3. Click the Edit (✎) button.
4. To change the name of the organization, enter a new name in the Name box.

   The name of an organization has the following requirements:

   - Can contain spaces.
   - Can add digits to the beginning of an organization's name.
   - Cannot be longer than 256 characters.

- Cannot include special characters, except spaces and the following characters: $, -, ., and _
- Cannot contain the carot (^) symbol.

5. To change the description of the organization, enter a new description in the **Description** box.

   You cannot enter more than 1024 characters in the **Description** box.
6. Click **Add or Remove Members**.
7. Add or remove elements as described in ”Adding an Organization” on page 363 and ”Removing Members from an Organization” on page 366.
8. Once you are done adding or removing elements, click **OK** in the Add Organization or Remove Organization page.
9. In the Edit Organization page, click **OK**.

Removing an Organization

When an organization is removed, users assigned only to that organization are no longer able to access its elements. 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.
- Only users belonging to the Domain Administrator role can delete organizations.
- You cannot delete an organization that contains a user who belongs to no other organizations. For example, assume you create an organization named Org1 that contains two users: User1 and User2. User1 belongs to two other organizations, while User2 only belongs to the organization you just created. You will not be able to delete Org1 because the organization contains User2, who only belongs to the organization you are trying to delete.

To delete an organization:

1. Click **Security** > **Organizations**.
2. Click the Delete (🗑)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 became 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.

Use one of the following methods to remove an element from an organization:

- In the Edit Organization window, click the Delete (🗑) 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 by clicking the appropriate check box, and then click **Remove**.
- Only users belonging to the Domain Administrator role can remove members from an organization.

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: WindowsHosts and SolarisHosts. If you want to view elements only in WindowsHosts and not in SolarisHosts organizations, you could use the filtering feature to activate only the WindowsHosts organization.

Keep in mind the following:

- Users assigned to the Admin account cannot filter organizations because the Admin account belongs to the Everything organization by default. As a result, these users do not have access to the filtering feature for organizations.
- If you do not want to view an element, deselect all child organizations containing that 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 SolarisHosts organization. The SolarisHosts organization is contained in the Hosts organization. You must deselect the SolarisHosts organization and the Hosts organization if you do not want to see the Solaris hosts.
- Events from all elements regardless of the user's organization are displayed by Event Manager.
- 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.
3. Deselect the organizations that contain the elements you do not want to obtain information about. For example, if you want to view only the elements in the WindowsHosts organization, you would select only WindowsHosts. If you have a parent organization named Hosts that contains SolarisHosts and WindowsHosts, you would need to deselect SolarisHosts and Hosts. You would need to deselect Hosts because it contains organizations other than WindowsHosts.

   If you belong to the Domain Administrator role, links are displayed for the organizations. To learn more about the contents of an organization, click its link.
4. Click **OK**.

You can now only obtain information about elements in the active organizations. These active organizations are listed in the link next to the filter button, as shown in the following figure.

Windows Host

Figure 26 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 to create and update the management server database. Default password: `change_on_install`
- SYSTEM — Used to create and upgrade, import, export and re-initialize the management server database. 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`
- **SIM_MANAGER** — Used for all HP SIM activity, including the HP SIM schema, maintenance, and login. Default password: `quake`

To change the passwords of the SYS, SYSTEM, RMAN_USER, SIM_MANAGER, and DB_SYSTEM_USER accounts, you must use the Database Admin Utility, so the management server is aware of the changes. Do not change the password for any 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.

IMPORTANT: If HP SIM and Storage Essential are using the same Oracle database, you must not only use the Database Admin Utility to change the password, but you must also use the `mxpassword` command to change the password as described in the following steps.

You must provide the same SIM_MANAGER password for the `mxpassword` command and the Database Admin Utility.

NOTE: You can't change the password for SIM_MANAGER if you are running HP SIM and Storage Essentials on Linux in a single-box environment.

The password requirements for the management server are:

- Must have a minimum of three characters
- Must start with a letter
- May contain only letters, numbers and underscores (_)
- May not start or end with an underscore (_)

To change the password of a system account:

1. If you are changing the SIM_MANAGER password and HP SIM and HP SE are using the same Oracle database, you must complete the following steps.:
   a. Log onto the server running HP Systems Insight Manager.
   b. Stop the AppStorManager service if it is started.
   c. Enter the following at the command prompt:

      ```
      C:\> mxpassword -m -x MxDBUserPassword=mynewPass
      ```

      where `mynewPass` is your new password for the database.
   d. Stop the HP Systems Insight Manager service so that it cannot access the database. It is very important that the HP Systems Insight Manager service does not access the database before you are finished with changing the password for the database.
2. Access the Database Admin Utility.
3. Click **Change Passwords** in the left pane.
4. Select an account name from the User Name box.
5. Enter the current password in the Old Password box.
6. Enter the new password in the New Password box.
7. Re-enter the password in the Confirm Password box.
8. Click **Change**.

   The Database Admin Utility changes the password for the specified account.

Using Active Directory/LDAP for Authentication

NOTE: Active Directory/LDAP is not supported with Storage Essentials Standard Edition.

The management server supports external authentication through Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) directory services. When you configure the management server to use external authentication, user credentials are no longer stored in the management server database. This configuration centralizes all security related requirements to the enterprise AD/LDAP infrastructure, such as password expiration, resets, and complexity requirements.

When a user attempts to log into the management server, the management server authenticates the user name and password against AD/LDAP for credential verification. If AD/LDAP verifies that this user has the correct credentials, the management server allows this user access to the application.

Keep in mind the following:

- The `login-handler.xml` file contains configuration information for both AD and LDAP. It is important to enable either AD or LDAP; you cannot enable both.
- If you want to go back and forth between internal and external (AD/LDAP) authentication, rename the `login-handler.xml` file before you modify it. This way you can easily switch back to internal authentication by changing the file name back to `login-handler.xml`.

To use AD/LDAP to authenticate your users, complete the following procedures:

- ”Step 1 — Configure the Management Server to Use AD or LDAP” on page 369
- ”Step 2 — Restart the AppStorManager Service and Login as the Designated Admin Account” on page 376
- ”Step 3 — Add Users to the Management Server” on page 377
- ”Step 4 — Provide Login Information to Your Users” on page 377

Step 1 — Configure the Management Server to Use AD or LDAP

If you want to use AD/LDAP, you must modify the `login-handler.xml` file. How you modify the `login-handler.xml` file depends on whether you plan to use AD or LDAP.

To configure the management server:

- To use AD, see ”Configuring the Management Server to Use Active Directory” on page 369
- To use LDAP, see ”Configuring the Management Server to Use LDAP” on page 373

Configuring the Management Server to Use Active Directory

By default, AD allows connections with domain\username, instead of with the distinguished name (DN) used by a generic LDAP server. However, you can use the generic LDAP server setup to authenticate with AD, as described in ”Configuring the Management Server to Use LDAP” on page 373.

To specify the management server to use AD:

1. Before switching to AD authentication mode, the management server needs to be configured with a designated AD user and other AD-specific credentials. At startup, the designated AD user is mapped to the built-in Admin user and overrides it with the AD user information.

   IMPORTANT: Make sure the administrator account has already been created in AD before you add it to the `login-handler.xml` file.

   a. On the management server look in one of the following locations:

   - **Windows:** `%MGR_DIST%\Data\Configuration`
   - **UNIX systems:** `$MGR_DIST/Data/Configuration`

   b. In the `login-handler.xml` file, change the value of the `<AdminAccountName>` tag to the name of a user account in AD, as shown in the following example:

```
<AdminAccountName>domain\PrimaryUser</AdminAccountName>
```

   where `PrimaryUser` is the name of the user account that is designated as the primary user in AD.

   For security reasons, it is recommended that the designated user not be the AD Domain Administrator

2. In the `login-handler.xml` file, comment out the section that contains `com.appiq.security.server.BasicLoginhandler`, which enables internal authentication mode. Only one login handler is allowed at a time.

```
<!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</LoginHan
dlerClass-->
```

3. Comment out the `<LoginHandlerType>Default</LoginHandlerType>` tag as follows:

   ```
   <!--LoginHandlerType>Default</LoginHandlerType-->
   ```

4. Uncomment the line containing the class name and login handler type so that it appears as follows:

   ```
   <LoginHandlerClass>com.appiq.security.server.ActiveDirectoryLoginHandler</L
   oginHandlerClass>
   <LoginHandlerType>ActiveDirectory</LoginHandlerType>
   ```

5. Replace `directory.hp.com` with the IP address or the fully qualified DNS name of your primary Domain Controller server in the `login-handler.xml` file, as shown in the following example:

   ```
   <PrimaryServer port="389">192.168.10.1</PrimaryServer>
   ```

   where

   - `192.168.10.1` is the IP address of the primary Domain Controller server running AD.
   - `389` is the port on which AD is running on the server.

6. Replace `directory2.hp.com` with the IP address or the fully qualified DNS name of your secondary Domain Controller server, if available.

   ```
   <SecondaryServer>192.168.10.2</SecondaryServer>
   ```

   where `192.168.10.2` is the IP address of the secondary Domain Controller server running AD.

7. If you want the password to be saved in the management server database, change the value of the `<ShadowPassword>` tags to `true`, as shown in the following example:

   ```
   <ShadowPassword>true</ShadowPassword>
   ```

   Saving the passwords in the management server database allows a user to also log into the management server if the management server is changed back to local mode. This, however, is not recommended as it defeats the purpose of externalizing a user's credentials.

   The `login-handler.xml` file contains two sets of `<ShadowPassword>` tags: one for AD and one for LDAP. Make sure you change the value of the `<ShadowPassword>` tags that are children of the `<ActiveDirectory>` tag.

8. If you want the user name to be case sensitive, change the value of the `<CaseSensitiveUserName>` tag to true, as shown in the following example:

   ```
   <CaseSensitiveUserName>true</CaseSensitiveUserName>
   ```

   If you change the value of `<CaseSensitiveUserName>` to `true`, the management server becomes case-sensitive to user names. The management server sees `MyUserName` and `myusername` as different users.

   IMPORTANT: AD servers are not case sensitive for user names, so changing this tag to `true` for AD authentication is not recommended.

   The `login-handler.xml` file contains two sets of `<CaseSensitiveUserName>` tags: one for AD and one for LDAP. Make sure you also change the value of the `<CaseSensitiveUserName>` tags that are children of the `<ActiveDirectory>` tag.

9. Provide the AD search base in which you want the management server to look up AD/LDAP user attributes. Allow no spaces between commas and put in all components of fully qualified domain name, for example, `hds.usa.com` would be `DC=hds,DC=usa,DC=com`.

   The search base is used to specify the starting point for the search. It points to a distinguished name of an entry in the directory hierarchy.

   ```
   <SearchBase> dc=MyCompanyName,dc=COM</SearchBase>
   ```

10. Save the `login-handler.xml` file with your changes.

    The following is an example of a modified `login-handler.xml` file for use with AD server authentication. Underlined text is information that was modified:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<LoginHandler>
<AdminAccountName>domain\primaryuser</AdminAccountName>
<!-- for the default, using database for authentication -->
<!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</LoginHan
dlerClass-->
<!--LoginHandlerType>Default</LoginHandlerType-->
<!-- uncomment the following to enable Active Directory login-->
<LoginHandlerClass>com.appiq.security.server.ActiveDirectoryLoginHandler</L
oginHandlerClass>
<LoginHandlerType>ActiveDirectory</LoginHandlerType>

<ActiveDirectory>
<PrimaryServer port="389">IP address of Primary Domain 
Controller</PrimaryServer>
<SecondaryServer>IP Address of Secondary Domain Controller</SecondaryServer>
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- provide SearchBase if full name and email attribute are to be
synchronized
between ActiveDirectory and the database.-->
<SearchBase>DC=domain_extension1,DC=domain_extension2,DC=COM</SearchBase>
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</ActiveDirectory>
<!-- uncomment the following for generic LDAP login
<LoginHandlerClass>com.appiq.security.server.LdapLoginHandler
</LoginHandlerClass>
<LoginHandlerType>LDAP</LoginHandlerType>
-->
<LDAP>
<!-- same as java.naming.provider.url ldap://ldap.companyname.com:389
-->
<Server port="389">IP address of LDAP server</Server>
<!-- LDAP env can be added, an example is shown below...
<LDAPEnv
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</LDAPEn
v>
-->
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- multiple DN entries are allowed, they will be tried one at a time -->
<DN>CN=$NAME$,OU=Engineering,DC=HP,OU=US,DC=COM</DN>
<!-- provide FullNameAttribute and EmailAttribute if full name and email
attribute
are to be synchronized between LDAP and the database -->
```

```
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</LDAP>
</LoginHandler>
```

When you are done with your changes, the login-handler.xml file, may resemble the following:

```
<LoginHandler>
  <AdminAccountName>domain\primaryuser</AdminAccountName>
  <LoginHandlerClass>
    com.appiq.security.server.ActiveDirectoryLoginHandler
  </LoginHandlerClass>
  <LoginHandlerType>ActiveDirectory</LoginHandlerType>
  <ActiveDirectory>
    <PrimaryServer>IP address of primary domain controller</PrimaryServer>
    <SecondaryServer>IP address of secondary domain
controller</SecondaryServer>
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<SearchBase>DC=MyCompanyName,DC=COM</SearchBase>
    <FullNameAttribute>displayName</FullNameAttribute>
    <EmailAttribute>mail</EmailAttribute>
  </ActiveDirectory>
</LoginHandler>
```

Configuring the Management Server to Use LDAP

The LDAP server requires a distinguished name (DN) and credentials. The DN can be configured, allowing name substitution and support for multiple DN configurations.

To configure the management server to use LDAP:

1. Before switching to LDAP authentication mode, the management server needs to be configured with a designated LDAP user through the `<AdminAccountName> tag`. At startup, the designated LDAP user is mapped to the built-in “admin” user and overrides it with the LDAP user information.

   IMPORTANT: Make sure the administrator account has already been created in LDAP before you add it to the `login-handler.xml` file.

   a. On the management server look in one of the following locations:

   - **Windows:** `%MGR_DIST%\Data\Configuration`
   - **UNIX systems:** `$MGR_DIST/Data/Configuration`

   b. In the `login-handler.xml` file, change the value of the `<AdminAccountName>` tag to the name of a user account in LDAP, as shown in the following example:

```
<AdminAccountName>Administrator</AdminAccountName>
```

where Administrator is the name of a user account in LDAP.

2. In the `login-handler.xml` file, comment out the section that contains `com.appiq.security.server.BasicLoginhandler`, which enables internal authentication mode. Only one login handler is allowed at a time.

   ```
   <!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</LoginHan
   dlerClass-->
   ```

3. Comment out the `<LoginHandlerType>Default</LoginHandlerType>` tag as follows:

   ```
    <!--LoginHandlerType>Default</LoginHandlerType-->
   ```

4. Uncomment the line containing the class name and login handler type so that it appears as follows:

```
 <LoginHandlerClass>com.appiq.security.server.LdapLoginHandler</Login-
HandlerClass>
 <LoginHandlerType>LDAP</LoginHandlerType>
```

5. Replace `directory.hp.com` with the IP address or the fully qualified name of your LDAP server in the `login-handler.xml` file, as shown in the following example:

   ```
   <Server port="389">192.168.10.1</Server>
   ```

   where

   - `192.168.10.1` is the IP address of the server running LDAP.
   - `389` is the port on which LDAP is running on the server.

6. If you want the password to be saved in the management server database, change the value of the `<ShadowPassword>` tags to `true`, as shown in the following example:

   ```
   <ShadowPassword>true</ShadowPassword>
   ```

   Saving the passwords in the management server database allows a user to also log into the management server if the management server is changed back to local mode. This, however, is not recommended as it defeats the purpose of externalizing a user's credentials.

   The `login-handler.xml` file contains two sets of `<ShadowPassword>` tags: one for AD and one for LDAP. Make sure you change the value of the `<ShadowPassword>` tags that are children of the `<LDAP>` tags.

7. If you want the user name to be case sensitive, change the value of the <CaseSensitiveUserName> tag to `true`, as shown in the following example:

   ```
   <CaseSensitiveUserName>true</CaseSensitiveUserName>
   ```

   If you change the value of `<CaseSensitiveUserName>` to `true`, the management server becomes case-sensitive to user names. For example, the management server sees `MyUserName` and `myusername` as different users.

   The `login-handler.xml` file contains two sets of `<CaseSensitiveUserName>` tags: one for AD and one for LDAP. Make sure you also change the value of the `<CaseSensitiveUserName>` tags that are children of the `<LDAP>` tags.

8. Provide the LDAP search base in which you want the management server to look up AD/LDAP user attributes. Allow no spaces between commas and put in all components of fully qualified domain name, for example, `hds.usa.com` would be `DC=hds,DC=usa,DC=com`.

   ```
   The search base is used to specify the starting point for the search. It
   points to a distinguished name of an entry in the directory hierarchy.
   ```

   ```
   <SearchBase>CN=$NAME$,dc=MyCompanyName,dc=COM</SearchBase>
   ```

   or:

<SearchBase>`CN=$NAME$,OU=NetworkAdministration,`
`dc=MyCompanyName,ou=US,dc=COM`</SearchBase>

The management server searches only those users in the company who are part of the NetworkAdministration organization (OU=NetworkAdministration) and in the United States (ou=US).

> **IMPORTANT:** Different LDAP implementations may be using different keynames for CN. The appropriate keyname should be named in `login-handler.xml`. Refer to the documentation for your LDAP server to determine how to obtain the appropriate keyname. Your keyname may start with uid instead of `CN, for example,:`
> `uid=$NAME$,ou=<Optional org unit if applicable>,`
> `dc=windows,dc=hp,dc=com`

9. Save the `login-handler.xml` file.

   The following is an example of a modified `login-handler.xml` file for use with an LDAP server. Underlined text is information that was modified:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<LoginHandler>
<AdminAccountName>PreferredUser\admin</AdminAccountName>
<!-- for the default, using database for authentication -->
<!--LoginHandlerClass>com.appiq.security.server.BasicLoginHandler</LoginHan
dlerClass-->
<!--LoginHandlerType>Default</LoginHandlerType-->
<!-- uncomment the following to enable Active Directory login>
<LoginHandlerClass>com.appiq.security.server.ActiveDirectoryLoginHandler</L
oginHandlerClass>
<LoginHandlerType>ActiveDirectory</LoginHandlerType-->

<ActiveDirectory>
<PrimaryServer port="389">IP address of Primary Domain
Controller</PrimaryServer>
<SecondaryServer>IP Address of Secondary Domain Controller</SecondaryServer>
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- provide SearchBase if full name and email attribute are to be
synchronized
between ActiveDirectory and the database.-->
<SearchBase>DC=domain extension1,DC=domain extension2,DC=COM</SearchBase>
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</ActiveDirectory>
<!-- uncomment the following for generic LDAP login-->
<LoginHandlerClass>com.appiq.security.server.LdapLoginHandler</LoginHandler
Class>
<LoginHandlerType>LDAP</LoginHandlerType>
<LDAP>
<!-- same as java.naming.provider.url ldap://ldap.companyname.com:389
-->
<Server port="389">IP address or DNS name of LDAP server</Server>
<!-- LDAP env can be added, an example is shown below...
<LDAPEnv
name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</LDAPEn
v>
-->
```

```
<ssl>false</ssl>
<ShadowPassword>false</ShadowPassword>
<CaseSensitiveUserName>false</CaseSensitiveUserName>
<!-- multiple DN entries are allowed, they will be tried one at a time -->
<DN>CN=$NAME$,OU=Engineering,DC=mycompanyname,OU=US,DC=COM</DN>
<!-- provide FullNameAttribute and EmailAttribute if full name and email
attribute
are to be synchronized between LDAP and the database -->
<FullNameAttribute>displayName</FullNameAttribute>
<EmailAttribute>mail</EmailAttribute>
</LDAP>
</LoginHandler>
```

When you are done with your changes, the `login-handler.xml` file, may resemble the following:

```
<LoginHandler>
  <AdminAccountName>Administrator</AdminAccountName>
  <LoginHandlerClass>
    com.appiq.security.server.LdapLoginHandler
  </LoginHandlerClass>
  <LoginHandlerType>LDAP</LoginHandlerType>
  <LDAP>
    <Server port="389">IP address of LDAP server</Server>
    <ssl>false</ssl>
    <ShadowPassword>false</ShadowPassword>
    <CaseSensitiveUserName>false</CaseSensitiveUserName>
    <DN>CN=$NAME$,OU=Engineering,DC=HP,OU=US,DC=COM</DN>
    <FullNameAttribute>displayName</FullNameAttribute>
    <EmailAttribute>mail</EmailAttribute>
  </LDAP>
</LoginHandler>
```

Step 2 — Restart the AppStorManager Service and Login as the Designated Admin Account

In this section, you will restart the AppStorManager service and login as the designated Admin account.

1. After you modify the `login-handler.xml` file, you must restart the AppStorManager service, which is the service for the management server for your changes to take effect.

   IMPORTANT: The service must be running for users to access the management server.

   On Microsoft Windows:

   a. Go to the Services window, usually accessible from the Control Panel.

   b. Right-click **AppStorManager**.

   c. Select **Stop** from the menu.

   d. To start the management server, right-click **AppStorManager** and select **Start** from the menu.

   On UNIX systems:

   a. Open a command prompt window.

b. Enter the following at the command prompt to stop the management server:

```
/etc/init.d/appstormanager stop
```

c. To start the management server, enter the following at the command prompt:

```
/etc/init.d/appstormanager start
```

2. Login as the designated administrator account you specified in "Step 1 — Configure the Management Server to Use AD or LDAP" on page 369.

   For example, the user name would be the following:

   - AD — domain\PrimaryUser
   - LDAP — PrimaryUser

   where `PrimaryUser` is the name of the user account in LDAP or is the designated primary user in AD.

   The password would be the following: `[NTdomainpassword]`.

Step 3 — Add Users to the Management Server

Once the management server is configured for Active Directory/LDAP, the users can be added to the management server. This is required to prevent accidental access to the management server from other AD/LDAP users. Until the user is authenticated against AD/LDAP, the management server views the user as an internal user, whose password can be changed within the management server.

Once a user is authenticated against AD/LDAP, the user is tagged as an external user and the user's password must be managed through AD/LDAP.

To add a user to the management server:

1. Log onto the management server by using the designated Admin account specified in "Step 1 — Configure the Management Server to Use AD or LDAP" on page 369.
2. Create the users as described in "Adding Users" on page 356 observing the following rules:
   - *AD:* Prefix the user name with the domain name, for example: domain\newuser.
   - The user names you create by using the management server must match the user names in AD/LDAP.
   - It is not necessary to create a password, since the passwords used for login are those already configured on either the AD or LDAP server.

Step 4 — Provide Login Information to Your Users

Notify your users that they are now able to log into the management server, and provide them with the user name and password you have specified in Active Directory/LDAP

IMPORTANT: Remind your users not to give the password they use to access the management server to anyone. Since user credentials are now stored in AD/LDAP, the password used to access the management server may also be used to access other accounts. In some instances, it may even be their network user name and password.

21 Troubleshooting

HP Storage Essentials Standard Edition supports a subset of the devices supported by Enterprise Edition. See the *HP Storage Essentials Standard Edition Support Matrix* for a list of supported devices. The support matrix is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

This chapter contains the following topics:

- Troubleshooting Installation/Upgrade, page 379
- Configuring the Java Console, page 385
- java.lang.SecurityException: Failed to validate one time key, page 385
- "Data is late or an error occurred" Message, page 385
- appstorm.<timestamp>.log Filled with Connection Exceptions, page 385
- Receiving HTTP ERROR: 503 When Accessing the Management Server, page 386
- Permanently Changing the Port a CIM Extension Uses (UNIX Only), page 388
- Configuring UNIX CIM Extensions to Run Behind Firewalls, page 389
- Volume Names from Ambiguous Automounts Are Not Displayed, page 393
- Installing the Software Security Certificate, page 393
- Troubleshooting Discovery and Discovery Data Collection, page 395
- Troubleshooting Topology Issues, page 403
- Troubleshooting Provisioning, page 414
- Troubleshooting CLI Errors, page 415
- Troubleshooting Hardware, page 415

Troubleshooting Installation/Upgrade

This section provides help with troubleshooting installations and upgrades.

- If Your Installation or Upgrade Failed, Capture the Logs, page 380
- Checking Installation Log Files, page 380
- "The environment variable 'perl5lib' is set." Message, page 381
- "SEVERE: OUI-10029..." Message, page 382
- Brocade API Switches Displaying Stale Data, page 382
- SIM Connector Fails to Install for Single–Server Configurations, page 382
- Re-installing the HP SIM Connector (If Your HP SIM User Name or Password is Incorrect or was Changed), page 383
- "Reverse Lookup Failed" Message (Windows only), page 382
- Re-installing the HP SIM Connector (If Your HP SIM User Name or Password is Incorrect or was Changed), page 383
- Increasing the time-out for the HP SIM Connector, page 383

If Your Installation or Upgrade Failed, Capture the Logs

(Windows management servers only) You can quickly gather system information and log files for troubleshooting by running the `srmCapture.cmd` program in `<HP Storage Essentials installation directory>/tools`.

IMPORTANT: The `srmCapture.cmd` program requires that `zip.exe` is in the same folder as `srmCapture.cmd`. If you are missing `zip.exe`, you can find it in the tools directory of the management server CD.

The following information is gathered by `srmCapture.cmd`:

- List of environment variables, look for file `srmListEnvVar.txt`.
- Results from running `ipconfig /all`, look for file `srmListIpconfigAll.txt`.
- Results from running ` netstat -noab`, look for file `srmListNetstatNoab.txt`.
- Results from running `netstat -rte`, look for file `srmListNetstatRte.txt`.
- Results from running `netsh diag show test`, look for file `srmListNetshDiagShowTest.txt`.
- Install wizard log files (all files are found in `%systemdrive%\srmInstallLogs`).
- `srmwiz.ini`.
- Oracle export log file.
- File SRM log files.
- File SRM configuration files.
- HP SIM install log file
- Oracle log files
- Zero G registry content

If you see a message resembling the following, "`Current location, d:\Tools, is not writable`," the current working subdirectory is not writable. The `srmCapture.cmd` program will go through the following directories in order until it finds one that is writeable:

1. %temp%
2. %tmp%
3. %systemdrive%

Checking Installation Log Files

- The following log files are generated by the installer and can be found on the management server in the following directories: **C:\srmInstallLogs** includes these log files:

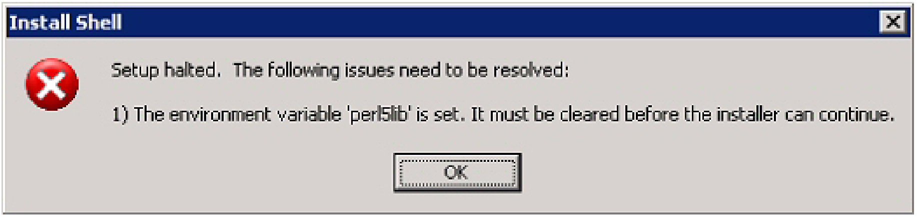
  - **srmInstall.log** — This is the master log file of the installation wizard session. It provides information for troubleshooting installation of the management server and related components.
  - **srmInstallOracle10g.log** — Log file that provides information about the Oracle 10g database installation.
  - **srmInstallSrm.log** — Log file that provides information about the management server installation.
  - **srmOracle<monthyear>Patch.log** — Log file that provides information about the installation of the specified Oracle patch.

    Where <monthyear> is the date of release of the specified Oracle patch.

  - **srmInstallConnector.log** — Log file that provides information about the SIM Connector installation.
  - **srmInstallSim.log** — Log file that provides information about the installation of HP Systems Insight Manager.
- **C:\hpsim.log** — HP SIM installation log file created by the HP SIM installer. This file is located on the server where HP SIM is installed.

"The environment variable 'perl5lib' is set." Message

(Windows only) If the perl5lib environment variable is set, the installation/upgrade fails with the following message:



Setup halted. The following issues need to be resolved:

1) The environment variable 'perl5lib' is set. It must be cleared before the installer can continue.

Figure 27 Perl5lib environment variable message

This variable may have been set by another application. The environment variable may have also been set if your upgrade of Oracle was suddenly stopped, for example, as a result of a power outage. You must remove the perl5lib environment variable before you can run the installation/upgrade again. For information about removing environment variables, refer to the documentation for the Windows operating system.

“SEVERE: OUI-10029...” Message

The installation wizard lets you specify an installation location for Oracle 10g. If you specify a location that is being used by another program or if you specify the Oracle DVD drive, Oracle displays the following message:

```
SEVERE: OUI-10029: You have specified a non-empty directory to install this
product. It is recommended to specify either an empty or a non-existent
directory. You may, however, choose to ignore this message if the directory
contains Operating System generated files or subdirectories like lost+found
```

If you see this message, contact customer support. Engineering has found this message to indicate the installation of your Oracle database may have failed.

Brocade API Switches Displaying Stale Data

All Brocade API switches are placed in quarantine after you upgrade to Build 6.0. This means previous data is preserved but you can no longer update the data using Discovery Data Collection. Therefore, data such as topology, zoning information will be stale until you migrate to Brocade SMI-A. See ”Discovering Brocade Switches” on page 116

SIM Connector Fails to Install for Single–Server Configurations

The installation for the SIM Connector fails when the password for SIM_MANAGER is not set to `quake`. When Oracle is upgraded from 9i to 10g as part of the upgrade, the password for the SIM_MANAGER database account is reset to the default value which is quake. You must use the mxpassword command in HP SIM to reset the SIM_MANAGER password:

- Microsoft Windows: Enter the following at the command prompt:

```
C:\> mxpassword -m -x MxDBUserPassword=mynewPass
```

  where `mynewPass` is your new password for the Oracle database.

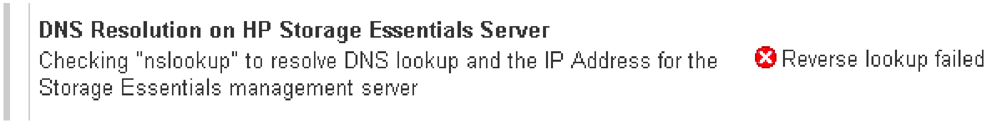
- Linux: Enter the following at the command prompt:

```
[/opt/mx/bin]# ./mxpassword -m -x MxDBUserPassword=mynewPass
```

  where `mynewPass` is your new password for the Oracle database.

“Reverse Lookup Failed” Message (Windows only)

If you do not have DNS installed on a server, you are shown the following “Reverse Lookup Failed” message in the Verify System Requirements screen of the Storage Essentials for Windows installation wizard:



DNS Resolution on HP Storage Essentials Server

Checking "nslookup" to resolve DNS lookup and the IP Address for the Storage Essentials management server

✖ Reverse lookup failed

Figure 28 Reverse Lookup Failed

This error message is displayed when the Storage Essentials installation wizard can not detect the fully qualified domain name assigned to the server. You will need to provide the fully qualified domain name manually:

1. Enter the following at the command prompt, where `mycomputer` is the shortened DNS name of the machine:

   ```
   nslookup mycomputer
   ```

   The fully qualified domain name and IP address is displayed, as shown in the following example:

   ```
   Server:   server.yourcompany.net
   Address:   192.168.135.52
   Name:     mycomputer.domain.my.net
   Address:   192.92.12.131
   ```

2. Open the following file in a text editor, such as Microsoft Notepad:
   `C:\windows\srmwiz.ini`
3. Assign the fully qualified domain name to the FQDN property in the `srmwiz.ini` file and save the file.
4. Do one of the following:
   - Rerun the installation wizard (Start the Storage Essentials installation wizard (double-click **setup.exe** in the `srm` directory or re-insert the Storage Essentials CD in the CD–ROM drive of the Storage Essentials server)
   - Run `connector.exe`.

Re-installing the HP SIM Connector (If Your HP SIM User Name or Password is Incorrect or was Changed)

If you enter the credentials for the HP SIM server incorrectly, you must re-install the SIM Connector component to provide the correct credentials:

1. Put the Storage Essentials CD-ROM in the CD-ROM drive of the management server.

   The Welcome screen is displayed. The installer determines that all components are installed on the system and will go directly to the HP Systems Insight Manager Service Account Credentials screen.
2. Make your changes and click **Next**. The installer re-installs the HP SIM Connector.

Increasing the time-out for the HP SIM Connector

The HP SIM Connector times out if HP-SIM is not fully running in five minutes after system startup. HP SIM may take longer than five minutes to start if HP-SIM has just been upgraded where there are many events in the HP-SIM database, for example. You may increase the five minute time-out by changing connector-time-out-minute in

`%JBOSS4_DIST%\server\appiq\conf\hp-config.xml` on the management server:

```
<?xml version="1.0" encoding="UTF-8"?>

  <HP-config>HP configuration

    <host-name>management-server-hostname</host-name>

    <trusted-host>management-server-hostname</trusted-host>

    <trusted-host>192.168.1.100</trusted-host>
```

```
<admin-user>management-server-domain\administrator</admin-user>
    <SIM-on-windows>true</SIM-on-windows>

<event-unknown-severity-handling>false</event-unknown-severity-handling
>
<connector-time-out-minute>MINUTES</connector-time-out-minute>
  </HP-config>
```

Set MINUTES to an appropriate value for your system (like 30, 60, or 90) based on the startup time of HP SIM.

Storage Essentials Menus Are Not Shown in HP SIM

If the HP SIM Connector component was not installed correctly or you entered the wrong credentials on the HP Systems Insight Manager Service Account Credentials screen, the Storage Essentials menus will be missing on the HP SIM menus. You must re-install the HP SIM Connector. See, Re-installing the HP SIM Connector (If Your HP SIM User Name or Password is Incorrect or was Changed), page 383.

NoSuchElement Error

See "Using the CLI Command While Upgrading" on page 415.

Difficulty Displaying Storage Essentials Pages After Generating a Custom Certificate

Generating a custom certificate for HP SIM from a Certificate Authority after HP Storage Essentials is installed results in HP Storage Essentials pages not being displayed. To resolve this, re-install the HP SIM connector as described in the *HP Storage Essentials Installation Guide.*

Troubleshooting the Oracle Database (Windows)

This section provides Oracle troubleshooting help:

- Use Only the Installation Wizard (or Unix Scripts) to Install/Upgrade Oracle, page 384
- Existing Oracle Database Is Detected, page 385

Use Only the Installation Wizard (or Unix Scripts) to Install/Upgrade Oracle

With this release of the product, the Oracle database is automatically installed using the new Installation Wizard (or Unix scripts) developed to install the management server along with the Oracle database used by the management server. Installing Oracle separately is no longer recommended.

IMPORTANT: Do not install the Oracle database separately, the management server Installation Wizard (or Unix scripts) automatically configures the Oracle database for use with the management server. If you install the Oracle database separately, the database will not meet the configuration settings required by the management server.

Existing Oracle Database Is Detected

If the Windows installation wizard installer (or the Unix installation scripts) detects an existing Oracle database, the following message is displayed: Existing Oracle Database is Detected. Call customer support if you need to uninstall the Oracle database.

Configuring the Java Console

It is recommended you configure your Java Console as follows for optimal performance. Please refer to the documentation for your Java Console for more information on how to make these changes.

To increase:

- The Memory, add -Xmx128m to the Java console
- The heap size, add -Xms128m to the Java console

java.lang.SecurityException: Failed to validate one time key

If you click the **Back** button in your Web browser, you may be shown the following message:

```
java.lang.SecurityException: Failed to validate one time key
```

You can safely ignore this message. This is expected behavior for security reasons. The product was designed to have tight security, and therefore it sometimes prevents the **Back** button from working.

"Data is late or an error occurred" Message

If you see the message "Data is late or an error occurred" when you try 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.

appstorm.<timestamp>.log Filled with Connection Exceptions

When an Oracle redo log becomes corrupt, the management server is unable to connect to the database. Whenever this occurs, the management server writes to the `appstorm.<timestamp>.log` file. Many exceptions may cause the application log on Windows to become full.

To correct this problem, stop the management server and Oracle, and 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_appstorm.<timestamp>.log` file, which can be found in one of the following locations:
   - **Windows:** `\oracle\admin\APPIQ\bdump`.
   - **Unix systems:** `$ORACLE_BASE/admin/APPIQ/bdump`

   You can verify if the redo log listed in the `alert_appstorm.<timestamp>.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;
```

The following sections describe how to start the database for the management server.

Windows

In the Services window, make sure the OracleOraHome92TNSListener service has started and is set to automatic. See 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.

Unix systems

To verify the Oracle service has started, enter the following at the command prompt:

```
# ps -ef | grep ora
```

If the service has started, output resembling the following is displayed:

```
/opt/oracle/product/9.2.0.1.0/bin/tnslsnr LISTENER -inherit
 ./appstormservice /opt/productname/ManagerData/conf/solaris-wrapper.
  oracle   356     1  0   Jul 30 ?        0:01 ora_pmon_APPIQ
  oracle   358     1  0   Jul 30 ?        0:26 ora_dbw0_APPIQ
  oracle   360     1  0   Jul 30 ?        1:13 ora_lgwr_APPIQ
  oracle   362     1  0   Jul 30 ?        0:39 ora_ckpt_APPIQ
  oracle   364     1  0   Jul 30 ?        0:10 ora_smon_APPIQ
  oracle   366     1  0   Jul 30 ?        0:00 ora_reco_APPIQ
  oracle   368     1  0   Jul 30 ?
```

If you find your service for the Oracle has not started, you can start the service by entering the following at the command prompt:

```
# /etc/rc3.d/S98dbora start
```

If you need to stop the service for Oracle, enter the following at the command prompt:

```
# /etc/rc3.d/S98dbora stop
```

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. To save space, the text has been shortened:

```
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/conf` directory.
2. Open the `cim.extension.parameters` 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` is the new port for the CIM extension

3. Save the file.
4. Restart the CIM extension for your changes to take effect.

> **NOTE:** The CIM extension looks for parameters in the `cim.extension.parameters` file whenever it starts, such as when it is started manually or when the host is rebooted.

5. 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.

   Enter the port number on the System Protocol Settings page (**Options** > **Protocol Settings** > **System Protocol Settings**) under the WBEM section. See the SIM documentation for more information.

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 cim.extension.parameters" column provides information on how you would modify the `cim.extension.parameters` file. See "Permanently Changing the Port a CIM Extension Uses (UNIX Only)" on page 388.

Table 27 Troubleshooting Firewalls

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
Firewall port 4673 opened between host and management server.	start		10.250.250.10 OR 172.31.250.10 OR 192.168.250.10 Communication Port: 4673

Table 27 Troubleshooting Firewalls (continued)

Configur-ation	**Manual Start Parameters for CIM Extension**	**If Mentioned in cim.extension.parameters**	**Step 1 Discovery and RMI Registry Port**
Firewall port 1234 opened between host and management server.	start -port 1234	-port 1234	10.250.250.10:1234 OR 172.31.250.10:1234 OR 192.168.250.10:1234 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 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 Communication Port: 1234
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012.	start -on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012	-on10.250.250.10:1234 -on172.31.250.10:5678 -on 192.168.250.10: 9012	10.250.250.10:1234 OR 172.31.250.10:5678 OR 192.168.250.10: 9012 Communication Port: 1234, 5678, 9012

Table 27 Troubleshooting Firewalls (continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
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.	start		172.16.10.10 Communication Port: 17001
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 Communication Port: 17001

Table 27 Troubleshooting Firewalls (continued)

Configur-ation	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
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 -on 172.31.250.10:5678 -on 192.168.250.10:9012	-on10.250.250.10:1234 -on172.31.250.10:5678 -on 192.168.250.10:9012	172.16.10.10:1234 OR 172.16.20.20:5678 OR 172.16.30.30:9012 Communication Port: 1234, 5678, 9012
False DNS or IP is slow to resolve.		jboss.properties, cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673
No DNS, never resolve.		jboss.properties cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable 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. Communication Port: 4673

Table 27 Troubleshooting Firewalls (continued)

Configuration	Manual Start Parameters for CIM Extension	If Mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
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 -on10.250.250.10:1234 -on172.31.250.10:5678 -on192.168.250.10:9012 -credentials abcuser:passwd	-on10.250.250.10:1234 -on172.31.250.10:5678 -on 192.168.250.10:9012 -credentials abcuser:passwd	10.250.250.10:1234 OR 172.31.250.10:5678 OR 192.168.250.10:9012. Specify abcuser and passwd in the discovery list. Communication Port: 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 or 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-separated 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-separated 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.

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.

This section contains the following topics:

- Installing the Certificate by Using Microsoft Internet Explorer 6.0, page 394

- Changing the Security Certificate to Match the Name of the Server, page 394

Installing the Certificate by Using Microsoft Internet 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**.
3. When you are told there is a problem with the site's security certificate, click **View Certificate**.
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**.

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 program to delete the original certificate, and then use the generateAppiqKeystore program to create a new certificate and to copy the new certificate to the management server.

Windows

To change the certificate on Windows:

1. Go to the `%MGR_DIST%\Tools` directory.
2. To delete the original certificate, enter the following at the command prompt:
   ```
   %MGR_DIST%\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:

   ```
   %MGR_DIST%\Tools> generateAppiqKeystore.bat
   ```

4. If the program is unable to detect a DNS name, enter the following at the command prompt:

   ```
   %MGR_DIST%\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:

   ```
   %MGR_DIST%\Tools> generateAppiqKeystore.bat copy
   ```

   The new certificate is copied to the correct location.

and Linux

To change the certificate on and Linux:

1. Go to the `[Install_Dir]` directory and run the following command:

   ```
   eval `./usersvars.sh`
   ```

   IMPORTANT: The quotes in the example must be entered as left single quotes as shown.

2. Go to the following directory:

   ```
   [Install_Dir]/Tools
   ```

   where `[Install_Dir]` is the directory into which you installed the management server.

3. To delete the original certificate, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl del
   ```

   The original certificate is deleted.

   NOTE: If you see an error message when you enter this command, a previous certificate may not have been created. You can ignore the error message.

4. To create a new certificate containing the DNS name of the management server, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl
   ```

5. If the program is unable to detect a DNS name, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl create mycomputername
   ```

   where `mycomputername` is the DNS name of the computer

6. To copy the new certificate to the management server, enter the following at the command prompt:

   ```
   perl generateAppIQKeyStore.pl copy
   ```

   The new certificate is copied to the correct location.

Troubleshooting Discovery and Discovery Data Collection

This section contains the following topics:

Troubleshooting Mode

Troubleshooting Mode can be used to assist you in identifying and resolving host configuration issues during discovery, as described in the following steps:

1. If errors occur during discovery, an error message will display at the top of the screen below the discovery step where the errors occurred. If you receive an error message, enable Troubleshooting Mode by selecting the **Enable Troubleshooting Mode** check box located near the top of the page for each discovery step.
2. A red icon will display in the **Problems** column for each host for which a problem was detected. Clicking this icon for a particular host will cause a list of troubleshooting tips to display below the **Enable Troubleshooting Mode** check box. Use these tips to assist in the resolution of configuration problems for that host.
3. You can also enter Troubleshooting Mode by clicking the link located in the error message for one of the discovery steps. For example, if you are on discovery step 3, you can click the "Discovery->Setup in Troubleshooting mode" link located in the step 1 error message. Clicking this link will bring you to the step 1 page with Troubleshooting Mode enabled.

When Troubleshooting Mode is enabled during Discovery Data Collection, the following additional information is provided to assist in the identification of configuration issues:

- Host OS
- CIM Extension Version
- HBA (Driver Version)
- Multipathing

Unable to discover Emulex host bus adapters

The Emulex driver does not contain the required library that is required by HP Storage Essentials. You must install Emulex HBAnywhere software so that HP Storage Essentials can discover hosts configured with HBAnywhere and hbatest can detect the Emulex host bus adapter.

CIMOM Service Not Starting After Trying to Discover Sybase or SQL Server Applications

If your management server is running on Linux, you will not be able to discover Sybase or SQL Server applications. If you already added a Sybase or SQL Server entry to be managed in the Discovery setup page and performed a Get All Element Details operation, entries for the Sybase or SQL server will be added to the oracle listener configuration file. On the next system reboot, or on the next restart of the Oracle service, the Oracle listener will error out, and the CIMOM service will not start.

To correct the issue:

1. Edit `ORA_HOME/network/admin/listener.ora` and remove the SID_DESC text blocks containing the `PROGRAM=hsodbc` string.

   where `ORA_HOME` is the Oracle home

   For example: `. /opt/oracle/product/9.2.0.4`

   If you have a SID_DESC block similar to the text block below, remove this entire block.

   ```
   (SID_DESC =
   (SID_NAME = SQLSERVERSID)
   (ORACLE_HOME = /opt/oracle/product/9.2.0.4)
   (PROGRAM = hsodbc)
   ```

2. Restart Oracle with the following command:

   ```
   /etc/init.d/dbora restart
   ```

3. Restart the appstormanager service.
4. After the service has started, delete any Sybase or SQL entries from the Application tab in the discovery setup page. This is necessary to prevent them from being re-added to the `listener.ora` on further discoveries.

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. See 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 are sent as follows:

   - `gaedemail` property is empty - The e-mail is sent to users whose roles have System Configuration selected.
   - `gaedemail` property is populated - The e-mail is sent only to users whose e-mail is assigned to the `gaedemail` property.

3. If you want additional users to receive the status reports for Discovery Data Collection, do the following:

   a. Select **Options** > **Storage Essentials** > **Manage Product Health**, and then click **Advanced** in the Disk Space tree.

   b. Click **Show Default Properties** at the bottom of the page.

   c. Copy the `gaedemail` property.

   d. Return to the Advanced page.

   e. Paste the copied text into the Custom Properties box.

   f. Assign the e-mail accounts you want to receive the report to the `gaedemail` property. For example, if you want user1@mycompany.com and user2@mycompany.com to receive these status reports, modify the `gaedemail` property in the Custom Properties box as follows:

   ```
   gaedemail=user1@mycompany.com;user2@mycompany.com
   ```

   NOTE: Make sure the hash (#) symbol is removed from the `gaedmail` property.

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

Increasing the Time-out Period and Number of Retries for Switches in Progress

If you are having difficulty obtaining information from switches with SNMP connections 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 switch 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. If it does not receive a response from the switch a second time, the management server says it cannot contact the switch.

To change the time-out period and number of retries for switches, modify the properties as described in the following steps:

1. Access the management server.
2. Select **Options** > **Storage Essentials** > **Manage Product Health**, and 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 28 on page 399.
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. 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 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 28 Time-out Properties

Switch	Property
McDATA/Connectrix discovered through SNMP	`cimom.McData.Snmp.Timeout`
Cisco	`cimom.Cisco.Snmp.Timeout`
Other switches discovered through SNMP: • Sun StorEdge • QLogic	`cimom.snmp.switch.timeout`

1. To modify the number of retries, repeat steps 4 through 6 by copying and pasting the property specified in the table below. 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 29 Retry Properties

Switch	Property
McDATA/Connectrix discovered through SNMP	`cimom.McData.Snmp.Retries`
Cisco	`cimom.Cisco.Snmp.Retries`
Other switches discovered through SNMP: • Sun StorEdge • QLogic	`cimom.snmp.switch.retries`

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

"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 these items, run Discovery Data Collection again. If you continue to see the error message, contact customer support.

An Element is Not Listed on the Discovery Data Collection Page

If HP SE cannot identify an element passed to it by the HP SIM Connector, the element is not listed when you run Discovery Data Collection. HP SE may have failed to identify the device due to an incorrect credential.

Check the `appstorm.yyyymmdd-hhmmss.log` and `cimom.yyyymmdd-hhmmss.log` to look for problems.

You can test the element credentials in HP SE to verify that they are correct.

1. Select **Tools > Storage Essentials > Home**.
2. Click **Discovery** and then click **Setup**.
3. Click **Add Address**.
4. Enter the IP address or DNS name and the credentials you want to test. Click **OK**.

5. Click **Test**.
6. When you are finished, select the IP address or DNS name you added and click the Delete icon.
7. Repeat the steps to discover the element. See "Discovering Elements" on page 113 for instructions.

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/Logs for Brocade Switches in Same Fabric

Duplicate listings: Targets tab

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
```

Duplicate Logs

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
```

Duplicate entries for the same element on the Discovery Data Collection page

If an element is discovered through two different protocols, it may be listed twice on the Discovery Data Collection page.

If you want to change the protocol used to discover an element that has already been discovered, delete the element before attempting to rediscover it. See "Discovery Data Collection" on page 153 for more information.For some elements, duplicate entries may result if a second protocol is available. For example, you could choose to discover an element through a supported API, but if the element supports SMI-S, and the SMI-S provider is also available, the element could be discovered again. In this example, you could fix the issue by disabling the SMI-S provider.

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.

Management Server Does Not Discover Another Management Server's Database

In some situations, the management server may not discover another management server's database. Make sure that the Oracle monitoring software (CreateOracleAct.bat for Microsoft Windows) is installed on the management server to be discovered and that the Oracle instance is added to the discovery list.

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. See 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, see 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 the 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.

Do Not Run Overlapping Discovery Schedules

If you are creating multiple discovery schedules, care must be taken to avoid scheduling conflicts—concurrently scheduled Discovery tasks—and that each scheduled task has enough time to start and finish before the next Discovery task is scheduled to start. For example, if a scheduled Discovery is still in progress when another scheduled Discovery attempts to start, the Discovery task that attempts to start will not start, because the first discovery is still running. The discovery that is unable to start is rescheduled according to its recurring rule. If the discovery task is scheduled to run on a daily basis, for example, then the discovery will start again on the next day. To check the status of scheduled discovery tasks, view the `appstorm.<timestamp>.log` file in the following directory:

```
[Install_Dir]\jbossandjetty\server\appiq\logs
```

"This storage system uses unsupported firmware. ManagementClassName: class_name" Message

The following message is displayed when an LSI storage system is discovered, and is running unsupported firmware:

```
This storage system uses unsupported firmware. ManagementClassName:
class_name
```

Where `class_name` is the management class name for the unsupported array.

The management class name for the unsupported array is displayed in the message.

New releases of storage system firmware are supported with each new release of this software. See the support matrix for your edition for the latest information on supported firmware.

Troubleshooting Topology Issues

This section contains the following topics:

- About the Topology, page 404
- Undiscovered Hosts Display as Storage Systems, page 407
- Solaris Machines Appear to Have Extra QLogic HBAs, page 407

About the Topology

The software determines the topology by looking at the following:

- **Fibre Channel switch** - The Fibre Channel switch contains a list of all elements within the fabric. The software 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.

Table 30 on page 405 provides details about how to correct problems that might occur during discovery and data collection.

Table 30 Troubleshooting Discovery and Discovery Data Collection

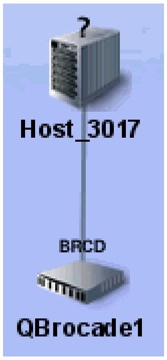
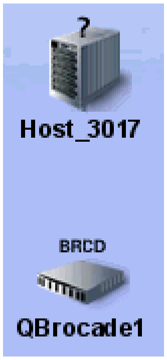
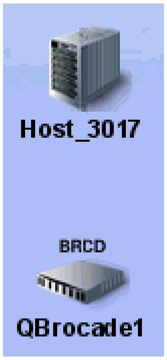
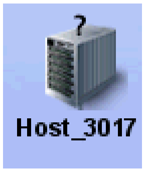
Scenario	Description	What to do
 The host appears discovered and it is connected to the switch.	The software is aware of the host, but it cannot obtain additional information about it.	Verify that a CIM extension is installed on the host. Discover the host again in HP SIM, and then run Discovery Data Collection.
 Host appears discovered and it is not connected to the switch.	The switch was previously made aware of the host, but it can no longer contact it. If the steps provided do not work, see "Link Between a Brocade Switch and a Host Disappears from the Topology" on page 407.	Verify that the host is on and the network cables are connected to it. Try discovering the element again in HP SIM, and then run Discovery Data Collection.

Table 30 Troubleshooting Discovery and Discovery Data Collection (continued)

Scenario	Description	What to do
 The host appears managed, but it is not connected to the switch.	There is a problem with Discovery Data Collection from the host. If the steps provided do not work, see "Link Between a Brocade Switch and a Host Disappears from the Topology" on page 407.	Try Discovery Data Collection again. 1.
 The element appears discovered, but a connected switch does not appear.	The switch has not been discovered.	Try discovering the switch again. See "Discovering Elements" on page 113. 1.
When discovering a Windows-based host, the correct IP address is entered, but the host does not appear in the topology. The following can be seen on the host: • In Windows Event Manager the `WinMgmt.exe` process is not running. This process starts WMI.* • In the Windows Event Log, DCOM error messages are shown.	An invalid user account was entered	Enter a valid user account that has administrative privileges so it can start WMI.

*The CIM extension for Microsoft Windows enhances Windows Management Instrumentation (WMI) so that it can gather information from host bus adapters and make the information available to the management server.

IMPORTANT: One way to determine what is happening is to look at the log messages during discovery and getting element details. See "Viewing Log Messages" on page 161 for more information.

Undiscovered Hosts Display as Storage Systems

On rare occasions, the management server displays undiscovered hosts as storage systems in System Manager. To resolve this issue, provide the host's world wide name (WWN) as described in the following steps:

1. Determine the host's WWN. This information is available on the IEEE Standards Association web site at http://standards.ieee.org/regauth/oui/oui.txt.
2. Select **Options** > **Storage Essentials** > **Manage Product Health**, and then click **Advanced** in the Disk Space tree.
3. Click **Show Default Properties** at the bottom of the page.
4. Copy the following property:

```
#hostPortWWNs=
```

5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Uncomment the `hostPortWWNs` property by removing the hash mark (#) in front of `hostPortWWNs`.
8. Enter the host's WWN in hexadecimal format. Multiple WWNs can be entered as a comma-separated list. For example:

```
hostPortWWNs=00-01-C9,00-01-C8
```

9. Click **Save**.

Solaris Machines Appear to Have Extra QLogic HBAs

Solaris machines using Fibre Channel drives internally will always appear to have extra QLogic HBAs. After discovering a Solaris machine, internal fiber channel drives will show an extra QLogic adapter on the host adapters page.

No Stitching for Brocade Switches with Firmware 3.2.0

Stitching does not appear for hosts attached to Brocade switches running firmware 3.2.0. There is no stitching when the PID format is 0. The port setting must be the same for all Brocade switches in the fabric, or the fabric will become segmented. The PID format should be set to `1` for all Brocade switches running firmware later than 2.6.0 and 3.0. The PID=0 setting is a legacy Port ID format that does not support the numbers of ports beyond 16.

Link Between a Brocade Switch and a Host Disappears from the Topology

If a link that used to work between a Brocade switch and a host disappears from the topology, you may need to rediscover the Brocade switch and the host. Also, confirm that both are online and there are no network connection issues. As a last resort, you may need to reboot the switch. In some instances, the API of the Brocade switch has been known to hang. Rebooting the switch clears the switch of the API hang.

Incorrect Topology Sometimes Displayed for CNT Switches

The CNT SMI-S provider for CNT switches does not return the correct topology information when more than one fabric is managed by the same InVSN™ Storage Network Manager. McDATA, which completed its acquisition of CNT in the summer of 2005, has been made aware of this issue.

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 you are 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.

Sun 6920 Storage Systems: “ReplicatorSQLException: Database create error”
During Discovery Data Collection

While performing a Discovery Data Collection, the Sun 6920 provider will return the error “ReplicatorSQLException: Database create error” under certain circumstances. This error appears in the management server logs but can be safely ignored. Sun Microsystems is aware of this issue.

Mirrored Volumes Cannot Be Provisioned on Sun 6920 Storage Systems

Mirrored volumes are not represented properly by the management server. You cannot use the management server to provision mirrored volumes on Sun 6920 storage system.

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, discover the McDATA switches as described in "Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries" on page 105.

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, if 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. See 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 because the service processor is 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 IOs per second.

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 or three minutes and 45 seconds on Unix systems. 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 the `cimom.CimXmlClientHttpConnectTimeout` property to more than 20 seconds on Windows or three minutes and 45 seconds on Unix systems, 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. Select **Options** > **Storage Essentials** > **Manage Product Health**, and 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.
5. Return to the Advanced page.
6. Paste the copied text into the Custom Properties box.
7. Make your changes in the Custom Properties box. 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 milliseconds 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**.

"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 tries 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 Discovery Data Collection operation the management server performs 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. Select **Options** > **Storage Essentials** > **Manage Product Health**, and 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`.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your changes in the Custom Properties box by changing the value of `cimom.mcData.swapiThrottle`. For example, the default is 200 ms. To change the value to 800 ms, 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**.

Re-establishing Communication with EFCM

To re-establish communication with EFCM, perform the following steps:

1. To check the status of the connection, click the **Test** button on the Discovery Setup screen. If the McDATA provider reports that it can connect to EFCM, the connection has been restored. A provider is a component of the management server that is used to gather information about an element. In this case, the McDATA provider gathers information about McDATA switches for the management server. To ensure the management server does not have corrupt data as a result of the loss of communication, perform Discovery Data Collection to obtain the latest information from the element.
2. If the ping to EFCM fails, there is a network problem that must be resolved. Once network connectivity is restored, click the **Test** button to verify the McDATA provider can communicate with EFCM, then do a Discovery Data Collection.
3. If the Test button results from the management server indicate that it still cannot communicate with EFCM, wait approximately three minutes for the lost SWAPI connection to time out, and then click the **Test** button again. If this works, do a Discovery Data Collection.
4. If the Test button results continue to indicate a lost connection after three minutes, perform the following steps to restore the connection. Note that these steps involve restarting services on the EFCM server. Any other applications using SWAPI to communicate with EFCM are affected by these actions.
   a. Open the EFCM client. Make sure that the EFCM is still actively managing at least one switch. If there are no switches under management, you will not be able to connect to this EFCM.
   b. On the EFCM server, stop and restart the Bridge Agent service. Repeat Steps 1 through 3. If the connection is still down, proceed to Step c.
   c. On the EFCM server, stop and restart the EFCM services. On Windows, use the McDATA EFCM Manager options in the **Start** > **Programs** menu. Repeat Step 1 through 3. If the connection is still down, proceed to Step d.

d. Reboot the EFCM server. Repeat Step 1 through 3. If the connection is still down, proceed to Step e.

e. Stop and restart the service for the management server. Repeat Step 1 through 3. If the connection is still down, proceed to Step f.

f. Reboot the management server. Repeat Step 1 through 3. If the connection is still down, proceed to Step g.

g. If none of the above steps have restored the connection, see the support matrix for your edition to determine if the EFCM and switch versions are all supported. Contact technical support for further information.

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, use the **Test** button on the discovery screen to check the status of the SWAPI connection. If necessary, 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, run Discovery Data Collection for this element to update the zoning information. See "Discovery Data Collection" on page 153 for more information.

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 that you want to communicate through a secure connection (SSL) and another that 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 following steps. 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. Select **Options** > **Storage Essentials** > **Manage Product Health**, and 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.
4. Return to the Advanced page.
5. Paste the copied text into the Custom Properties box.
6. Make your changes in the Custom Properties box. 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.

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 to 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**, and then click **Advanced** in the Disk Space tree.
2. Paste the following text into the Custom Properties box.

   ```
   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 200,000 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 starts to question whether its partner is still alive. If one entity (management server or extension) does not receive a message from the other during the interval set by the timeout property, it sends an “are you there” message. If that message is not acknowledged during the interval set by the timeout

property, the entity concludes that the connection is no longer functioning. The CIM extension stops attempting to make a connection. When this occurs on the side of the management server, the management server attempts to re-connect (and continues the attempt until the host becomes available). The default value is 1,000 ms. You are modifying it to wait 200,000 ms or 3.33 minutes.

3. Click **Save**.

ERROR replicating APPIQ_EVAStorageVolume during Discovery Data Collection for an EVA array

Errors similar to `ERROR replicating APPIQ_EVAStorageVolume` might occur when an EVA-specific data cache is updated during a Discovery Data Collection operation. For example, when Data Protector creates a snapshot, a new virtual disk is automatically created on the EVA array, and the EVA database used by the management server is updated to reflect this change.

If the EVA database is changed during a Discovery Data Collection operation, small replication errors may be seen as a result. The array information will be updated with the correct information next time Discovery Data Collection runs.

Recalculating the Topology

When Recalculating the topology or running Discovery Data Collection, other tasks using the management server can be delayed.because the management server must recalculate the topology, which is a resource intensive operation. Recalculation occurs after a Discovery Data Collection when provisioning is done, and when you choose to recalculate the topology manually.

During the recalculation period, you may not be able to log into the application. If you are already logged into the application, navigation may not be possible until the topology recalculation is complete.

Troubleshooting Provisioning

This section contains the following topics:

- Cannot Access a Resource Owned by Another Controller, page 414
- Error -56, page 414
- “Can't delete this zone” Message, page 415
- Changes in EFC Manager Requiring Discovery Data Collection, page 415

Cannot Access a Resource Owned by Another Controller

If you receive a message about not being able to access a resource owned by another controller, it is because you tried to access a controller that has not been discovered. You should discover all controllers on the LSI storage system.

For example, assume you discovered only one of the controllers on an LSI storage system with two controllers. If you want to change a volume, such as add or delete a LUN, you will not be able to make the change to the volume associated with the controller that has not been discovered.

See ”Discovering Switches, Storage Systems, NAS Devices, and Tape Libraries” on page 105 for more information on how to discover a controller.

Error -56

If you see `error -56`, the switch has network connection failures or problems. To solve the problem, make sure the switch is physically connected to the network, and then redo the task you were originally trying to complete.

If you now see `-21(OBJECT_NOT_FOUND)` errors, the switch needs to be rediscovered.

“Can't delete this zone” Message

If you see the following message when you try to delete a zone, move the zone to an inactive zone set, and then delete the zone.

```
Can't delete this zone, it is member of an Active Zoneset
```

Changes in EFC Manager Requiring Discovery Data Collection

If you use EFC Manager to delete zones or zone sets, perform Discovery Data Collection on the management server afterwards. The changes are not reflected by the management server until Discovery Data Collection is done.

Troubleshooting CLI Errors

This section includes the following:

- ”Using the CLI Command While Upgrading” on page 415
- ”NoSuchElement Error” on page 415

Using the CLI Command While Upgrading

When upgrading HP SIM integrated Storage Essential (SE), if you are logged in with a different user name to perform an upgrade (other than the original user name that was used to do the initial installation of the product), the corresponding (different) user is created in HP SIM and SE. That SE user is automatically associated with an SE role of SIMViewOnly. In addition, the SE user is also mapped to the default admin user in SE. If the installation user's SE role is different from the default SE admin user's role, attempts by the installation user to use the SE command line may result in “NoSuchElement” exceptions displayed in the command line window. To prevent this, assign the installation user a role, within Storage Essentials, that is the same as the default admin user. See ”About Security for the Management Server” on page 349 for more information.

NoSuchElement Error

See ”Using the CLI Command While Upgrading” on page 415.

Troubleshooting Hardware

This section contains the following topics:

- About Swapping Host Bus Adapters, page 415
- “Fork Function Failed” Message on AIX Hosts, page 416

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 are 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 Table 31 on page 416 provides a description of the known device issues. You can find the latest information about device issues in the release notes.

Table 31 Known Device Issues

Device	Software	Description

AIX host	NA	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 occurs, you see a message containing the following when you start the CIM extension:
		`CXWS 3.1.0.144 on 0.0.0.0/0.0.0.0 now accepting connections`
		To fix this situation, add the following line to the `/opt/APPQcime/tools/start` file on the AIX host:
		`export NSORDER=local,bind`

AIX host using an IBM Storage System	NA	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.
Hosts running SGI IRIX version 6.5.22 or 6.5.24	NA	If a host is 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.

Table 31 Known Device Issues (continued)

Device	Software	Description
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/output 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 HBAAPI. 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. Once you discover the host with the switches and storage, it reports its drives as being external. It reports 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."
Solaris host	HDLM	If you do a Discovery Data Collection for the host by itself, on the bindings page, the controller number begins with c-1, for example, `c-1t0d58`. Perform Discovery Data Collection on the host with storage and switches. The controller numbers are displayed correctly.

Table 31 Known Device Issues (continued)

Device	Software	Description
Solaris host	VxVM	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. 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 fiber are shown as external.
Windows host	VxVM	When a Windows host with VxVM is used, the SCSI bus number is always reported to be `1` in the SCSI bus column of the Disk Drives page.
Any host	NA	The Unmounted Volume box 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, or if your license does not allow you to discover a particular storage system. See the support matrix for Standard or Enterprise Edition to determine which storage systems you can discover. The List of Features is accessible from the Documentation Center (**Help** > **Documentation Center** in Storage Essentials).

Table 31 Known Device Issues (continued)

Device	Software	Description
IBM Storage Systems	Subsystem Device Driver (SDD) or MPIO (multipath I/O)	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 HBAAPI 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.

```
SYMAPI routine SymDevMaskSessionStart failed with error code 188: The
operation failed because another process has an exclusive lock on the local
Symmetrix.
```

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.

After the management server has detected the lock on the Symmetrix storage system, it tries to access the storage system for 15 minutes and then 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 before you remove the lock manually. Be sure that no other processes are occurring on the storage system. To learn how to remove the lock, see 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 Manager 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