

HP Systems Insight Manager 5.0 Installation and User Guide



* 5 9 9 1 - 4 4 9 8 *

Part number: 5991-4498
published December 2005
Edition: 4.0



© Copyright 2003-2005 Hewlett-Packard Development Company, L.P.

Legal Notices

The information in this document is subject to change without notice.

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

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

U.S. Government License

Proprietary computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

©Copyright 1983-2006 Hewlett-Packard Development Company, L.P. All rights reserved. Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under copyright laws.

Trademark Notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel® and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a U.S. registered trademark of Linux Torvalds.

Java™ is a US trademark of Sun Microsystems, Inc.

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

UNIX® is a registered trademark of The Open Group.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SUSE® is a registered trademark of SUSE Linux AG.

Publication History

The manual publication date and part number indicate its current edition. The publication date will change when a new edition is released. The manual part number will change when extensive changes are made.

To ensure that you receive the latest edition, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Please direct comments regarding this guide to:

Hewlett-Packard Company
HP-UX Learning Products
3404 East Harmony Road
Fort Collins, Colorado 80528-9599

Or, use this web form to send us feedback:

<http://docs.hp.com/assistance/feedback.html>

Typographic Conventions

We use the following typographical conventions.

`audit(5)` HP-UX manpage. *audit* is the name and *5* is the section in the *HP-UX Reference*. On the web and on the Instant Information DVD, it might be a hot link to the manpage itself. From the HP-UX command line, you can enter " `man audit` " or " `man 5 audit` " to view the manpage. See `man(1)`.

Book Title Title of a book. On the web and on the Instant Information DVD, it might be a hot link to the book itself.

`Command` Command name or qualified command phrase.

`ComputerOut` Text displayed by the computer.

Emphasis Text that is emphasized.

Emphasis Text that is strongly emphasized.

KeyCap

Name of a keyboard key. Note that **Return** and **Enter** both refer to the same key.

Term

Defined use of an important word or phrase.

UserInput

Commands and other text that you type.

Variable

Name of a variable that you can replace in a command or function or information in a display that represents several possible values.

[]

Contents are optional in formats and command descriptions. If the contents are a list separated by |, you must choose one of the items.

{ }

Contents are required in formats and command descriptions. If the contents are a list separated by |, you must choose one of the items.

...

Preceding element can be repeated an arbitrary number of times.

|

Separates items in a list of choices.

Table of Contents

1 Product overview	
Features.....	6
.....	9
What's new for HP SIM 5.0?.....	9
Product architecture.....	10
Central Management Server.....	10
Managed systems.....	11
System collections	11
Network clients.....	11
Authorizations.....	11
Default toolboxes.....	11
User privileges.....	12
Tools.....	12
Information storage.....	13
HP SIM audit log.....	13
Database.....	13
Database software.....	13
Secure access.....	14
Command line interface.....	14
Graphical user interface.....	14
Secure data transmission.....	14
Management protocols.....	15
Web server security	16
Self-signed certificates	16
X application security.....	16
Managing servers behind a firewall	16
2 Installation overview and requirements	
Process overview.....	17
System requirements.....	17
CMS requirements.....	17
HP-UX Central Management Server.....	17
HP-UX Patches.....	18
Linux Central Management Server.....	19
Windows Central Management Server.....	19
Managed System Requirements and Recommendations.....	20
SSH Requirements.....	23
3 Installing on Windows	
Preparing the system.....	24
Typical install.....	25
Custom install.....	27
Next steps.....	34
4 Installing on HP-UX 11i	
Preparing the System.....	35
Installing and Configuring the Software.....	36
Tuning HP SIM (Optional)	38
Next Steps.....	38
5 Installing on Linux	
Preparing the system.....	39
Installing and Configuring the Software.....	41
Automatically installing HP Systems Insight Manager	41
Manually installing HP Systems Insight Manager.....	41
After Installing HP Systems Insight Manager.....	43
Next steps.....	44

6 Upgrading from Insight Manager 7 Service Pack 2.3 to HP Systems Insight Manager 4.2	
Types of Migration.....	46
Performing an In-Place Migration.....	47
Performing a Remote Migration.....	48
7 Upgrading from HP Servicecontrol Manager to HP Systems Insight Manager	
Upgrading from SCM 3.0 to HP Systems Insight Manager 4.2.....	50
Upgrading Existing Managed Systems.....	53
8 Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0	
Upgrading HP SIM 4.x to HP SIM 5.0 - Windows.....	54
Typical install.....	55
Custom install.....	56
Upgrading HP SIM 4.x to HP SIM 5.0 - HP-UX.....	62
Next steps.....	64
Upgrading HP SIM 4.x. to HP SIM 5.0 - Linux.....	64
9 Uninstalling HP Systems Insight Manager	
Uninstalling HP Systems Insight Manager from a Windows system.....	66
Uninstalling HP Systems Insight Manager from an HP-UX system.....	66
Uninstalling HP Systems Insight Manager from a Linux system.....	67
10 Using the Graphical User Interface	
Accessing the GUI.....	68
Graphical User Interface Features.....	68
Default Home Page Features.....	69
Customizing the GUI.....	70
Customizing the Home Page.....	70
Customizing the System Status Panel.....	70
11 Using the Command Line Interface	
Logging in to the CLI.....	72
Logging in Directly on the CMS.....	72
Remotely Using an SSH Client.....	72
HP SIM Commands.....	72
12 Initial Setup	
Setting Up Managed Systems	75
Overview.....	75
Installing required and optional managed system software.....	75
Installing the ProLiant Support Pack on Windows systems for the first time.....	75
Installing the ProLiant or Integrity Support Pack on a Linux system for the first time.....	82
Installing the required software on an HP-UX system.....	82
Configuring the Managed System Software.....	83
Run the Configure or Repair Agents feature from the CMS.....	83
Setting Up Managed Systems Manually.....	85
Setting Up HP-UX Managed Systems Manually.....	86
Setting Up Linux Managed Systems Manually.....	89
Examples.....	90
Setting up Windows managed systems.....	90
Setting up remote Linux systems from a Linux CMS.....	90
Setting up remote HP-UX systems from an HP-UX CMS.....	91
Configuring Protocol Settings.....	91
Configuring and Executing Discovery.....	92
Configuring and Executing Automatic Discovery.....	92
Configuring and Executing Manual Discovery.....	93
Adding Users.....	94
Configuring Email Settings.....	96
Configuring Paging Settings.....	97
Setting Up Automatic Event Handling.....	97

Adding Toolboxes.....	100
Adding Authorizations.....	100
Setting Up Managed Storage Systems.....	102
Installing SMI-S Providers.....	102
Verifying SSL.....	102
Configuring SMI-S providers.....	102
Configuring HP SIM to discover storage systems.....	102
13 Configuration options	
CPU utilization during data collection.....	104
Overview.....	104
Implementation.....	104
GUI time-out policy.....	104
Overview.....	104
Implementation.....	105
HP SIM Audit Log configuration.....	105
Overview.....	105
Implementation.....	106
Lifetimes for Entries on the Task Results Page.....	106
Overview.....	106
Implementation.....	107
14 Troubleshooting	
GUI Issues.....	108
Installation Issues.....	108
Login Issues.....	108
Servicecontrol Manager and HP SIM Issues.....	109
Servicecontrol Manager and HP-UX 11i Issues.....	110
Upgrade Issues.....	111
glossary.....	112
Index.....	125

1 Product overview

HP Systems Insight Manager (HP SIM) combines the strengths of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Microsoft® Windows®, Linux, and HP-UX. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms.

HP SIM can be extended to provide system management with plug-ins for HP clients, storage, power, and printer products. Plug-in applications for rapid deployment, performance management, HP BladeSystem Integrated Management partition management, and workload management enable you to pick the value-added software required to deliver complete lifecycle management for your hardware assets.

Features

HP SIM provides the following features:

- **Easy and rapid installation.**
HP SIM installs on your server platform of choice running HP-UX, Windows, or Linux, or on a Windows desktop or workstation.
- **First Time Wizard.**
HP SIM provides you with step-by-step, online guidance for performing the initial configuration of HP SIM. The wizard helps you configure HP SIM settings on the Central Management Server (CMS).
- **Automatic discovery and identification.**
HP SIM automatically discovers and identifies systems attached to the network. Use discovery filters to prevent discovery of unwanted system types. Discovery filters enable you to limit discovery to specific network segments or IP address ranges.
- **Fault management and event handling**
HP SIM provides proactive notification of actual or impending component failure alerts. Automatic Event Handling enables you to configure actions to notify appropriate users of failures through e-mail, pager, or Short Message Service (SMS) gateway, and enables automatic execution of scripts or event forwarding to enterprise platforms, such as HP OpenView Network Node Manager or HP OpenView Operations.



NOTE Pager support is only for Windows-based CMS.

- **Consistent multisystem management**
HP SIM initiates a task on multiple systems or nodes from a single command on the CMS. This functionality eliminates the need for tedious, one-at-a-time operations on each system.
- **Secure remote management**
HP SIM leverages operating system security for user authentication and Secure Sockets Layer (SSL) and Secure Shell (SSH) to encrypt management communications.
- **Role-based security**
HP SIM enables effective delegation of management responsibilities by giving system administrators granular control over which users can perform which management operations on which systems.
- **Tool definitions**
HP SIM defines tools using simple XML documents that enable you to integrate off-the-shelf or custom tools. These tools can be command line tools, Web-based applications, or scripts. Access to these integrated tools is governed by role-based security.
- **Data collection and inventory reports**
HP SIM performs comprehensive system data collection and enables you to quickly produce detailed inventory reports for managed systems. Reports can be generated in HTML, XML, or CSV format.

- **Snapshot comparisons**
HP SIM enables you to compare configuration snapshots of up to four different servers or configuration snapshots of a single server over time. This functionally assists IT staff in pinpointing configuration issues that can contribute to system instability. Snapshot comparisons can also be used to save a picture of standard configuration for comparisons to other systems.
- **HP Version Control**
HP SIM automatically downloads the latest BIOS, driver, and agent updates for HP ProLiant servers running Windows and Linux, identifies systems running out-of-date system software, and enables system software updates across groups of servers. For HP-UX systems, Software Distributor is integrated into HP SIM.
- **Two user interfaces**
HP SIM provides a web browser graphical user interface (GUI) and command line interface (CLI) to help incorporate HP SIM into your existing management processes.
- **Ability to edit system properties on managed systems**
The **Edit System Properties** link on the **System Page** enables users with full configuration rights to reconfigure system properties for a single system. To set system properties for multiple systems, Click **Options**→**System Properties**→**Set System Properties**. This setting affects the system properties as reported by HP SIM, but it does not change the properties on the target systems.
- **Ability to suspend and resume monitoring of systems**
HP SIM enables you to set the timer for suspending monitoring. This enables a system to be excluded from status polling, identification, data collection, and the automatic event handling features of HP SIM. The **Suspend/Resume Monitoring** link under the **Tools & Links** tab of the **System Page** enables you to set the timer for suspending or resuming system monitoring. To suspend or resume system monitoring for multiple systems, Click **Options**→**System Properties**→**Suspend or Resume Monitoring**. The available suspend lengths include the predetermined increments of five minutes, 15 minutes, one hour and one day. The suspend feature can be turned on indefinitely.
- **Ability to install the OpenSSH tool**
runs from the CMS and installs the OpenSSH service onto target Windows systems and then runs the `mxagentconfig` command to complete the configuration.



NOTE This feature is only available on the Windows CMS.

- **Optional installation of OpenSSH through Initial ProLiant Support Pack Install**
HP SIM enables you to install OpenSSH through the Initial ProLiant Support Pack Install process by selecting **Install and initialize OpenSSH (Secure Shell)** on the **Initial ProLiant Support Pack Install** page.



NOTE This feature is only available on the Windows CMS.

- **Support for HP-UX Serviceguard clusters**
HP SIM recognizes HP-UX Serviceguard clusters and displays them in the GUI. HP Serviceguard Manager is opened by clicking a Serviceguard cluster in a search list and provides information on the clusters.
- **WBEM indications for HP-UX, Linux, and SMI-S devices**
HP SIM enables you to subscribe and unsubscribe to WBEM indications through the GUI. You can also subscribe or unsubscribe to WBEM indications from the CLI. For HP-UX, this feature is only available on 11i v2 September 2004.
- **HP Instant Support Enterprise Edition (ISEE)**
HP Instant Support Enterprise Edition (ISEE) is a proactive remote monitoring and diagnostic tool to help manage your systems and devices, a feature of HP support. ISEE gives you a simple, unified approach to monitoring your entire data center. Instead of using separate technologies for each of your platforms, you can monitor and manage a diverse IT environment with a single solution. ISEE helps you proactively

manage and support HP-UX, Microsoft Windows, Linux, OpenVMS, Tru64 UNIX®, NonStop and Sun Solaris servers, connected peripherals, and storage and network devices. It reduces cost and complexity by supporting both mission-critical and non-mission critical systems and devices. ISEE provides continuous hardware event monitoring and automated notification to identify and prevent potential critical problems. Through remote diagnostic scripts and vital system configuration information collected about your systems, ISEE enables fast restoration of your systems. Install ISEE on your systems to help mitigate risk and prevent potential critical problems.

- HP System Management Homepage

The System Management Homepage is a web-based application that provides a consolidated interface for single system management. By aggregating the data from HP web-based agents and management utilities, the System Management Homepage provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server.

- HP ProLiant Essentials Performance Management Pack (PMP) access

HP SIM provides a software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers and HP StorageWorks Modular Smart Array (MSA) shared storage. PMP tools available in HP SIM consist of Online Analysis, Offline Analysis, CSV File Generator Report, System Summary Report, Static Analysis Report, Configuration, Licensing, and Manual Log Purge. PMP is automatically installed with HP SIM and operates in conjunction with HP SIM. No software installation on the monitored servers is required, other than the Insight Management Agents. PMP 4.0 includes:

- Support for HP SIM 5.0 (This version of PMP does not support HP SIM 4.x.)
- Support for Oracle database (local or remote)
- Support for select HP Integrity servers

The following features are new in PMP 4.0.1:

- Support for Red Hat Linux 4.0
- Support for HP ProLiant BL25p Servers
- An option to remove or retain old PMP database files during the installation process

Refer to <http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/pmp/index.html> for more information.

- HP ProLiant Essentials Vulnerability and Patch Management Pack (VPM) access

VPM identifies and provides advice to resolve security vulnerabilities and delivers advanced patch management through automated acquisition, optimized deployment, and continuous enforcement of security patches. VPM must be manually installed from the Management CD and requires one license for each target system being managed. Five fully functional non-expiring licenses, for use on servers or desktops, are provided with VPM for evaluation purposes. For more information about installation and setup, refer to the *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster* and the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*, both on the Management CD. For more information on VPM, go to HP ProLiant Essentials Vulnerability and Patch Management Pack at <http://www.hp.com/servers/proliantessentials/vpm>.

- HP ProLiant Essentials Virtualization Management Software (VMS)

Virtual machine management capabilities integrated into HP SIM extends its capabilities to deliver unified management of an IT infrastructure consisting of both physical and virtual server resources and to simplify and consolidate the provisioning, management, and migration of all server resources from one central interface.

The virtual machine management capabilities in HP SIM are provided by integrating the HP ProLiant Essentials Virtual Machine Management Pack (VMM) and the HP ProLiant Essentials Server Migration Pack (SMP). Both these components are installed together as one component, but licensed separately.

- HP ProLiant Essentials Virtual Machine Management Pack

VMM provides central management and control for virtual machines of type Microsoft's Virtual Server and VMware's GSX or ESX. Using VMM, all virtual machines and virtual machine (VM) hosts can be managed from the HP Systems Insight Manager (HP SIM) console. The **Virtual**

Machine Management Pack displays a tree view of the VM hosts and VM guests in the left pane of the HP SIM console. After selecting a system in the left pane tree, information for the system selected appears in the right pane. You then have options to deploy, register, unregister, and upgrade. VMM is now integrated into HP SIM, Refer to <http://www.hp.com/servers/proliantessentials/vmm> for documentation and more information on VMM.

- HP ProLiant Essentials Server Migration Pack
SMP extends the functionality of the VMM to provide integrated physical-to-virtual (P2V) and virtual-to-virtual (V2V) migrations. The SMP enables you to simplify the server consolidation process, thereby freeing you to focus on other priorities. SMP now offers a new SMP license type that allows unlimited migrations for one year after the first migration is initiated. To purchase additional licenses, refer to <http://www.hp.com/servers/proliantessentials/smp>.
- HP BladeSystem Integrated Manager in HP Systems Insight Manager
HP SIM delivers a blade environment designed to consolidate access to blade deployment, configuration, and monitoring tools. Picture views are available of racks and enclosures. HP BladeSystem Integrated Manager is automatically installed with HP SIM, no license key is required. To access HP BladeSystem Integrated Manager, Click **Tools**→**Integrated Consoles**→**HP BladeSystem**. Refer to <http://h18004.www1.hp.com/products/servers/management/bsme/index.html> for more information.
- HP Configure or Repair Agents
The Configure or Repair Agents feature is an HP SIM feature that enables you to repair credentials for SNMP settings, System Management Homepage, or Management HTTP Server trust relationships on Windows, Linux, and HP-UX systems supported by HP SIM. For more information, refer to the Configure or Repair Agents Online Help at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- HP ProLiant Essentials Rapid Deployment Pack (RDP) - Windows Edition
RDP is a multiserver deployment tool that enables IT administrators to easily deploy large volumes of servers in an unattended, automated fashion. RDP is installed separately from HP SIM and requires a license for each server being managed. RDP is installed from its own CD. Refer to <http://www.hp.com/servers/rdp> for information about network environment setup, prerequisites for the deployment server, and installation instructions. When installed, you must register your product registration number to receive a license file. A license is required for each server being managed by RDP.
- Data collection and inventory reports for Superdomes and other complexes
Data collection and reporting has been added for Superdome systems and other cellular complexes. The type of data that can be collected includes information on chassis, cabinets, cells, memory, and hard partitions (nPars). The type of data actually collected depends on which filters are selected.
- HP Storage Essentials
HP is changing the economics of management in the data center. HP Storage Essentials is the first open, standards-based suite of storage products designed to integrate into HP SIM. For more information on HP Storage Essentials, go to <http://h18006.www1.hp.com/products/storage/software/esuite/index.html>.
- Manage SSH keys
The **SSH Keys** feature enables you to view and manage the public SSH keys, stored in the `known_hosts` file, from the CMS. SSH keys enable the CMS and a managed system to authenticate a secure connection.

What's new for HP SIM 5.0?

- The new look for the GUI which has the look and feel of other HP products.
- HP SIM no longer requires JRE to be installed on the client systems.

- Discover storage systems through their installed SMI-S providers. Refer to <http://www.hp.com/go/hpsim/providers> for information about the supported devices and SMI-S providers.
- Cluster Monitor monitors MSCS clusters only.
- Reports are now available in XML format.
- A new report engine is available along with new default reports.
- You can view a consolidated list of all server and storage events from a single event viewer and configure automated actions.
- You can view storage array capacity details, including unallocated space, RAID overhead, usable bytes assigned to ports, and usable bytes not assigned to ports.
- Flexible role-based security enables you to decide which administrators have access to server and storage details.
- You can launch server and storage element managers from a single system viewer.
- Lists and folders are now called collections.
- You can now assign privileges to operating system user groups to give these users access to HP SIM without creating each individual user.
- Access to discovery options, which include a **Discovery** page with tabs for **Automatic**, **Manual**, and **Hosts Files** configuration, has improved.
- New CLI commands, including `mxreport`, `mxcert`, `mxglobalprotocolsettings`, `mxglobalsettings`, `mxcollections`, and `mxgethostname`, are now available.
- You can set system properties for multiple systems at the same time.
- You can suspend or resume monitoring of multiple systems at the same time.
- A new tree view is available for system and cluster collections.
- You can create, edit, and delete discovery tasks.
- You can create new command line tools, including copying a file, removing a tool, and creating command line, web launch, and X Window tools on HP-UX and Linux systems.
- HP SIM supports the use of an Oracle database (locally or remotely) for Windows, HP-UX, and Linux.
- Support for managed system configuration has been added to include Linux, HP-UX, and Windows operating systems.
- The First Time Wizard provides you with step-by-step, online guidance for performing the initial configuration of HP SIM and helps you configure HP SIM settings on the (CMS).
- The HP Services analysis tools, **Web-Based Enterprise Services (WEBES)**, and **Open Service Event Manager (OSEM)**, generate service notifications to HP SIM through a specific SNMP trap type if analysis has determined there are serviceable events. If ISEE is installed, the service notification provided by WEBES and OSEM also provide status about the remote support incident.

Product architecture

HP Systems Insight Manager (HP SIM) leverages a distributed architecture that can be broken into three types of systems (central management server (CMS), managed systems, and network clients).

The CMS and the managed systems together are called the HP SIM management domain.

Central Management Server

Each management domain has a single CMS. The CMS is the system in the management domain that executes the HP SIM software and initiates all central operations within the domain. In addition to the HP SIM software, the CMS maintains a database for storage of persistent objects, and it can reside on a separate

system. Typically, applications for the [multiple-system aware \(MSA\)](#) tools also reside on the CMS. These applications are not required to reside on the CMS. They can reside anywhere on the network.

Because the CMS is a system within the management environment, it manages itself as part of the domain. You can add the CMS as a managed system within another management domain if you want to manage it using a separate CMS.

Managed systems

Systems that make up a management domain are called managed systems. A system can be any device on the network that can communicate with HP SIM, which includes servers, desktops, laptops, printers, workstations, hubs, storage systems, SANs, and routers. In most cases, these devices have an IP address or IPX address associated with them. A managed system can be managed by more than one CMS if desired.

Systems to be managed must have one or more [management agents](#) installed. WMI found a wide variety of agents, such as the ProLiant Management Agents based on [SNMP](#), [Windows Management Instrumentation](#) found on Windows systems or [WBEM](#) providers, such as the System Fault Management providers for HP-UX. Those agents provide management information and alerts (indications) to the CMS. The [SSH agent \(service\)](#) then enables the HP SIM CMS to log in to the managed system to execute commands through scripts.



NOTE IPX systems can only be discovered and managed on a Windows CMS.

System collections

System collections provide a way to group systems in the HP SIM database. A collection can be used to filter systems that share common attributes, such as operating system type or hardware type. System collections can also be arbitrary collections of systems. Systems can belong to one or more system collections. Many default shared system collections are provided, and you can create your own shared and private collections. Working with system collections increases your efficiency because you can perform a task on each system in a system collection with a single step.

Network clients

HP SIM can be accessed from any network client. The network client can be part of the management domain. The network clients must be running a compatible browser to access the [GUI](#) or a [SSH client application](#) to securely access the [CLI](#).



NOTE Access to the web server on the CMS can be restricted to specific IP address ranges for specific users.

Authorizations

An HP SIM user must have a valid operating system login on the CMS. After a user is added to HP SIM, he or she can be [authorized](#) to use a [toolbox](#) on one or more systems in the [management domain](#).

Each toolbox is associated with a set of tools that a user might need for a particular task, such as database administration or software management. Authorizing a user for a toolbox on a [system](#) or [system group](#) enables the user to run the associated set of tools on that system or systems that are members of the system group.



IMPORTANT Authorization for a toolbox might enable users with non-privileged access (for example, non-root users or users that are not members of the Windows Administrators group) to run tools as root/administrator or as another specified user. Be careful when granting users permission to run tools as root or administrator. Consider all the capabilities given by a tool, above and beyond the capabilities it is designed for, before you associate it with a toolbox.

Default toolboxes

The [All Tools toolbox](#) is a default toolbox installed with HP SIM. The **All Tools** toolbox provides complete access to all tools for the authorized system or system group. When a tool is added to HP SIM, the tool is automatically added to this toolbox. Tools cannot be removed from the **All Tools** toolbox, and the **All Tools** toolbox cannot be deleted from HP SIM. If you do not want a user to have access to all available tools for

a specific system or system group, they should not be authorized for the **All Tools** toolbox on that system or system group.



CAUTION Users assigned to the **All Tools** toolbox on the **CMS** can execute commands as any user. Therefore, these users could grant the full configuration rights user privilege to themselves.

Another default toolbox is the **Monitor Tools** toolbox. This toolbox contains tools that display the state of managed systems but not tools that change the state of managed systems.

HP SIM can have up to 32 defined toolboxes, including the default toolboxes. All toolboxes other than **All Tools** and **Monitor Tools** can be enabled, disabled, or deleted.

User privileges

Full configuration rights user

Full configuration rights users have been given special privileges to administer the HP SIM software. Full rights users manage:

- Authorizations
- Systems
- System groups
- Users
- Toolboxes
- Tools

In addition, full rights users maintain and back up the database and monitor the HP SIM audit log.

By default, root on an HP-UX or Linux CMS or the administrative account used to install HP SIM on a Windows CMS is assigned the full configuration rights user privilege, but this permission can later be revoked. This user is automatically authorized for the **All Tools** toolbox on all systems, including the CMS. The full configuration rights user privilege can be given to one or more users, and HP SIM requires that at least one user is a full configuration rights user.

Limited configuration rights user

Limited configuration rights users have limited capability to configure the CMS. They have permission to create, modify, and delete all reports and their own tools.

No configuration rights user

No configuration rights users cannot configure the CMS. Their ability to manage systems are based on their authorizations.

Tools

Tools are applications, commands, or scripts that are launched from within HP SIM. You can add custom tools into HP SIM and execute them across multiple systems simultaneously. Three types of tools are supported in the HP SIM environment: Web tools, X Window tools, and command line tools.

Web tools	Web tools must reside on a web server. The web server can be running on the CMS or a managed system. HP SIM launches the URL from a CLI or GUI. When a Web tool is launched from the command line, HP SIM opens a browser to display the tool. When a Web tool is launched from the HP SIM GUI, it opens in the workspace or in a separate browser window.
X Window tools	X Window tools require that an X server is running. These tools can reside on the CMS or on a managed system. When accessing HP SIM from a network client, you must have X server software running on the network client to execute an X Window tool. From the CLI or GUI, HP SIM invokes the X Window application using the command line and passes the location of the X server by requesting the device for display from the user.
Command line tools	Command line tools include applications, commands, and scripts. They can reside on the CMS or another managed system. They can be launched directly from the CLI or GUI.

Information storage

HP SIM uses an audit log and a database to track activity and store your management domain information.

HP SIM audit log

HP SIM logs all tasks performed by all HP SIM users on all systems. The information is stored in the audit log on the CMS. HP SIM logs all tasks with the following information:

- Time stamp
- User name
- Systems
- Event
- Tool result

For command tools, the verbose level of `stdout` and `stderr` is frequently large and time-sensitive, so it is only logged by default for the `ps` command. The option to log this output for the `ps` and other commands is configurable. In addition, other aspects of the audit log, such as maximum file size, is also configurable. Information about configuring the audit log is available in [Chapter 13. Configuration options](#) and in the "Administering the Software" section of the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

Database

HP SIM uses a database to store vital management domain information. The database contains information about:

- Authorizations
- Systems
- System lists
- System group definitions
- Users
- Passwords
- Toolbox definitions
- Tool definitions
- Events
- Inventory data

Database software

HP SIM supports the use of several databases:

- PostgreSQL is supported on HP-UX or Linux CMS.
- Microsoft SQL Server Desktop Engine (MSDE) or Microsoft SQL Server 2000 is supported on a Windows CMS. HP SIM ships with MSDE, but you can choose to use Microsoft SQL Server 2000, which provides more advanced enterprise features.
- Oracle 9i Release 2 is supported on all platforms.



NOTE The Oracle database must be created before installing HP SIM. The thin client jar file location must be specified. HP SIM requires Oracle database and TNS listener services to be up and running when system is restarted. Oracle by itself does not start the Oracle database and TNS listener automatically. An Oracle DBA must set these services to be restarted when the server is reset. Refer to Oracle Documentation for details on how to auto start these services.

http://download-east.oracle.com/docs/html/A96167_01/post-inst.htm#sthref548

Under the section: "Automating Database Startup and Shutdown for HP, Linux and Solaris (Optional)."
" Access to this link requires registration, which is free. The Oracle DBA who manages the Oracle installation must perform this task.

Secure access

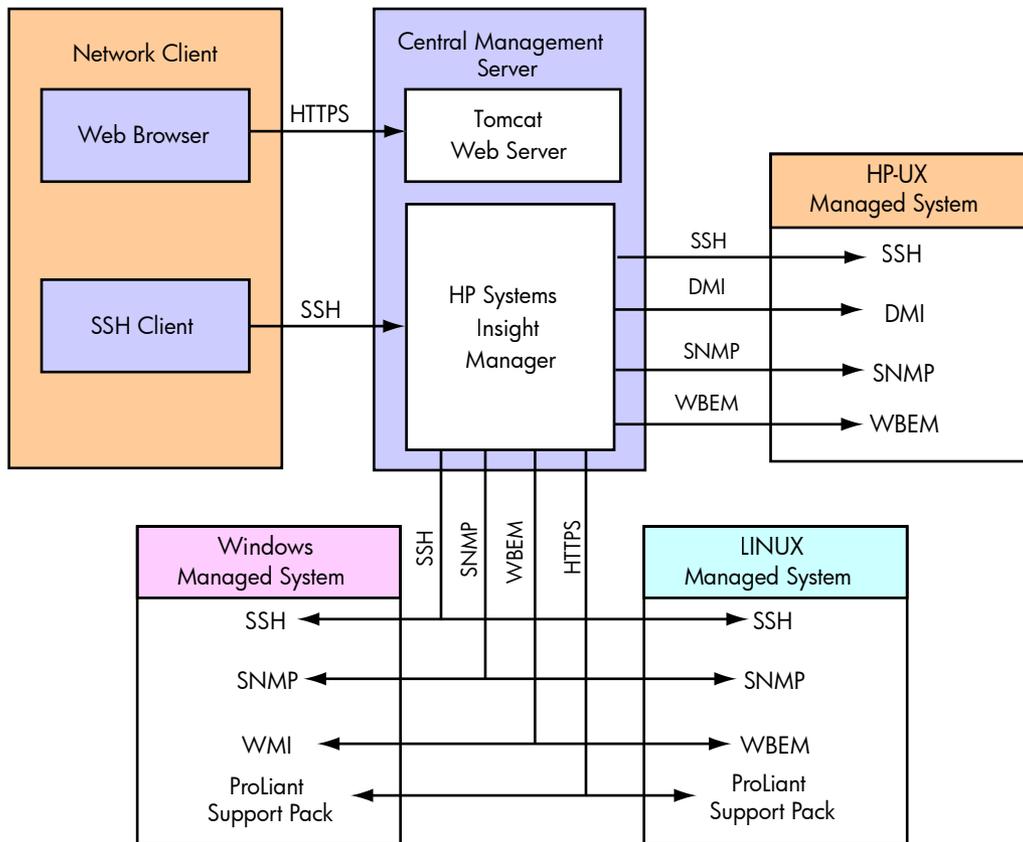
HP SIM utilizes several technologies to provide secure access. You can access HP SIM through the command line or a web browser. Both of these user interfaces can be accessed from anywhere on your network.

Command line interface

When you access HP SIM from the CLI, your operating system login is used to identify you to HP SIM. You have access to use the HP SIM commands based on your authorizations. If you access HP SIM from any system other than the CMS, be sure you use an SSH client. Programs like telnet, rlogin, and FTP do not provide encrypted access. When you use one of these applications to access HP SIM, your data, including your password, is transmitted across the network unencrypted. In addition, these protocols are not spoof-protected. If you have a Windows CMS, then only administrators have command line access to HP SIM. A remote desktop connection to the CMS can be used to access the command line.

Graphical user interface

When you access the HP SIM from a web browser, you log on using the secure HTML login page. The user name and password for the login page are the same as your CMS operating system user name and password. A Windows CMS also requires a domain name. Your information is securely transmitted using the SSL protocol. SSL provides data encryption and server authentication by using a public and private key technology. The web server on the CMS uses a certificate for server authentication. By default, this certificate is self-signed, but it can be replaced by a certificate that is signed by a trusted certificate authority. Your web browser should import this certificate to trust the CMS.



Secure data transmission

The security of the transaction depends on your networking environment and the management protocol that each tool is using.

Management protocols

The basic supported management protocols and applications are SSH, Web-Based Enterprise Management (WBEM), Secure HTTP (HTTPS), Desktop Management Interface (DMI), and SNMP. Tools are not limited to these protocols, and they can provide a custom management protocol. SSH is the only protocol that must be installed on every managed system. Tools require specific protocols, and they can only be run on a managed system if the protocol they require is installed and configured correctly.

SSH

SSH is a program that enables you to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels. SSH uses a public/private key pair to provide a secure mechanism to authenticate and encrypt communication. SSH keys are used to identify the execute-as user on the managed system. Typically, the execute-as user is either root or administrator, but other users can be configured, depending on the tool that will be executed on the managed system. The private key is kept secure on the CMS, while the public key is installed on each managed system.

The SSH-2 protocol is used by the Distributed Task Facility (DTF) to communicate with managed systems. The DTF improves operator efficiency by replicating operations across the systems or system groups within the management domain using a single command. This functionality reduces the load on administrators in multi-system environments. X Window and CLI tools use the DTF to execute and support the following:

- Executing scripts, commands, and applications remotely on managed systems
- Copying files to managed systems

The DTF connects the CMS to the SSH server software running on each managed system. The DTF tells the SSH server what tasks must be performed on the system. The SSH server then performs the tasks and returns the results to the DTF. The DTF consolidates the feedback it receives from all the managed systems.

WBEM

WBEM is an industry standard that simplifies system management. It is based on a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. It provides access to both software data and hardware data that is readable by WBEM compliant applications.

HP SIM keeps a database of passwords for managed systems running WBEM. The database contains the user names and passwords for each managed system, which are required to provide user authentication for tools using this protocol. These accounts do not need to have other access capabilities, such as log on rights. They are only used for WBEM access by HP SIM. The WBEM user name and password can be set from the CLI or GUI. For more information, refer to the "Administering the Software" section in the HP Systems Insight Manager Technical Reference Guide at

<http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

HP SIM uses HTTPS to access WBEM data, providing a secure path for system management data. For access to Windows management data instrumented in Windows Management Instrumentation (WMI), a WMI Mapper running on a Windows system converts the HTTPS WBEM requests into WMI requests, which use Distributed Component Object Model and NT security.

HTTPS

HTTPS is simply HTTP over SSL, a protocol that supports sending data securely over the Web. HTTPS is used to access WBEM data as explained in the previous section, and it is used to access ProLiant agent information. Digital certificates are used instead of user names and passwords to establish trust between the agent and the CMS. The certificate of the CMS should be loaded into each agent to be managed by that CMS.

Desktop Management Interface

DMI is an industry-standard protocol, primarily used in client management, established by the Desktop Management Taskforce. DMI provides an efficient means of reporting client system problems. DMI-compliant computers can send status information to a CMS over a network. DMI is supported for system inventory collection where the information is not available from WBEM and SNMP. A Windows CMS uses DMI to gather information from third-party servers. An HP-UX CMS uses DMI to gather system information from other HP-UX systems. DMI is not supported on a Linux CMS. DMI is not a secure protocol. Therefore, anyone with access to your network can intercept and view DMI transactions.

SNMP

SNMP is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. There are multiple versions of SNMP. SNMP Version 1, used by HP SIM, is not a secure protocol. Therefore, anyone with access to your network will be able to intercept and view SNMP transactions.

HP SIM keeps a database of read and write community names for managed systems running SNMP. The community name must match those configured on the management system. The SNMP community names and passwords can be set from the CLI or GUI. For more information, refer to the "Administering the Software" section in the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

HP SIM does not use SNMP SetRequests. By default, the supported operating system platforms have SNMP SetRequests disabled. For improved security, do not enable SNMP SetRequests on the CMS or the managed systems. Even SNMP GetRequest responses can be spoofed, so all information from SNMP should be regarded as insecure.

Web server security

HP SIM uses the Tomcat web server on the CMS. Tomcat features that are not required by HP SIM are turned off by default. These features include Server Side Includes and Common Gateway Interface scripts.

Self-signed certificates

The self-signed certificates used for WBEM and web server authentication make it possible for another system to impersonate the CMS if the valid certificate is not securely imported into the client or browser, which is known as spoofing. To prevent the possibility of spoofing, use a certificate signed by a trusted Certificate Authority (CA) or securely export the certificate by browsing locally to the CMS and then securely importing it into your browser. You can also obtain the server certificate by browsing remotely and saving it in the browser the first time you access HP SIM, but this option is less secure and still susceptible to a possible "man-in-the-middle" attack. Information about importing CA-signed certificates is available in the "Administering the Software" section of the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

X application security

The data exchanged between an X client (or application) running on a managed system and an X server on the network client is transmitted in clear text over the network. HP does not recommend X clients in environments in which security is a concern.

Managing servers behind a firewall

HP SIM supports managing servers that are located behind a firewall when using the SSH, HTTPS, and WBEM protocols. HP does not recommend the SNMP and DMI protocols because they are not secure protocols. The firewall must be configured to allow this traffic through the firewall. The following ports are used:

- WBEM uses HTTPS over port 5989
- Web Agents use HTTPS over port 2381
- DTF uses SSH-2 over port 22

For a complete list of ports used by HP SIM, refer to the *Understanding HP SIM Security* white paper. This white paper is available at <http://www.hp.com/go/hpsim/>.

2 Installation overview and requirements

This chapter provides an overview of the HP SIM installation process, and it identifies the system requirements for a CMS, a managed system, and a network client.

Process overview

1. Install and configure the CMS. The procedure to complete this step is in the installation chapters of this guide. Follow the appropriate chapter based on the operating system of your CMS. Refer to [Chapter 3. Installing on Windows](#) , [Chapter 4. Installing on HP-UX 11i](#) , or [Chapter 5. Installing on Linux](#) for details.
2. Install and configure the required Management Agents on the systems that will be managed by the CMS. This step is covered in the first section of [Chapter 12. Initial Setup](#) .
3. Configure HP SIM for your environment. The remaining sections in [Chapter 12. Initial Setup](#) cover these recommended tasks.

System requirements

This section identifies the hardware and software requirements and recommendations for HP Systems Insight Manager. These requirements are broken into sections by system type for the CMS, managed system, and network client.

CMS requirements

This section contains the requirements for the operating system that is used for the CMS. Review the section requirements that applies to your CMS. Refer to:

- ["HP-UX Central Management Server"](#)
- ["Linux Central Management Server"](#)
- ["Windows Central Management Server"](#)

HP-UX Central Management Server

- **Operating system**
 - HP-UX 11i v1
 - HP-UX 11i v2 (September 2004 or later)

Note: The required patches must be installed for each of these operating systems. Refer to ["HP-UX Patches"](#) for more information.
- **Hardware**
 - Any HP system (PA-RISC 2.0 or Integrity) server with a minimum of 2 GB RAM
 - Any HP system with Oracle installed with a minimum of 4 GB RAM
- **Software**
 - OpenSSH (distributed with the operating system)
 - HP WBEM Services for HP-UX, installed and active for HP-UX 11i or greater
 - (Optional) Oracle 9i release 2
 - Java Out-of-Box installed (shipped as optional selectable software as part of the operating system)
- **Free disk space**
 - 20 MB for CMS (/)
 - 600 MB for the CMS and DTF agent (/opt)
 - 500 MB minimum recommended for data (/var/opt)

- **Swap space**
 - 3 GB minimum total swap space for PA-RISC systems
 - 4 GB minimum total swap space for Intel® Itanium®-based systems
- **Networking**
 - Properly configured and working Domain Name System (DNS) or Windows Internet Naming Service (WINS) for host name resolution



NOTE If running OpenView NNM or OpenView Operations on the same system, the SNMP trap listening port must be changed in those products to function properly. Refer to the OpenView product documentation in the HP Systems Insight Manager and HP OpenView white paper at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

NOTE Legacy Novell systems with only an IPX network enabled will not be manageable by an HP-UX or Linux CMS. An IP-based network must be available.

NOTE If you are using Network Information Services (NIS), ping localhost of HP-UX, and if you receive no response, create or edit the file `/etc/nsswitch.conf` and add the following entry in the file: `hosts: files dns nis`. If NIS server is not in the network, do not add the `nis` entry in `/etc/nsswitch.conf`.

HP-UX Patches

There are required patches that must be installed to run HP Systems Insight Manager. All patches should be installed before running HP Systems Insight Manager.

Note: To determine the Java version installed, execute:

```
/opt/mx/j2re/bin/java -version
```

Note: For more information about patches, go to <http://www.hp.com/go/java>, and select **Patches** from the **Site information**. This site determines the recommended patches for the Java application. Follow the instructions given. To download all of the patches, go to the ITRC download center (login required). For more information on individual patches, click the patch name.

Downloading and installing HP-UX patches

To download patches:

1. Browse to the patch database:
<http://www2.itrc.hp.com/service/patch/mainPage.do>
2. Click the **HP-UX** link.
3. Select the appropriate hardware and operating system. For example, 800 and 11.11.
4. Select **Search by Patch IDs**, enter the patch IDs, and click **search**.
5. Select the patches, and click **add to selected patch list** at the bottom of the page to add dependent patches.
6. Click **download selected**, and follow the directions on the screen. HP recommends the *gzip* package format.

To install patches:

1. Create a `/var/tmp/patches` directory, and copy the downloaded patches into that directory.
2. Execute:

```
gunzip patch_file
tar -xvf patch_file
```
3. Load the patches into `/var/tmp/patches/depot`:

```
./create_depot_hp-ux_11
```
4. Install the patches:

```
swinstall -x autoreboot=true -s /var/tmp/patches/depot \ *
```

Note: Only the applicable patch file sets are loaded. Continue with the installation after you reboot.

Linux Central Management Server

- **Operating system**
 - Red Hat Enterprise Linux 3 AS and ES U4 and U5 for x86
 - Red Hat Enterprise Linux 4 AS and ES U1 for x86
 - SUSE Linux Enterprise Server 8/UnitedLinux 1.0 for x86 with Service Pack 3
 - SUSE Linux Enterprise Server 9 for x86 with Service Pack 1 or 2
- **Hardware**
 - Any HP IA-32 system with:
 - Minimum: 1.5-GHz processor and 768 MB RAM
 - Recommended: 2.4-GHz processor and 1 GB RAM
 - Any HP system with Oracle 9i installed minimum 4 GB RAM
- **Software**
 - OpenSSH
 - ProLiant Support Pack for Linux 7.00 or later
 - (Optional) Oracle 9i release 2
 - For Red Hat Enterprise Linux 3.0 AS/ES update 4 and 5:
 - PostgreSQL 7.4.1
 - For Red Hat Enterprise Linux 4:
 - PostgreSQL 7.4.7-2
 - For SUSE Linux Enterprise Server 8, Service Pack 3:
 - PostgreSQL 7.4.0
 - For SUSE Linux Enterprise Server 9:
 - PostgreSQL 7.4.2-36.3



NOTE PostgreSQL 8.0.x is not supported on HP SIM 5.0 on Japanese installations.

- **Free disk space**
 - 2 MB for CMS (/)
 - 400 MB for the CMS and DTF agent (/opt)
 - 500 MB minimum recommended for data (/var/opt)
- **Swap space**
 - 3 GB minimum total swap space for Itanium-based systems
- **Networking**
 - Static or dynamic host name resolution



NOTE On Linux, look for the entry 127.0.0.1 localhost, the local system IP address, and the system name in the /etc/hosts file. If they are not present, add the entries manually.

- SNMP (optional)

Windows Central Management Server

- **Operating system**
 - Microsoft Windows 2000 Server with Service Pack 4 for x86
 - Microsoft Windows 2000 Advanced Server with Service Pack 4 for x86

- Microsoft Windows 2003 Server with Service Pack 1 for x86
- Microsoft Windows 2003, Standard or Enterprise Edition, for x86 with Service Pack 1 (running on x86 or x64/AMD64 platforms)
- Microsoft Windows XP Professional with Service Pack 2 for x86
- Microsoft Windows Server 2003 R2

Important: The Windows server must have at least one partition formatted for the NT File System (NTFS) on which the HP SIM server software is to be installed. NTFS provides the ability to restrict file access based on user accounts and groups. Without NTFS, the CMS cannot be adequately secured against unauthorized access, and potentially sensitive operations and data could be made available to unauthorized users.

Note: The required Windows service packs must be installed for each of these operating systems.

- **Hardware**

- Any HP ProLiant x86 system with:
 - Minimum: 1.5-GHz processor with 768 MB RAM
 - Recommended: 2.4-GHz processor with 1 GB RAM

Note: HP Netserver platforms can be used for the CMS as long as the Instant Toptools software is not installed and all other requirements are met.

- **Software**

- MSDE 2000 with Service Pack 3a (bundled with HP Systems Insight Manager) or one of the following:
 - Microsoft SQL Server 2000, Standard Edition with Service Pack 3 or Service Pack 4 (for Standard Server operating system)
 - Microsoft SQL Server 2000, Enterprise Edition with Service Pack 3 or Service Pack 4 (for "Advanced Server" operating system)
 - Oracle 9i Release 2

Note: Windows XP Professional does not support a local installation of SQL Server 2000, only MSDE 2000. SQL Server 2000/Oracle 9i can be used as a remote database for a CMS on Windows XP Professional.

- ProLiant Support Pack for Windows 6.30 or later
- Microsoft Internet Explorer 6.0

- **Free disk space**

- 500 MB recommended

- **Networking**

- Static or dynamic host name resolution
- TCP/IP
- SNMP

Managed System Requirements and Recommendations

This section contains requirements and recommendations for managed systems.

- **Supported operating systems**

- HP Tru64 UNIX
- HP NSK
- HP OpenVMS
- HP-UX 11i
- HP-UX 11i v2 (September 2004 or later)
- IBM OS/2

- Microsoft Windows 2003 Standard for x86
- Microsoft Windows 2003 Standard with Service Pack 1 for x86
- Microsoft Windows 2003 Enterprise for x86
- Microsoft Windows 2003 Enterprise Service Pack 1 for IA-32
- Microsoft Windows 2003 Enterprise for Itanium-based Systems
- Microsoft Windows 2003 Enterprise with Service Pack 1 for Itanium-based Systems
- Microsoft Windows 2003 Extended Systems for x64 and AMD64
- Microsoft Windows 2003 Web Edition for x86
- Microsoft Windows 2003 Data Center
- Microsoft Windows 2003 Small-Medium Business for x86
- Microsoft Windows Professional for x86
- Microsoft Windows Data Center for x86
- Microsoft Windows 2000 Server with Service Pack 4 for x86
- Microsoft Windows 2000 Advanced Server with Service Pack 4 for x86
- Microsoft Windows 2000 Server for x86
- Microsoft Windows 2000 Advanced Server for x86
- Microsoft Windows 2000 with Service Pack 1 or later for x86
- Microsoft Windows XP with Service Pack 2
- Microsoft Windows XP with Service Pack 1
- Microsoft Windows XP
- Microsoft Windows 98
- Microsoft Windows 98 Millinium Edition
- Microsoft Windows Virtual Server
- Novell NetWare 6.5
- Novell NetWare 6.0
- Novell NetWare 5.1
- SCO Open UNIX 8
- SCO Unixware 7
- SCO OpenServer 5
- Red Hat Linux 9
- Red Hat Linux 8
- Red Hat Linux 7.3 Workstation
- Red Hat Linux 7.2
- Red Hat Enterprise Linux 4 for x86
- Red Hat Enterprise Linux 4 for AMD64 and EM64T
- Red Hat Enterprise Linux 4.0 for IA-32 and Itanium-based systems
- Red Hat Enterprise Linux 3 AS for Itanium-based systems
- Red Hat Enterprise Linux 2.1 for Itanium-based systems
- Red Hat Enterprise Linux 2.1 for x86
- Sun Solaris 9 Intel Platform
- Sun Solaris 8 Intel Platform
- SUSE Linux Enterprise Server 9 for Itanium-based systems
- SUSE Linux Enterprise Server 9 for x86

- SUSE Linux Enterprise Server 9 for AMD64 and Intel EM64T
- SUSE Linux Enterprise Server 8 for Itanium-base systems
- SUSE Linux Enterprise Server 8
- SUSE Linux Enterprise Server 8/United Linux 1.0
- SUSE Linux 7.2
- SUSE Linux 7.0
- VMware ESX
- VMware GSX

Note: Operating systems with only IPX enabled will not be identified by an HP-UX or Linux CMS.

Note: Microsoft Windows 2002 and 2003 International Server - French, German, Spanish, and Japanese (latest service pack available for each language).

- **Hardware**

- For HP-UX:
 - Any HP PA-RISC system
 - Any HP Itanium-based system
- For Linux:
 - Any HP x86 system
 - Any HP Itanium-based system
- For Windows:
 - Any HP x86 system

- **Software**

Note: This software is not required, but if you want improved management capabilities, HP recommends that you install these components.

- For HP-UX:
 - SSH
 - WBEM
- For Linux:
 - SSH
 - ProLiant Support Pack for Linux 7.0 or later
 - SNMP (recommended as an alternative to WBEM)
 - WBEM (for Integrity systems only)
- For Windows:
 - OpenSSH 3.7.1
 - ProLiant Support Pack 6.30 or later
 - WBEM/WMI
 - SNMP (recommended as an alternative to WBEM)

Note: This software is not required, but if you want improved HP SIM capabilities, HP recommends that you install these components, which can be purchased or downloaded from many software suppliers.

- SSH Client
- X Window Server

- **Networking**

- Static or dynamic host name resolution
- SNMP

- **Required web browsers**

- For HP-UX:
 - Mozilla 1.7.3 or later
To download, refer to <http://software.hp.com>.
- For Linux:
 - Mozilla 1.7.3 or later
- For Windows:
 - Microsoft Internet Explorer 6 with Service Pack 1 or later

Note: For all Internet Explorer browsers, you must have the SSL 3.0 or TLS 1.0 browser security options enabled for HP SIM to work properly.

- **Managed storage system**

To view the latest information regarding HP SIM support for a particular storage system including Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters). Refer to the HP SIM SMI-S Provider web page at:

<http://www.hp.com/go/hpsim/providers>.

This webpage also offers information on obtaining and installing SMI-S providers.

SSH Requirements

SSH is locally configured during HP SIM installation locally on the CMS. Additional steps to complete the configuration on the CMS can be provided in the HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibary.html>. **Custom commands** on the **Tools** menu require SSH on the CMS to run properly. These commands run on the CMS with environment variables set to the context of specific events or devices. SSH on the CMS is also used by the **Initial ProLiant Support Pack Install** on the **Deploy**→**Deploy Drivers, Firmware and Agents** menu.

You can optionally install and configure SSH on each of the managed systems and have HP SIM exchange keys with the managed systems (through the `mxagentconfig` command or for Windows, through the Install SSH task). If you do this, then the **Command Line Tools** option on the **Tools** menu works for these managed systems. If you choose not to configure it to work with remote SSH clients, then these commands fail. There is no other loss of functionality without SSH.

3 Installing on Windows

Preparing the system

This procedure verifies that your system meets the minimum requirements and prepares your system for installation.



NOTE The Windows installer will fail if Internet Explorer 6.0 or later is not present. If Internet Explorer 5.x or earlier is installed, it must be upgraded to Internet Explorer 6.0 or later for the HP SIM installation to complete successfully.

NOTE If installing HP SIM with a local MSDE or SQL database on a Windows XP SP2 machine that is not a member of a domain, **Simple File Sharing** is automatically disabled. The Simple File Sharing setting on Windows XP Professional changes the way local users are authenticated.

Enabled = Guest only. Local users authenticate as Guest.

Disabled = Classic. Local users authenticate as themselves.

This setting is located in the Local Security Policy Editor under Start>Control Panel>Administrative Tools>Local Security Policy. Select Security Settings>Local Policies>Security Options>Network access: Sharing and security model for local accounts. This change is necessary for the database install.

To verify and prepare your system:

1. Verify your system meets the minimum requirements. Refer to "System requirements" for details.
2. Install the required Windows and Microsoft SQL Server 2000 Server or MSDE Service Packs.

Note: The Typical install for HP SIM does not support an Oracle database.

3. Verify your system has at least one partition formatted for the NTFS file system, on which the HP SIM server software is to be installed.

If this requirement is not yet met, create or format an NTFS partition for use by HP SIM.

4. Verify that Microsoft Access Data Components (MDAC) 2.7 Service Pack 1 or higher is installed. Navigate to C: \Program Files\Common Files\System\Ado, and right-click the icon for the msado15.dll file. Select **Properties**, and click the **Version** tab to display the version number. If the file is not found in this path, use the Windows search engine to find the file. If you must download MDAC, refer to <http://www.microsoft.com/downloads/>, and search for MDAC Service Pack.
5. Download the software, or install it from the HP Management CD.

To download the software, refer to <http://www.hp.com/go/hpsim>, and on the upper-left of the page under HP management software, click **Download**. The HP SIM **Download** Page appears. Under **HP Systems Insight Manager and related components**, select **HP SIM-Windows>Download latest version of HP SIM - Windows** for a full product install.

To install the software from the Management CD, place the CD in the CD-ROM drive. The CD has an autorun feature that launches a license agreement. Agree to the license agreement, and click the **Products** tab. Click **Install** under HP SIM to launch the Installer. Or click the **Products** tab, click **Explore CD**, and then run setup.exe located at \hpsim\win_ia32\ to launch the Installer.

6. Before you proceed with install if you are going to install HP ProLiant Essentials Performance Management Pack, HP ProLiant Essentials Virtual Machine Management Pack, or the System Management Homepage you need to refer to the following documents for specific username requirements for the product administrator, service account and database administrator. For more information refer to
 - HP ProLiant Essentials Performance Management Pack documentation at <http://www.hp.com/products/pmp>
 - HP ProLiant Essentials Virtual Machine Management Pack User Guide at <http://www.hp.com/servers/proliantessentials/vmm>
 - System Management Homepage Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>

HP SIM can be installed in two ways:

- Typical install - Requires minimal user interaction. Refer to [Typical install](#) for more information.
- Custom install - Enables you to select the components you want to install. Refer to [Custom install](#) for more information.

The **HP Systems Insight Manager Setup** window appears. The **Setup** window displays links to the following documentation:

- ReadMe (Adobe format)
- Release Notes (Adobe format)
- Installation and User Guide (Adobe format)

7. Click **Install** to start the install process.

Note: The installing account and the HP SIM service account, both included in the local admins group, will be the initial login account.

The **HP Systems Insight Manager Setup** Installation status window appears with the following three stages:

- Pre-Installation

Examines this system for local instances of MSDE, SQL Server 2000 and Oracle9i and will display the **Optional MSDE 2000 SP3a installation** window if none are found.

Note: If the server reboots, the setup shell restarts automatically. If setup was initiated from a mapped drive and the mapped drive is not available on reboot, then the setup shell fails to launch.

- Installation

Launches the Install Shell and installs HP SIM and other HP management software products.

- Post-Installation

Completes the import of PMP data when doing an upgrade.

Note: This window is immediately covered by the **HP Systems Insight Manager SetUp Check** window. However, the **HP Systems Insight Manager Setup** Installation status window remains open, and when each stage of the setup is complete, it states, "Done." When a stage is in progress, it states "In Progress." If this is a clean installation, the status for the Post-Installation will state, "Not Run." After HP SIM and all components have been installed, click **Finish** to close the **HP Systems Insight Manager Setup** Installation status window and return to the desktop.

8. From the **HP Systems Insight Manager SetUp Check** window, click **Install MSDE** to start the install process.

If supported versions of MSDE, Microsoft SQL Server, or Oracle are not detected locally, you are prompted to install MSDE 2000 Service Pack 3A or point to a remote SQL Server installation later.

Note: For a list of supported databases, refer to *HP Systems Insight Manager Release Notes at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>* for details.

After MSDE installation is complete, the installer reboots your system, if required. If the server reboots, the Setup Shell restarts automatically and then repeats the previous step to launch the installer. You will not see the option to install MSDE again.

9. The **HP Systems Insight Manager Installer** window appears. Click **Install** to begin. The **Select Installation Type** window appears.

Refer to [Typical install](#) or [Custom install](#) for more information.

Typical install

1. Click **Typical** to install the included components with minimal user interaction listed under the **Available Components for Install**. The **Typical Install - Service Account Credentials** window appears. The Domain and Username fields default to the installing account credentials and these fields cannot be edited.

Available components for install	Typical installation	Custom installation
System Management Homepage	Included	Included
OpenSSH for Windows 3.7.1p1-1	Included	Optional
WMI Mapper	Included	Optional
HP Systems Insight Manager	Included	Included
HP ProLiant Essentials Performance Management Pack	Included	Optional
HP Version Control Repository Manager	Included	Optional
HP ProLiant Essentials Virtualization Management Software	Included	Optional
HP Systems Insight Manager Installation Information	Included	Optional

Note: If a component is not listed as being available for installation on the CMS, then the HP SIM install shell has determined one of the following:

- The installation prerequisites for the component have not been met.
- The component is currently installed.

If the component that is present on the CMS is an older version than what is bundled with the HP SIM install shell and it supports an in-place upgrade, it appears in the component list.

2. Enter the Password for this account. Click **Next**.

Note: The HP SIM Service account will be the installing account. This user account will be used to run the HP SIM service.

3. The **Typical Install - Database Configuration** window appears. Enter the **Account Credentials** for the database server. The installing user account is pre-populated in the Username field, and cannot be edited. The Host field prepopulated with the local host name, can be edited. If using a local SQL Server or MSDE, provide the password for the installing user, and click **Next** to proceed. Typical install requires the installing user account to exist on the remote database server. If your database is not local, supply the database server name and password. Click **Next**. The **Typical Install-Software Selection** window appears. This window displays the complete list of the available components with a checkbox next to each one. If the checkbox is selected, the component is deemed a mandatory component and cannot be deselected. All the components that are under the Typical Install column of the **Select Installation Type** window should have disabled checkboxes. The amount of required disk space is also listed for each component.

Note: HP SIM does not support the following in a user name and password:

- A blank password
- A space followed by a double-quote
- A backslash (\)

If you use these characters in your user name or password, the HP SIM database initialization fails.

Note: In case of a reboot, if you just installed MSDE, the administrative credentials are those you used to log in before installing MSDE. Windows authentication is required to connect to the SQL server (whether locally or remotely). In addition, these credentials will also be your HP SIM administrative user login credentials. Any account that is a member of the administrator group will have administrator rights to MSDE. The local security policy will be modified to give you the following rights: log on as a service, create a token object, and replace a process level token. In addition, for Windows XP SP2, Windows 2003 SP1 or later, Component Object Model (COM) security will be updated to allow remote access and activation by everyone and anonymous users. See the HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more details.

4. Click **Next** to check if enough disk space exists for the selected components, and if enough exists, the **Typical Install – Summary** window appears.
5. Select **Install** to initiate the installation process. This process installs all the products listed in the **Selected Components** table. The **Typical Install - Status** window appears. As each component is being installed, it states "In Progress" beside the component's name. After the component has installed, it states "Installed Successfully." When all of the HP SIM components have been installed, the **HP Systems**

- Insight Manager Installation Information** window appears. This window has links for the Version Control Installation Guide, to help you configure Version Control and the System Management Homepage.
- Click a link to view the Version Control Installation guide, or click **OK** and the **Typical Install - Status** window appears again. After all components have been installed, they have an installed status. The HP SIM Installation Information status states, "Success." Click **Finished**. Typical Installation is complete. Refer to "Next steps" for more information.

Note: For more information regarding where the System Management Homepage default settings are stored during a Typical installation and how to change them, refer to the System Management Homepage Installation Guide at

<http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Custom install

- Click **Custom** to select the individual components under the **Available Components for Install** and configure them during installation.

Available components for install	Typical installation	Custom installation
System Management Homepage	Included	Included
OpenSSH for Windows 3.7.1p1-1	Included	Optional
WMI Mapper	Included	Optional
HP Systems Insight Manager	Included	Included
HP ProLiant Essentials Performance Management Pack	Included	Optional
HP Version Control Repository Manager	Included	Optional
HP ProLiant Essentials Virtualization Management Software	Included	Optional
HP Systems Insight Manager Installation Information	Included	Optional

Note: If a component is not listed as being available for installation on the CMS, then the HP SIM install shell has determined one of the following:

- The installation prerequisites for the component have not been met.
- The component is currently installed.

If the component that is present on the CMS is an older version than what is bundled with the HP SIM install shell and it supports an in-place upgrade, it appears in the component list.

- The **Custom Install-Software Selection** window appears. This window displays the complete list of the available components with a checkbox next to each one. If the checkbox is selected and disabled, the component is deemed a mandatory component and cannot be cleared. The amount of required disk space is also listed for each component.
- Click **Next** to verify if enough disk space exists for the selected components. If enough space exists, the **Custom Install – Summary** window appears.
- Select **Install** to initiate the installation process. This process installs all the products listed in the **Selected Components** table. The **Custom Install - Status** window appears. As you install each component, it states "In Progress" beside the component's name. After the component has installed, it states "Installed Successfully."
- install System Management Homepage:

If the System Management Homepage is not installed, the **System Management Homepage Setup** window appears. This InstallShield Wizard guides you through the install of System Management Homepage. Click **Next**. The **Operating Systems Groups** window appears.

Note: If at any time during the install of System Management Homepage you click **Cancel**, the installation and setup of the System Management Homepage ends.

- a. Select **Administrator**, **Operator**, or **User** from the **Operating Systems Group Name** field.
- b. Enter the group name of an operating systems group in the **Group Name** field. Click **Add**. The group name is added. A maximum of five entries can be added for each group level. Click **Next** to continue.

Note: To delete a group name, select the group name, and click **Delete**.

- c. From the **User Access** window, configure the System Management Homepage for the following access types:

- Select **Anonymous Access** to enable anonymous access to unsecured pages.
- Select **Local Access Anonymous** or **Local Access Administrator** to set up the System Management Homepage to automatically grant local IP addresses at the selected access level.

Caution: Selecting **Local Access** with Administrator privileges provides any users with access to the local console full access without prompting them for a user name or password.

- d. Click **Next**. The **Trust Mode** window appears.

- e. Select the level of security you want to provide from one of the three trust modes:

- Trust By Certificate
 - i. Select **Trust By Certificate**, and click **Next**. The **Trusted Certificates** window appears. The **Trusted Certificates** window allows trusted certificate files to be added to the **Trusted Certificate List**.
 - ii. Click **Add File** to browse and select any certificates to be included in the **Trusted Certificate List**. The **Select File** window appears. If an invalid file name is entered in the file name field, an error message appears, indicating the file does not exist. Click **OK** to select another file, or click **Open** to add the file to the **Trusted Certificate List**. The **Trusted Certificate List** appears. Click **Next**.

Note: If you click **Next** without adding any certificates to the list, and no certificates exist from a previous installation, a message appears, indicating that if you do not specify any trusted certificates, HP SIM cannot access the HP Insight Management Agent on this system. Click **OK** if you do not want HP SIM to access the Insight Management Agent on this system, or click **Cancel** to close the window and add the trusted certificates to the list.

Note: The **Trust By Certificates** option enables the System Management Homepage system and the HP SIM system to establish a trust relationship by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before enabling access.

or

- i. Click **Import**. The **Import Server Certificate** window appears.
- ii. Enter the name or IP address of the server whose certificate you want to import.
- iii. Click **Get Cert**. The certificate information appears.
- iv. Verify the certificate information. If you want to add this certificate to the **Trusted Certificate List**, click **Accept** and the certificate is added to the **Trusted Certificate List**, or click **Cancel** if you do not want to add it to the **Trusted Certificate List**. The **Trusted Certificate List** appears. Click **Next**.

Note: You can add an unlimited number of trusted certificates.

Note: To delete a certificate, select the certificate, and click **Delete**. The selected certificate is removed.

- v. From the **IP Binding** window, select the IP Binding checkbox if you would like to bind to IP addresses that match a specific subnet and mask. Click **Next**.
 - vi. From the **IP Restricted Logins** window, select the Enable IP Restricted Logins checkbox if you would like to include or exclude specific IP addresses or IP address ranges. Click **Next**, and the **Summary Panel** appears.
- Trust By Name
 - i. Select **Trust By Name**. Click **Next**.
 - ii. The **Trusted Server** window appears. Enter the names of the servers you want to trust.

Note: Although the **Trust By Name** mode is a slightly stronger method of security than the **Trust All** mode, it still leaves your system vulnerable to security attacks. The **Trust By Name** mode sets up the System Management Homepage to only accept certain requests from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure and can prevent non-malicious access. For example, you might want to use the **Trust By Name** option if you have a secure network, but your network has two groups of administrators in two separate divisions. The **Trust By Name** option would prevent one group from installing software to the wrong system. This option does not verify anything other than the HP SIM server name submitted.

Note: The server name cannot contain the following characters:
 ~ ! ` @ # \$ % ^ & * () + = " : ' < > ? , | ;
 - iii. Click **Add** to add the name of a server you want to trust. Click **Next**.

Note: If you click **Next** without adding any server names to the list, an error message appears, indicating that if you do not specify any trusted server names, HP SIM cannot access the Insight Management Agent on this system. Click **OK** to proceed without trusting any systems, or click **Cancel** to close the window and add server names to the list.

Note: To delete a certificate, select the certificate and click **Delete**. The selected certificate is removed.
 - iv. From the **IP Binding** window, select the IP Binding checkbox if you would like to bind to IP addresses that match a specific subnet and mask. Click **Next**.
 - v. The **IP Restricted Logins** window appears. Select the Enable IP Restricted Logins checkbox if you would like to include or exclude specific IP addresses or IP address ranges. Click **Next**, and the **Summary Panel** appears.
 - Trust All
 - i. Select **Trust All**. Click **Next**.
 - ii. The **IP Binding** window appears. Select the IP Binding checkbox if you would like to bind to IP addresses that match a specific subnet and mask. Click **Next**.

Note: The **Trust All** option leaves your system vulnerable to security attacks and sets up the System Management Homepage to accept certain requests from any server. For example, you might want to use **Trust All** if you have a secure network, and everyone in the network is trusted.

Note: You can add up to five subnet IP address/netmask pairs.

Note: If you click IP Binding but do not specify the IP address/netmask then you might not be able to connect to the System Management Homepage.

The **IP Restricted Logins** window appears. The **IP Restricted Logins** window enables you to select specific IP addresses or IP address ranges to include or exclude from gaining login access. Although optional, the System Management Homepage can restrict login access based on the IP addresses of the machine attempting to gain access.
 - iii. Select **Enable IP Restricted Logins**, and click **Next**. The **IP Addresses to Include** window appears. This window enables you to specify the IP address or IP address ranges to grant login access permission. If there are IP addresses in the **Inclusion** list, then only those IP addresses are enabled for login privileges. If there are no IP addresses in the

Inclusion list, then login privileges are permitted to all IP addresses that are not in the **Exclusion** list.

Note: A single address and ranges of addresses can be accepted in the **IP Restricted Logins** window. Enter the single address in the first box.

- iv. In the **Include** field, enter a beginning IP address to which you want to grant login access. In the **To** field, enter an ending IP address to which you want to grant login access. All IP addresses that fall between the beginning and ending IP addresses are granted login access. Click **Add**. The IP address or IP address range is added to the **Exclusion** list. Select an IP address or IP address range, and click **Delete** to remove it from the **Exclusion** list. Click **Next**.

Note: If you entered an invalid IP address or IP address range, an error message appears indicating the IP address is invalid. Click **OK**. Enter a valid IP address or IP address range, and click **Add** again. The **IP Addresses to Exclude** window appears.

In the **Exclude** field, enter a beginning IP address to which you want to deny login access.

- v. In the **To** field, enter an ending IP address to which you want to deny login access. All IP addresses that fall between the beginning and ending IP addresses are denied login access.
- vi. Click **Add**. The IP address or IP address range is added to the **Inclusion** list. Select an IP address or IP address range, and click **Delete** to remove it from the **Inclusion** list. Click **Next**.

Note: If you entered an invalid IP address or IP address range, an error message appears, indicating the IP address is invalid. Click **OK**. Enter a valid IP address or IP address range, and click **Add** again.

Note: If **Next** is selected without adding any IP addresses to either the **Include** or **Exclude** lists, a warning message appears stating, **IP Restricted Login checkbox will be marked as disabled. Do you want to proceed without adding any IP Address restrictions?** If you select **OK**, the **IP Restricted Login** option on the **IP Restricted Login** window is cleared.

The **Summary Panel** appears. The **Summary Panel** lists the location where the System Management Homepage is installed, the amount of space the installation requires, and the summary of the options that you specified during the installation.

- f. Click **Next**. The installation process is started. Click **Finish** to exit the wizard.

Note: If HP SIM is installed after System Management Homepage is installed, the System Management Homepage 2048-bit key pair will be replaced with the HP Systems Insight Manager 1024-bit key pair.

6. Install OpenSSH:

On the **Welcome to the OpenSSH Services for HP Systems Insight Manager Setup Wizard**, click **Next**.

- a. The **Select Destination Location** window appears. Setup will install OpenSSH into the following folder `C:\Program Files\OpenSSH`. To change the location, use the **Browse** button. Click **Next**.
- b. The **OpenSSH Service Log On As User** window appears. Enter your account password. The user name and domain fields are prepopulated. Although these fields are prepopulated, you may change these values to specify any user you choose. However, the account credentials you do choose must have local administrator rights (be a member of the local "Administrators" group). Click **Next**.

Note: The **OpenSSH Service Log On As User** window appears only if installing on a Windows XP or Windows 2003 system. If you are installing on a Windows 2000 system, the OpenSSH Service runs as "localsystem" and does not ask for credentials.

- c. The **Ready to Install** window appears. Click **Install** to continue with the installation.

- d. After installing OpenSSH, if prompted, click **No, I will restart the computer later**.
- e. Click **Finish**.

Note: The local security policy will be modified to give you the following rights: log on as a service, create a token object, and replace a process level token. Refer to HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more details.

7. Install WMI Mapper:

On the **Welcome to the Pegasus WMI Mapper v2.1 Setup Wizard**, click **Next**.

- a. The **End-User License Agreement** window appears. After reading the license agreement, click **I accept the terms in the License Agreement**. Click **Next**.
- b. The **Choose Setup Type** window appears. Select the setup type. (The basic requirement for HP SIM is Typical installation. If you select Typical, omit step d.)
- c. Select the default location C:\Program Files\The Open Group\WMI Mapper or change the destination location using **Browse**. Click **OK**. Click **Next**.
- d. The **Ready to Install** window appears. Click **Install** to continue with the installation.
- e. Click **Finish**.

Note: For Windows XP SP2 or Windows 2003 SP1 or later, COM security will be updated to allow remote access and activation by everyone and anonymous users. Refer to HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more details.

8. Install HP Systems Insight Manager:

When the **Welcome to the HP Systems Insight Manager Setup Wizard** appears, click **Next**. The **Service Account Credentials** window appears, with User name, Password, and Domain fields. The fields are pre-populated with the installing account credentials but can be edited if needed.

- a. Provide a valid password and proceed or provide different account details. This account should have administrative privileges. Click **Next**. The **Database Configuration** window appears.

Note: This user account will be used to run the HP SIM service.

- b. Specify **Oracle** or **SQL Server** as your Database Server. Enter the requested information appropriately. Defaults are provided where possible.

Note: HP SIM does not support the following in a user name and password:

- A blank password
- A space followed by a double quote
- A backslash (\)

If you use these characters in your user name or password, the HP SIM database initialization fails.

Note: Microsoft SQL Server Desktop Engine (MSDE) is selected by default.

For SQL Server 2000:

If your database is local, then the **Username, domain, port (default is 1433), and Database Server name** fields are prepopulated and can be changed if necessary. Provide the valid password, and click **Next** to proceed. If your database is not local, supply the name of the remote **database server** and valid values for the **domain, port, and user credentials**, if different from what is already populated. HP SIM creates a database name with the format "Insight_V50_0_XXXXXXXX (timestamp)." For example, "Insight_V50_0_172541227." It then updates the database.props file, which can be found in C:\Program Files\HP\System Insight Manager\Config. Click **Next**.

For Oracle:

The Oracle database with Unicode (AL32UTF8) as the character set must be created before installing HP Systems Insight Manager. An Oracle user with Database Administrator (DBA) privileges must be created in this database for the exclusive use by HP Systems Insight Manager. HP SIM must be

installed in an empty Oracle database schema. The thin client .jar file (ojdbc14.jar) must be copied on to the system, and its location must be specified during installation. Provide valid values for:

- User name: This Oracle user name must be assigned DBA role.



NOTE An Oracle user name cannot contain a backslash (/) or a forward slash (\).

- Password:
 - Host: This must be the name of the remote or local server where Oracle is installed. An IP address may also be used.
 - Database: This is the name of the database created on Oracle for the use of HP SIM.
 - Port: The default is 1521.
 - JarFile: This is the full path that points to the ojdbc14.jar file which needs to be copied locally.
- c. The **Select Destination** window appears. Select or enter a different folder name using Browse. Click **OK>Next**.
- d. The **Select Start Menu Folder** appears. Select or enter a different folder name using Browse. Click **OK>Next**.
- e. The **Ready to Install** window appears. Click **Install**. The **Install Progress** window appears.
- f. Click **Finish** when the installation is complete to close the **HP Systems Insight Manager Installer** window.
9. Install HP ProLiant Essentials Performance Management Pack:
- Note:** PMP does not support a remote MSDE database. For PMP to connect to a local or remote Oracle database, install the Oracle client application on the server on which PMP is installed.
- a. Optional unless you plan to use an Oracle database. Install Oracle client. If not, proceed to [step b](#).
- i. Insert the Oracle 9i Release 2 CD in the CD-ROM drive of the server where PMP is installed.
- ii. At the autorun, click **Install/Deinstall Products** .
- iii. At the Welcome screen, click **Next**.
- iv. Enter the source and destination path for support files, and click **Next**.
- v. Select **Oracle 9 Client 9.2.0.1.0**, and click **Next**.
- vi. Select Custom, and click **Next**.
- vii. In the Available Product Components, select:
- Oracle Network Utilities 9.2.0.1.0
 - Oracle Database Utilities 9.2.0.1.0
 - SQL *Plus 9.2.0.1.0
 - Oracle Windows Interfaces 9.2.0.1.0
 - Oracle Call Interfaces 9.2.0.1.0
- Click **Next**.
- viii. Specify the destination location of the Java Runtime Environment 1.1.8.16.0 or select the default location, and click **Next**.
- ix. Specify the port number or select the default port, and click **Next**.
- x. Verify the installation summary, and click **Install**.
- xi. When prompted, insert the Oracle 9i Release 2 CD 2 in the CD-ROM drive, and click **OK**.
- xii. When prompted, insert the Oracle 9i Release 2 CD 3 in the CD-ROM drive, and click **OK**.
- xiii. At the Oracle Net Configuration Assistant screen, click **Cancel**.
- xiv. When prompted to cancel the Oracle Net Configuration Assistant, click **Yes**.
- xv. Click **OK** when the error message appears.
- xvi. At the Configuration Tools window, click **Next**.
- xvii. At the End of Installation screen, click **Exit**.
- xviii. Click **Yes** to confirm.

Note: During the installation of the HP ProLiant Essentials Performance Management Pack, the following warning appears: "Warning: As part of PMP installation the HP SIM service must be stopped and restarted. Click **OK** to stop the service and continue PMP installation or click **Cancel** to abort the installation."

The Welcome to the HP ProLiant Essentials Performance Management Pack Setup Wizard appears. Click **Next**. The **Service Account Credentials** window appears.

a. Enter your account password. Click **Next**.

Note: If you are using an Oracle database, the **Database Configuration** screen appears. Enter your valid user name, password and database name, and click **Next**.

b. The **HP ProLiant Essentials Performance Management Pack Installing** window appears and installation begins. Click **Finish** to exit the HP ProLiant Essentials Performance Management Pack setup.

10. Install HP Version Control Repository Manager:

When the **HP Version Control Repository Manager Setup** window appears, click **Install**.

a. The **HP Version Control Repository Manager Setup Repository Directory** window appears. Select the directory from which HP Version Control Repository Manager will retrieve support pack information using the **Browse** button. This directory must be manually created later if it does not exist. Click **OK**. Click **Next**.

b. The **HP Version Control Repository Manager Automatic Update** window appears. Select the **Enable Automatic Update** checkbox to enable automatic downloading of ProLiant Support Packs and components at a specified interval and time.

c. Click **Finish**. Installation of HP Version Control Repository Manager proceeds and completes.

Note: If the HP Version Control Agent is configured to use the HP Version Control Repository Manager, warning appears: "At least one HP Version Control Agent must be configured to use the HP Version Control Repository Manager." If none are configured, verify the HP Version Control Agent settings to ensure proper operation of the automatic update feature. Click **OK**.

d. Click **Close**.

11. Install HP ProLiant Essentials Virtualization Management Software (VS):

Note: During the installation of the HP ProLiant Essentials Virtualization Management Software, the following warning appears: "The Virtualization Management Software installation requires HP SIM and database services to be running. During Installation, the HP SIM service will be restarted." Click **OK** to start the HP SIM status check.

a. On the **Welcome to the HP ProLiant Essentials Virtualization Management Software Setup Wizard**, click **Next** to continue with the installation.

b. The **Available Components** window appears with the following components to be installed:

- Virtual Machine Management Pack 2.0.1
- Server Migration Pack 2.0.1

Click **Next** to continue.

c. The **Service Account Credentials** window appears. Enter your account password.

d. Click **Next**. Installation begins.

e. The **VMware VirtualCenter Settings** appears.

Select one of the following:

- Configure VMware VirtualCenter Setting Later
- Configure VMware VirtualCenter Setting now

If you select to configure VMware VirtualCenter Setting now, enter your password.

Click **Next**.

Note: If you decide to configure at a later time, select **Options>Virtualization Management>Security>VMWare VirtualCenter Settings** from the HP SIM menu.

The **Completing the HP Virtualization Management Software Setup Wizard** window appears. Click **Finish** to exit setup.

Note: For Oracle, if you are installing the VS and want to connect to a local or remote Oracle database, enter your password and .jar file location on the Database Configuration screen. The HP ProLiant Essentials Virtualization Management Software must be installed in an empty Oracle database schema. VS database installation may be omitted if the VS database already exists in the specified schema. Click **Yes** to bypass VS database installation and use the current database. Click **No** to specify a different database name.

12. Install HP Systems Insight Manager information:

When all of the HP SIM components have been installed, the **HP Systems Insight Manager Installation Information** window appears. This window has links for the Version Control Installation Guide to help you configure Version Control and the System Management Homepage. Click a link to view the Version Control Installation guide or click **OK**, and the **Custom Install - Status** window appears again. After all components have been installed, they will have an installed status. The HP SIM Installation Information status states, "Success."

13. Click **Finished** to complete the component installation that you selected.

14. The **HP Systems Insight Manager Setup** window appears. Click **Finish** in the Initial Setup HP SIM window to complete the installation.

15. If any of the components indicated that a reboot is necessary, reboot your system.



NOTE When installing HP SIM, CMS host name that exceeds 15 characters are truncated, and the truncated name must be used to complete the installation. After the install, two administrator accounts are created. One account includes the original hostname\administrator and the other account includes the truncated hostname\administrator. To sign in, use the original host name in the Domain field on the Sign in page.

Next steps

Refer to [Chapter 12. Initial Setup](#) for details about Installing and configuring the required Management Agents on the systems that will be managed by the central management server (CMS). Next, complete the initial setup of HP Systems Insight Manager. Initial setup involves adding managed systems, adding users, setting up authorizations, and configuring event handling.

HP SIM is now installed and initialized on the CMS. To browse to HP SIM, use the icon that is placed on your desktop after installation is complete, or start the HP SIM GUI using Internet Explorer or Mozilla at <http://localhost:280/>.

Refer to [Chapter 10. Using the Graphical User Interface](#) for details.



NOTE The HP Systems Insight Manager First Time Wizard appears the first time when a user with full configuration rights logs in to HP Systems Insight Manager. The First Time Wizard configures only the basic settings of an initial setup for HP Systems Insight Manager. There are other options available. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

4 Installing on HP-UX 11i

Preparing the System



NOTE The "\" at the end of each command line represents that the rest of the command is on the next line.

NOTE These steps are for a clean installation of HP SIM on your HP-UX 11i system. If a previous version HP SIM or HP Servicecontrol Manager is installed on your system and you want to upgrade your data, refer to Chapter 8. Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0 or Chapter 7. Upgrading from HP Servicecontrol Manager to HP Systems Insight Manager for more information on upgrade.

This procedure verifies that your system meets the minimum requirements and prepares your system for installation. Refer to "System requirements" for details.

1. Install the latest recommended HP-UX 11i patches.

For a list of the recommended patches, refer to

<http://www.hp.com/products1/unix/java/patches/index.html> for details.

2. Verify that a previous version of HP Servicecontrol Manager or HP SIM is not installed and configured for use, using the following commands:

```
swlist -l bundle B8337BA B8339BA B8338BA T2414BA
```

```
swlist -l product ServControlMgr AgentConfig SysMgmtServer SysMgmtAgent
```

If any of these are installed and have been configured for use, use the upgrade steps described in Chapters 7 and 8 to save your data. If the version of the SysMgmtServer product starts with B.04 or C.04 use the steps in Chapter 8, "Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0 ." If the version of the SysMgmtServer product starts with B.03, use the steps in Chapter 7 "Upgrading from HP Servicecontrol Manager to HP Systems Insight Manager".

Or you can uninstall HP Servicecontrol Manager or HP SIM using the following command:

```
swremove ID
```

where ID is the product or bundle ID. For example:

```
swremove -x enforce_dependencies=false B8339BA
```

or

```
swremove -x enforce_dependencies=false T2414BA
```

Remove the old product subdirectories by executing the following command:

```
rm -fr /opt/mx /etc/opt/mx
```

Perform a clean install. Refer to "Installing and Configuring the Software" located in this chapter for more information.

3. Download the software, or locate a copy of the software on a depot server.

To download the software, refer to <http://www.hp.com/go/hpsim>, and on the upper-left of the page under **HP management software**, select **Download**. The HP Systems Insight Manager's **Download** Page appears. Under **HP Systems Insight Manager and related components**, select **HP SIM-HP-UX**, and **Download latest version of HP SIM-HP-UX** for a full product install.

4. When installing HP SIM, Java Out-of-Box (JAVAOOB) is required and is automatically selected for installation. For additional information, refer to <http://www.hp.com/products1/unix/java/java2/outofbox/index.html>. The kernel parameter values it adjusts are listed in the following table.

Java Out-of-Box settings	Kernel parameter values
max_thread_proc	3000
maxdsiz	2063835136

maxfiles	2048
maxfiles_lim	2048
maxusers	512
nfile	4097
nkthread	6000
nproc	2048
tcp_conn_request_max	2048

Additionally, HP SIM adjusts the following kernel parameters.

Java Out-of-Box settings	Kernel parameter values
nfile	30000
semms	2048
semmsi	1024

Installing and Configuring the Software

When you install HP Systems Insight Manager, the following software dependencies are required: hpSysMgmtDB, JAVA_OOB, AND SSH, (HP-UX Secure Shell). If you would like HP SIM to manage your central management server (CMS) you must install WBEM, if it is not already installed. If you downloaded your software from the Web, these dependency packages are included in the depot file. The installation procedure is described using this depot.

To install HP Systems Insight Manager:

1. Install HP Systems Insight Manager:

```
swinstall -s /directory/depot -x autoreboot=true HPSIM-HP-UX
```

where directory is the path to the depot file and depot is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot -x autoreboot=true HPSIM-HP-UX
```



NOTE All required dependencies are selected automatically for installation.

2. (Optional, required only if you plan to use an Oracle database). Configure HP SIM to use a newly created Oracle database using the following command:

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

The command executes and asks for user information for the the following host/port/Database/Username/Password/Jar file path with the file name.

```
mxoracleconfig
```

Or

```
Mxoracleconfig -h hostname -n port number -d database name -u user name -p password -j driver jar file location] [-f ]
```

-h Hostname

Full DNS name or IP address of the Oracle server.

-n Port number

Port number to be used to connect to the oracle instance. Default port is 1521.

-d Database name

Name of database instance.

-u Username

Database user name.

-p Password

Database password for the corresponding user name.

-j Driver file location

Full path to thin driver jar file. This is not required if the jar file is already in the class path for HP SIM and jboss. Mxoracleconfig will report an error if the driver class cannot be loaded. Mxoracleconfig will not copy over a jar file if it already exists in the classpath for HP SIM and jboss.

-f Force flag to force a re-run.

Typically this command is run only once. This flag is provided if a re-run is required because of some type of user error such as specifying the wrong Oracle server or database instance.

3. Test the prerequisites:

```
/opt/mx/bin/mxinitconfig -l
```

This verifies and list all the prerequisites are present. You can review the log file found in `/var/opt/mx/logs/initconfig.log` to verify that the initialization completed.



NOTE HP SIM recommends resolving any warnings before continuing with the setup process.

4. Initialize HP Systems Insight Manager:

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

Note: The initialization of the upgrade is done in the background, which takes several minutes. To verify if the upgrade is 100% complete, view the file `/var/opt/mx/logs/initconfig.log`.

5. Verify that the `mxdomainmgr` and `mxdtf` daemons are running:

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

If they are not running, start them:

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

6. (Optional) If you plan to run the Mozilla browser on the CMS verify that Mozilla 1.7.3 or later is installed. To verify which version is installed, open the Mozilla browser, and select **Help> About Mozilla**.
7. (Optional) To use the CMS as a managed system, install WBEM, if it is not already installed. Because WBEM requires OpenSSL, be sure OpenSSL is installed on the CMS by running:

```
swlist OpenSSL
```

If this command returns "Error: Software "OpenSSL" was not found on host", then OpenSSL is not installed.

OpenSSL is available on Software Depot at

<http://www.hp.com/go/softwaredepot> or on your operating system media.

- a. Install the OpenSSL Software:

```
swinstall -s/directory/OpenSSL_depot OpenSSL
```

where `directory` is the path to the depot file, and `OpenSSL_depot` is the name of the OpenSSL depot file.

- b. Now, install WBEM:

```
swinstall -s /directory/depot B8465BA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/WBEM_download.depot B8465BA
```



NOTE To verify if WBEM (`cimserver`, `cimserverd`) daemons are running:

```
ps -ef | grep wbem .
```

On HP-UX 11i v2 (September 2004 or later) (B. 11 .23) WBEM is installed by default.

8. (Optional) Configure the Central Management Server (CMS) to send SNMP traps to itself.
 - a. Add the name of the CMS as a trapdest in the file `/etc/SnmpAgent.d/snmpd.conf` trap-dest:
`<cms_full_hostname_or_ip_address>`
 - b. Stop the SNMP Master agent and all subagents with the following command:
`/sbin/init.d/SnmpMaster stop`
 - c. Restart the SNMP Master agent and all subagents with the following command:
`/usr/sbin/snmpd`



NOTE After installation is complete, log out of the operating system and log back in to configure the new parameters to your system environment variables.

Tuning HP SIM (Optional)

Using SAM or the HP-UX Kernel Configuration tool (kcweb) or kctune, complete the following optional manual parameter adjustments, if needed.

- ▲ Set the `dbc_max_pct` kernel parameter. This is the percentage of physical memory that can be dynamically allocated for the data buffer cache. It defaults to 50%, which is usually too high. Set this variable to the percentage of your system physical memory that equals approximately 200 MB. For example, a server with 1 GB of RAM should have this value set at 20%. Refer to the `dbc_max_pct` for additional details in tuning this parameter.



NOTE This value cannot be less than `dbc_min_pct`, which cannot be less than 1%. See the `dbc_max_pct` man page for additional details.

NOTE For HP-UX 11i v2 (September 2004 or later) (B. 11 .23), these parameters are dynamic, and when you modify the parameters, a reboot of the system is not necessary.

Next Steps

Install and configure the required [Management Agents](#) on the systems that will be managed by the CMS. Next, complete the initial setup of HP Systems Insight Manager. Initial setup involves adding managed systems, adding users, setting up authorizations, and configuring event handling. Refer to [Chapter 12. Initial Setup](#) for details.

HP SIM is now installed and initialized on the CMS. Start the HP SIM GUI using Mozilla at `http://localhost:280/`. Refer to [Chapter 10. Using the Graphical User Interface](#) for details.



NOTE The HP SIM First Time Wizard appears when a user with full configuration rights logs in to HP Systems Insight Manager for the first time. The First Time Wizard configures only the basic settings of an initial setup for HP Systems Insight Manager. There are other options available. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

NOTE If installing ServiceGuard Manager for the first time, install version 5.0. To download ServiceGuard Manager 5.0, refer to

<http://www.hp.com/go/softwaredepot>, for more information.

When you install HP Serviceguard Manager, it recognizes HP SIM and automatically registers it for you.

5 Installing on Linux

Preparing the system

This procedure verifies that your system meets the minimum requirements, and prepares your system for HP Systems Insight Manager installation.



NOTE The “\” at the end of each command line represents that the command is on the same line.

To verify and prepare your system:

1. Verify your system meets the minimum requirements. Refer to "System requirements" for details.
2. Verify that HP Servicecontrol Manager is not installed by executing the following command:

```
rpm -qa | grep mx
```

This command determines if `mxcms`, `mxagent`, or `mxrepository` are installed. If they are installed, it returns the list of components starting with package name "mx." To remove them, execute the following command:

```
rpm -e mxcms mxagent mxrepository
```

3. Verify that earlier versions of PostgreSQL are not installed, or if you plan to use an Oracle database, refer to your Oracle provider for instructions.

Note: If this is a clean install of HP Systems Insight Manager and if PostgreSQL is installed, even if it is a supported version, you must remove it and let the HP SIM installer install a supported version unless you are installing over a previous version of HP SIM (4.0.1, 4.1 and 4.2). Refer to

[Chapter 8. Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0](#) for details.

Note: Removing PostgreSQL will remove your current database. If the current database must be saved, back it up before PostgreSQL is removed.

4. To back up your database, execute the following command:

```
cp -rp /var/lib/pgsql /var/lib/pgsql.old1
```

The `p` retains the permission, time, and date of all files and folders.

5. Verify if PostgreSQL is installed by executing the following command:

```
rpm -qa | grep postgresql
```

If PostgreSQL is not installed, the previous command does not return any results. Proceed to [Step 8](#) for more information. If PostgreSQL is installed, the previous command returns the list of components starting with package name "PostgreSQL."

6. To remove PostgreSQL-server, execute the following command:

```
rpm -qa | grep postgresql | xargs rpm -e
```

This command queries the installed component, starting with "postgresql" as the name, and removes the installed component.

7. Execute the following command to remove the PostgreSQL folder:

```
rm -rf /var/lib/pgsql
```

Note: The saved database file might not be compatible with the newer version of PostgreSQL that is installed with HP Systems Insight Manager. If you must access the data in this file, use a system that has the older version of PostgreSQL installed.

For Oracle:

Install Oracle on the local system before installing HP Systems Insight Manager. Create a database user name with DBA privileges, or if you plan on using Oracle as the remote database, you must have the database and user name with DBA privilege to configure HP Systems Insight Manager. Refer to [After Installing HP Systems Insight Manager](#) to configure HP Systems Insight Manager to use a newly created Oracle database.

8. Download the HP Systems Insight Manager software, or locate a copy on a depot server. To download the software, refer to <http://www.hp.com/go/hpsim>, and on the upper-left of the page under HP management software, select **Download**. The HP Systems Insight Manager's **Download** Page appears. Under **HP Systems Insight Manager and related components**, select **HP SIM-Linux** and **Download latest version of HP SIM-Linux** for a full product install.
9. In the directory where you downloaded or copied the files, change user permissions from read to read/write, and execute the `bin` file:

```
chmod +x *.bin
```

or

```
chmod +x HPSIM-Linux_C.05.00.01.00.bin
```

10. Verify that the following required software dependencies are available on your system, and install any that are not already installed.

- a. Verify that SSH is installed by executing the following command:

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

If SSH is not installed, the previous command does not return any results. Install SSH from your Linux operating system CD before continuing with the HP Systems Insight Manager installation.

- b. Verify that SNMP is installed by executing the following command:

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

If it is not installed, the previous command does not return any results. Install SNMP from your Linux operating system CD before continuing with the HP Systems Insight Manager installation.

- c. Verify that standard C++ libraries (`compat-libstdc++-7.3`) are installed:

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

If they are not installed, the previous command does not return any results. Install them from your Linux operating system CD before continuing with the HP Systems Insight Manager installation.

- d. Verify that the Linux glibc library is installed. If you plan to install Mozilla on your Central Management Server (CMS), the library must be installed first.

```
rpm -qa | grep glib
```

If it is not installed, the previous command does not return any results. Install it from your Linux operating system CD before continuing with the HP Systems Insight Manager installation.

- e. For Red Hat Enterprise ES Linux 3, verify that the GDK library (`gdk-pixbuf-0.22.0-3.0`) is installed. If you plan to install Mozilla on your CMS, this library must be installed first.

```
rpm -qa | grep gdk-pixbuf
```

If it is not installed, the previous command does not return any results. Install it from your Linux operating system CD before continuing with the HP Systems Insight Manager installation.

11. (Optional) If you are planning to run the Mozilla browser on the CMS, verify that Mozilla 1.7.3 or later is installed. To verify which version is installed, open the Mozilla browser, and select **Help**→**About Mozilla**.

Note: Mozilla is not required on the CMS. It can be used to access HP Systems Insight Manager from any network client. Most Linux distributions install Mozilla 1.0 as part of the base operating system.

To upgrade your version of Mozilla:

- a. Download the latest version for Linux at <http://www.mozilla.org/download> or <http://www.mozilla.org/releases>. Create a temporary directory called `mozillatemp`, and place the downloaded `.GZIP` file in that directory.
- b. Navigate into the `mozillatemp` directory, and decompress the archive:

```
cd path/mozillatemp
```

```
tar -zxvf moz*.tar.gz
```

where `path` is the location of the temporary directory you created in the previous step.

- c. Navigate into the `mozilla-installer` subdirectory that was created in the previous step, and run the installer:

```
cd mozilla-installer
./mozilla-installer
```

Follow the Mozilla install wizard to complete the remainder of the process.

- d. Verify that Mozilla installed correctly by running the browser:

```
/usr/local/mozilla/mozilla
```

The path `/usr/local/mozilla` is the default install directory. If you changed the install directory during the installation, this command must reference your path instead.

Note: If you are running GNOME or another desktop, you can edit the properties of the Mozilla icon to point to the version that you just installed.

Note: Use the **Tab** key to help enter in long commands accurately. Pressing the **Tab** key after entering the first letter or so of each directory name automatically fills in the rest of the name.

Installing and Configuring the Software

HP SIM can be installed automatically or manually.

Automatic install executes the `.bin` file, automatically laying down PostgreSQL and HP SIM with minimal user interaction. Manual install requires that you execute the separate steps to unpack files and install PostgreSQL and HP SIM.

Installation of HP Systems Insight Manager includes the PostgreSQL software dependency.

Automatically installing HP Systems Insight Manager

To install HP Systems Insight Manager with PostgreSQL, execute the following command:

```
./HPSIM-Linux_05.00.01.00.bin
```

Note: Refer to Chapter 5. Installing on Linux Preparing the System Step 9 for information on setting the permission on the file.

The `HPSIM-Linux_C.05.00.01.00.bin` file will extract the RPM Package Manager (RPM) install PostgreSQL, and then continue with the HP Systems Insight Manager installation.



NOTE To install HP Systems Insight Manager automatically, do not install PostgreSQL, or a older version of HP Systems Insight Manager.

NOTE After installation is complete, log out of the operating system and then log back in to set all the correct file permissions and system environmentals.

To complete the initial set up of HP Systems Insight Manager refer to ["After Installing HP Systems Insight Manager"](#) .

Manually installing HP Systems Insight Manager

1. Extract the `.rpm` files from the `.bin` file. Set the permissions to include the right to execute the `.bin` file by executing the following command:

```
./HPSIM-Linux_C.05.00.01.00.bin --keep --confirm
```

Note: Refer to Step 9 in the "Installing on Linux - Preparing the System" section for information on setting permissions.

2. Respond negatively to the prompt to run scripts for an Automatic install. The extracted files are placed in an `mxserver` subdirectory.
3. To change the directory to `mxserver`, execute the following command:

```
cd mxserver
```

4. Install the PostgreSQL database, using the appropriate .rpm files in the following order.

Note: The `rpm -i` command installs PostgreSQL on your system.

- Red Hat Enterprise Linux 3 Update 3 U4 and U5 AS/ES (This command is entered with no carriage returns.)

```
rpm -ivh postgresql-libs-7.4.1-1PGDG.i386.rpm \  
postgresql-7.4.1-1PGDG.i386.rpm \  
postgresql-server-7.4.1-1PGDG.i386.rpm
```

- Red Hat Enterprise Linux 4 U1 AS/ES (This command is entered with no carriage returns.)

```
rpm -ivh postgresql-libs-7.4.7-2PGDG.i386.rpm \  
postgresql-7.4.7-2PGDG.i386.rpm \  
postgresql-server-7.4.7-2PGDG.i386.rpm
```

- SUSE Linux Enterprise Server 8/UnitedLinux 1.0 Service Pack 3 (This command is entered with no carriage returns.)

```
rpm -ivh postgresql-libs-7.4-0.i586.rpm \  
postgresql-7.4-0.i586.rpm \  
postgresql-server-7.4-0.i586.rpm
```

- SUSE Linux Enterprise Server 9 Service Pack 1 or 2 (This command is entered with no carriage returns.)

```
rpm -ivh postgresql-libs-7.4.2-36.3.i586.rpm \  
postgresql-7.4.2-36.3.i586.rpm \  
postgresql-server-7.4.2-36.3.i586.rpm
```

5. Verify that the PostgreSQL status reads `running`.

- For Red Hat Enterprise Linux (all versions):

- a. Execute the `serviceconf` command. The Service Configuration window appears.

- b. Scroll down to the **postgresql** entry.

- c. Select the checkbox, save the changes, and start the service.

- d. Verify that the PostgreSQL daemon status is `running` by executing the following command:

```
/etc/rc.d/init.d/postgresql status
```

- For SUSE Linux Enterprise Server 8 and SUSE Linux Enterprise Server 9:

- a. View the status by executing the following command:

```
/etc/init.d/postgresql status
```

- b. Configure PostgreSQL to run during startup by executing the following command:

```
chkconfig postgresql 345
```

- c. If the status is `unused` in any version of Red Hat Linux or SUSE Linux, start the daemon by executing the following command:

- For SUSE Linux Enterprise Server 8 and SUSE Linux Enterprise Server 9

```
/etc/init.d/postgresql start
```

- For Red Hat Enterprise Linux (all versions)

```
/etc/rc.d/init.d/postgresql start
```



NOTE To install HP Systems Insight Manager on a system without OpenSSH or with a purchased version of SSH, use the `--nodeps` option on `rpm`.

For example, `rpm --nodeps -ivh` followed by the rpm files.

6. Install HP Systems Insight Manager using the .rpm files by executing the following command:

```
rpm -ivh hpsim-C.05.00.00.XXXXXXX.i386.rpm \  
hpsim-pgsql-config-C.05.00.00.XXXXXXX.i386.rpm
```

Note: Both files must be installed concurrently with a single command.

Note: After installation is complete, log out of the operating system and log back in to set all the correct file permissions and system environmentals.

After Installing HP Systems Insight Manager

1. If using Oracle as your database, continue with step 2. If you are using PostgreSQL as your database, continue with step 3.
2. For an Oracle database, run one of the following commands:

mxoracleconfig

located at `/opt/mx/bin` before proceeding with the following steps. This command can be invoked with or without command line arguments.

mxoracleconfig

You will be prompted for individual information for your Oracle database.

Or

```
mxoracleconfig -h hostname [-n port number] -d database name -u username  
-p password [-j driver jar file location] [-f ]
```

-h Hostname

Full DNS name or IP address of the Oracle server.

-n Port number

Port number to be used to connect to the Oracle instance. Default port is 1521.

-d Database name

Name of database instance.

-u Username

Database user name.

-p Password

Database password for the corresponding user name.

-j Driver file location

Full path to thin driver .jar file. This is not required if the .jar file is already in the class path for HP Systems Insight Manager; and jboss. Mxoracleconfig reports an error if the driver class cannot be loaded. Mxoracleconfig will not copy over a .jar file if it already exists in the classpath for HP Systems Insight Manager and jboss.

-f Force flag to force a re-run.

Typically, this command is run only once. This flag is provided if a re-run is required because of some type of user error such as specifying the wrong Oracle server or database instance.



NOTE Execute the **mxoracleconfig** command before the **mxinitconfig** command so that **mxinitconfig** will use Oracle as the database.

3. Test the prerequisites by executing the following command:

```
/opt/mx/bin/mxinitconfig -l
```

This utility should report that all server components are `Acceptable` and that it completed all tasks successfully.

Note: HP recommends resolving any warnings before continuing with the initializing and configuring HP Systems Insight Manager process.

4. Initialize and configure HP Systems Insight Manager by executing the following command:

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

Note: The initialization of the upgrade is done in the background, which takes several minutes. To verify if the upgrade is 100% complete, view the file by executing the following command:

```
/var/opt/mx/logs/initconfig.log
```

5. Verify that the `mxdomainmgr` and `mxdtf` daemons are running by executing the following command:

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

If they are not running, start them by executing the following command:

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

6. Configure the system to send SNMP traps.

Note: These steps might vary slightly, depending on your version of Linux. Refer to your Linux provider for details if these file paths and file names do not exist on your system.

- a. Verify that SNMP is installed by executing the following command:

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

If it is not installed, the previous command does not return a components list. Refer to your Linux provider for information on installing SNMP.

- b. Verify if the HP Server Management Drivers and Agents from the ProLiant Support Pack for Linux is installed by executing the following command:

```
rpm -qa | grep hpasm
```

If it is not installed, the previous command does not return a components list. If it is installed, verify that the HP Server Management Driver and agent daemon are running by executing the following command:

```
/etc/init.d/hpasm status
```

- c. If the the HP Server Management Drivers and Agents daemons are running, stop them using the following command:

```
/etc/init.d/hpasm stop
```

Note: If the HP Server Management Drivers and Agents daemon is not installed, omit this step and step F.

- d. Stop the SNMP daemon:

```
/etc/init.d/snmpd stop
```

- e. Edit the `snmpd.conf` file using any text editor.

For Red Hat Linux, run the following command for opening this file in the vi editor:

```
vi /etc/snmp/snmpd.conf
```

For SUSE Linux Enterprise Server 8, run the following command for opening this file in the vi editor:

```
vi /usr/share/snmp/snmpd.conf
```

- i. Remove the comment symbol (`#`) from the `trapsink` line, and add the IP address of the CMS. This system has HP Systems Insight Manager application running:

```
trapsink IPaddress
```

where *IPaddress* is the IP address of the CMS.

- ii. Add the CMS to the read-only community by adding the line:

```
rocommunity CommunityName IPaddress
```

where *CommunityName* is the SNMP community string used by the CMS and *IPaddress* is the IP address of the CMS.



NOTE Enter the information manually if it is not present.

- iii. Save the changes to the file. To save and close this file using the vi editor, press the Esc key, enter `:wq!`, and press the Enter key.

- f. Start the SNMP daemon by executing the following command:

```
/etc/init.d/snmpd start
```

- g. Start the HP Server Management Drivers and Agents daemon if it is installed on your system:

```
/etc/init.d/hpasm start
```

Next steps

Install and configure the required [Management Agents](#) on the [systems](#) that will be managed by the CMS. Next, complete the initial setup of HP Systems Insight Manager. Initial setup involves adding [managed](#)

systems, adding users, setting up authorizations, and configuring event handling. Refer to [Chapter 12. Initial Setup](#) for details.

Start the HP Systems Insight Manager graphical user interface (GUI) using Mozilla or Internet Explorer at <http://localhost:280/>. Refer to [Chapter 10. Using the Graphical User Interface](#) for details.



NOTE The HP Systems Insight Manager First Time Wizard appears when a user with full configuration rights logs in to HP Systems Insight Manager for the first time. The First Time Wizard configures only the basic settings of an initial setup for HP Systems Insight Manager. Other options are available. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

6 Upgrading from Insight Manager 7 Service Pack 2.3 to HP Systems Insight Manager 4.2



NOTE To upgrade from Insight Manager 7 Service Pack 2.3 to HP Systems Insight Manager 5.0, Insight Manager 7 Service Pack 2.3 must be upgraded to HP SIM 4.2 first. After this initial upgrade, follow the procedure to upgrade HP SIM 4.2 to 5.0. Refer to [Chapter 8. Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0](#) for more information.

The HP Systems Insight Manager Data Migration Tool is used to migrate Insight Manager 7 data to HP Systems Insight Manager. The Data Migration Tool exports user-defined data from Insight Manager 7 by extracting it and storing the information in a portable format. The Data Migration Tool then imports that user-defined Insight Manager 7 data into HP Systems Insight Manager. The migration process transfers custom data, which includes:

- User accounts and privileges
- User access control settings
- User-defined folders, tasks, and queries
- Discovered devices
- User-defined reports
- Device Type Manager rules
- Server certificate (for an in-place migration only)
- User-defined MIB and notice data (this must be manually recompiled)

In addition, received events and notices are archived.



NOTE You must be running Insight Manager 7 SP2.3 to upgrade to HP Systems Insight Manager 4.2. If you are running a version of Insight Manager 7 earlier than Insight Manager 7 SP2.3, upgrade to Insight Manager 7 SP2.3 before upgrading to HP SIM 4.2. If you have Insight Manager 7 Service Pack 2.3, 2.1, or 2.2 installed, the migration process offers an automatic upgrade to Insight Manager 7 Service Pack 2.3. If you have a version earlier than Service Pack 2, you are directed to the HP website to download the Softpaq that will enable you to upgrade to Insight Manager 7 SP2.3. Refer to the *Insight Manager 7 User's Guide* for information on upgrading from Insight Manager 7 to Insight Manager 7 SP2.3. Refer to the Transitioning to HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more in-depth detail on this process.

Your system must also meet the operating system and SQL/MSDE requirements listed in [Chapter 2. Installation overview and requirements](#).

NOTE The Data Migration Tool must be run by a user with full Windows administrative rights.

NOTE The HP Performance Management Pack was part of the Insight Manager 7 SP2.3 installation. If it is detected on your system, a migration utility for transferring data specific to it will also be launched.

Types of Migration

There are two types of migration:

- In-place
- Remote

In-place migration

This type of migration enables you to install HP Systems Insight Manager and, optionally, the HP Performance Management Pack on the same server that previously ran Insight Manager 7. As part of the in-place migration process, Insight Manager 7 is disabled and can only be re-enabled by uninstalling HP Systems Insight Manager and manually re-enabling Insight Manager 7. In-place migration preserves user-defined data, including the Insight Manager 7 server certificate.

Remote migration

This type of migration enables you to install HP Systems Insight Manager on a different server than Insight Manager 7. The remote migration process leaves Insight Manager 7 running after data has been exported and requires you to import the Insight Manager 7 and Performance Management Pack migration data files to your new HP Systems Insight Manager server. Remote migration preserves user-defined data except the Insight Manager 7 Server certificate.

Performing an In-Place Migration

1. Export Performance Management Pack and Insight Manager 7 data:
 - a. Upgrade from Insight Manager 7 Service Pack 2.3 to HP Systems Insight Manager 4.2 through the 7.20 HP Management CD or by downloading the HP Systems Insight Manager 4.2 software. To download the software, go to <http://www.hp.com/go/hpsim>, and click **Download**.
 - b. Begin the migration process by launching `setup.exe` from the download package or from the Management CD. Select **Products**→**HP Systems Insight Manager**→**Install** on the Insight Manager 7 server. The HP Systems Insight Manager Welcome screen appears. The Welcome screen displays links to the following documentation:
 - Readme (readme.txt)
 - Release Notes (hpsim-releaseNote.pdf)
 - User Guide (hpsim-userGuide.pdf)A background setup screen appears showing that pre-installation is “In Progress.” If the Performance Management Pack that was installed with Insight Manager 7 is detected on your system, the Performance Management Pack Migration Utility for data export is launched.
 - c. Follow the screen prompts to completion before continuing with the Insight Manager 7 data export. On completion of the data export for the Performance Management Pack, `setup` detects that you are running Insight Manager 7 SP2.3 or later and automatically launches the HP Systems Insight Manager Data Migration Tool. The Data Migration Tool dialog screen appears.
 - d. Click **Next** to continue.
 - e. Select **Next** to confirm data export to the following directory and file: `C:\Program Files\HP\System Insight Manager Data Migration Tool\user-data.dmt`. The export of data begins.
 - f. When the export of data successfully completes, click **Next**.
 - g. Select the **In-place migration (disable Insight Manager 7)** radio button.
 - h. Click **Next**. The HP Systems Insight Manager Data Migration Tool export success screen appears and indicates that Insight Manager 7 has been disabled.
 - i. Click **Finish** to continue with the installation of the HP Systems Insight Manager components. Refer to [Chapter 3. Installing on Windows](#) for details. The background setup screen shows that pre-installation is “Done” and the installation is now “In Progress.”
2. Click **Finish**. The background setup screen shows that installation is “Done” and the post-installation is now “In Progress.” The import of Insight Manager 7 and Performance Management Pack data has automatically begun.

After all the HP Systems Insight Manager components have been installed, the Insight Manager 7 Data Migration Tool dialog screen automatically appears.
3. Click **Next**. A data import screen appears, showing that the data will be imported from the following directory and file: `C:\Program Files\HP\System Insight Manager Data Migration Tool\user-data.dmt`.
4. Click **Next** to start the Data Import. The process might take more than an hour depending on the amount of user-defined data and the configuration of the HP Systems Insight Manager. A status window shows the progress.
5. When data import completes, click **Next**. A message appears, stating that you must log in to HP Systems Insight Manager to complete the migration process by verifying user accounts, assigning authorizations, and enabling tasks and Automatic Event Handling rules.
6. Click **OK**.

7. At the data import success screen, click **Finish**.
If the Performance Management Pack was upgraded, then the Performance Management Pack Migration Utility for data import is automatically launched.
8. Follow the screens to completion. The background setup screen shows the post-installation is “Done.”
9. Click **Finish** on the background setup screen, and reboot the system at this time if any HP Systems Insight Manager components indicated the need for this.



NOTE For an in-place migration the DMI Indication handler service should be disabled on the CMS.

Performing a Remote Migration

1. Export Performance Management Pack and Insight Manager 7 data:
 - a. Acquire HP Systems Insight Manager 4.2 by downloading the HP Systems Insight Manager software from <http://www.hp.com/go/hpsim> and selecting **Download** or through the 7.20 HP Management CD.
 - b. Start the migration process by launching `setup.exe` from the download package or from the Management CD. Select **Products**→**HP Systems Insight Manager**→**Install**.
The HP Systems Insight Manager Welcome screen appears. The Welcome screen displays links to the following documentation:
 - Readme (readme.txt)
 - Release Notes (hpsim-releaseNote.pdf)
 - User Guide (hpsim-userGuide.pdf)
 A background setup screen appears, showing that pre-installation is “In Progress.” If the Performance Management Pack that was installed with Insight Manager 7 is detected on your system, the Performance Management Pack Migration Utility for data export is launched.
 - c. Follow the screen prompts to completion before continuing with the Insight Manager 7 data export. On completion of the data export for the Performance Management Pack, `setup` detects that you are running Insight Manager 7 SP2.3 or later and automatically launches the HP Systems Insight Manager Data Migration Tool. The Data Migration Tool dialog screen appears



NOTE If Insight Manager 7 Service Pack 2, 2.1 or 2.2 is detected, the HP Systems Insight Manager Data Migration Tool displays an option to upgrade to Insight Manager 7 SP2.3. Select this option and follow the screen prompts to install the Softpaq. When complete, launch `setup.exe` again from the download package or from the Management CD, select **Products**→**HP Systems Insight Manager**→**Install** again to start the export of Insight Manager 7 data.

- d. Click **Next** to continue.
- e. Click **Next** to confirm data export to the following file: `C:\Program Files\HP\System Insight Manager Data Migration Tool\user-data.dmt`. The export of data begins.
- f. When the export of data successfully completes, click **Next**.
- g. Select the **Remote migration (do not disable Insight Manager 7)** radio button.
- h. Click **Next**. HP Systems Insight Manager Data Migration Tool export success screen appears and instructs you to copy the export file to the server on which HP Systems Insight Manager will be installed.
- i. Click **Finish** to exit the Data Migration Tool. The background process shows pre-installation is “Done” and installation is “In Progress.”
- j. Cancel out of the **Welcome screen** for the HP Systems Insight Manager install. The background setup shows that both installation and post-installation are “Not Done.”
- k. Click **Finish** on the background setup screen to close it out.
- l. Copy the file `C:\Program Files\HP\System Insight Manager Data Migration Tool\user-data.dmt` to a location where it can be accessed from the new HP SIM 4.2 server.
- m. Copy the file `PMP DMT installation directory\data\pmp.jar` to a location where it can be accessed from the new HP Systems Insight Manager 4.2 server. The Performance

Management Pack Data Migration Tool installation directory is usually `c:\Program Files\HP\Performance Management Pack Data Migration Tool`.

- n. Go to the server to be used for the new HP Systems Insight Manager, and launch `setup.exe` from the download package or from the Management CD. Select **Products**→**HP Systems Insight Manager**→**Install** to start the HP Systems Insight Manager components installation. The background setup screen will show pre-installation is “Not Done” and installation is now “In Progress:”
 - o. Click **Install** on the HP Systems Insight Manager welcome screen to begin the installation of HP Systems Insight Manager components. Refer to [Chapter 3. Installing on Windows](#) for details.
 - p. Click **Finish** when the installation is complete to close the HP Systems Insight Manager Installer window. The background set up screen will show installation is “Done” and post-installation is “Not Done.”
 - q. Click **Finish** on the background setup screen to close it out.
2. Import Insight Manager 7 and Performance Management Pack data:
 - a. After HP Systems Insight Manager 4.2 and all its components have been installed, launch `dmtshell.exe` from the download package or from the Management CD on HP Systems Insight Manager 4.2 server. The background setup screen will not display. The Insight Manager 7 Data Migration Tool dialog screen automatically appears.
 - b. Click **Next**.
 - c. Specify the location of the `user-data.dmt` file as noted during the export process when prompted.
 - d. Click **OK** to dismiss the prompt.
 - e. Click **Open** when the export file is located.
 - f. Click **Next**. Insight Manager 7 Data Import starts. The process might take more than an hour, depending on the amount of user-defined data and the configuration of the HP Systems Insight Manager. A status bar shows the progress.
 - g. Click **OK**.
 - h. Click **Finish**.
 3. If a migration file for the Performance Management Pack was created, launch `pmpdmt.exe` to import the Performance Management Pack data. Follow the screens to completion, pointing to the location of the `pmp.jar` file as noted during the export process.
 4. If the Performance Management Pack 2.1 server licenses/logged data is migrated and after HP Performance Management Pack 3.0 is installed, launch `pmpsshell.exe` to import Performance Management Pack 2.1 server licenses/logged data. Follow the screens to completion, pointing to the PMP data file (`pmp.jar`) as noted during the export process.
 5. Reboot the system at this time if any of the HP Systems Insight Manager components indicate the need

7 Upgrading from HP Servicecontrol Manager to HP Systems Insight Manager

This upgrade installs the HP SIM 4.2 files and migrates your HP Servicecontrol Manager (SCM) data to be compatible with HP SIM 4.2. The upgrade installation migrates all custom data including:

- Users
- Systems
- System groups
- Tools
- Toolboxes
- Authorizations

HP SCM and HP SIM cannot coexist on the same system.



NOTE Migration from SCM 3.0 to HP SIM 4.2 on a Linux CMS is not supported.

NOTE You must be running SCM 3.0 to upgrade to HP SIM 4.2. If you are running a version of SCM earlier than 3.0, you must upgrade to 3.0 before upgrading to HP SIM 4.2. Refer to the *HP Servicecontrol Manager 3.0 User Guide* for information on upgrading from SCM 2.5 to SCM 3.0.

NOTE Before upgrading SCM 3.0 to HP SIM 4.2, managed systems should be upgraded and have SSH installed.

NOTE If you have an unconfigured SCM 3.0 on your system, you can upgrade to HP SIM 5.0. If SCM 3.0 is configured and you try to install HP SIM 5.0, the upgrade will fail because you must upgrade to HP SIM 4.2 first.

Upgrading from SCM 3.0 to HP Systems Insight Manager 4.2

To upgrade a SCM 3.0 to HP SIM 5.0, SCM must be upgraded to HP SIM 4.2 first.



NOTE During an upgrade of SCM 3.0 to HP SIM, the existing database is migrated and the password is preserved in the back up directory.

NOTE When upgrading SCM 3.0 to HP SIM, new Remote Method Invocation (RMI) keys and a keystore are created. The keystore is moved to a back up directory.

1. Verify that SCM is running by entering the following:

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

Wait some time, and if SCM is not running, start the service:

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

2. Tune the kernel using the Java Out-of-Box fileset. For more information, go to <http://www.hp.com/products1/unix/java/java2/outofbox/index.html>. This product can be available for you to install with HP SIM, either as part of the download depot file containing HP SIM 5.0 or from the Application Release media. The kernel parameter values it adjusts are listed in the following table.



NOTE Java Out-of-Box is a stand-alone bundle that reboots the system after it is installed.

Java Out-of-Box settings

Java Out-of-Box settings	Kernel parameter values
max_thread_proc	3000
maxdsiz	2063835136
maxfiles	2048

maxfiles_lim	2048
maxusers	512
nfile	4097
nkthread	6000
nproc	2048
tcp_conn_request_max	2048



NOTE The maxusers parameter is obsolete in HP-UX 11i v2 (September 2004 or later) (B.1 1 .23).

3. Using System Administration Manager (SAM) or the HP-UX Kernel Configuration tool (kcweb), complete the following manual parameter adjustments.
 - a. Set the `dbc_max_pct` kernel parameter, which is the percentage of physical memory that can be dynamically allocated for the data buffer cache. It defaults to 50%, which is usually too high. Set this variable to the percentage of your system physical memory that equals approximately 200 MB. For example, a server with 1 GB of RAM should have this value set at 20%.

Note: This value cannot be less than `dbc_min_pct`, which cannot be less than 1% of your system physical memory.
 - b. Increase the `nfile` parameter to at least 12000. This value might be increased to 30000 depending on your environment. If you get an error that you cannot open a file, increase this value.
 - c. For proper database operation, set the "semms" kernel parameter to a minimum value of 2048 and the `semnmi` kernel parameter to a minimum value of 1024.

Note: For HP-UX 11i v2 (September 2004 or later) (B.11.23), these parameters are dynamic, and when you modify the parameters, a reboot of the system is not necessary.

4. Install PostgreSQL, SSH, and WBEM:

```
swinstall -s /directory/depot ixPostgreSQL T1471AA B8465BA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot ixPostgreSQL T1471AA B8465BA
```



NOTE To verify that the WBEM (`cimserver`, `cimserverd`) and SSH (`sshd`) daemons are running, enter the following commands:

```
psef | grep wbem
```

```
psef | grep ssh
```

5. Install HP Systems Insight Manager:

```
swinstall -s /directory/depot T2414BA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot T2414BA
```

6. Verify that the `mxdomainmgr` and `mxdtf` daemons are running:

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

If they are not running, start them:

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

7. (Optional) Configure SNMP to send traps to the CMS:
 - a. Add the full host name or IP address of the CMS as a trapdest in the file `/etc/SnmpAgent.d/snmpd.conf`.
`trap-dest: hostname_or_ip_address`
 - b. Stop the SNMP Master agent and all subagents with the following command:
`/sbin/init.d/SnmpMaster stop`
 - c. Restart the SNMP Master agent and all subagents with the following command:
`/usr/sbin/snmpd`
8. Log in to the HP SIM GUI. For assistance with this, refer to [Chapter 10. Using the Graphical User Interface](#).
9. If, after logging in to HP SIM, you find that some items (toolboxes, users, tools, systems, system groups, or authorizations) did not upgrade correctly, perform the following. Otherwise, continue to step 10.

IMPORTANT: These steps must be performed in the order specified. You can, however, start with the first step that applies to you. For example, if node groups and authorizations failed to migrate, but everything else migrated properly, start with step e.

 - a. Migrate toolboxes (roles) by running the following command from the command line on the CMS:
`mxtoolbox -af /var/opt/mx/bak/3.0/zzz_mxrole.3_0.xml`
 If the message A toolbox named <toolbox> already exists in the system appears, log in to HP Systems Insight Manager and delete all toolboxes except for All Tools and Monitor Tools, and repeat this step.
 - b. Migrate users by running the following command from the command line on the CMS:
`mxuser -af /var/opt/mx/bak/3.0/zzz_mxuser.3_0.xml`
 If the message A user named <user> already exists in the system appears, log in to HP SIM and delete all users except for the user used to log in, and repeat this step.
 - c. Migrate tools by running the following command from the command line on the CMS:
`mxtool -af /var/opt/mx/bak/3.0/zzz_mxtool.3_0.xml`
 This command can display many Cannot add <tool> because it already exists in the system messages, but these messages can be safely ignored.
 - d. Migrate updated definition of tools and ensure all the tools are displayed correctly within the HP Systems Insight Manager tool menu by running the following command from the command line:
`sh fixmenu.sh scmtdefs.data /var/opt/mx/bak/3.0/tools /var/opt/mx/tools`
 - e. Migrate systems (nodes) by running the following command from the command line on the CMS:
`mxnode -af /var/opt/mx/bak/3.0/zzz_mxnode.3_0.xml`
 If mxnode encounters any duplicate systems (nodes), it continues without displaying any messages.
 If mxnode encounters a host name that cannot be resolved, the following error message appears. Unknown host: <node_name>. Node ignored. The remaining nodes continue to be processed. However, the missing node might affect the success of migrating node groups.
IMPORTANT: When the command returns, log in to HP Systems Insight Manager, display the All Systems list, and wait for all of the expected nodes to appear in the list before proceeding to the next step. The amount of time varies based on system performance and the number of nodes being added.
 - f. Migrate system groups (node groups) by running the following command from the command line on the CMS:
`mxngroup -af /var/opt/mx/bak/3.0/zzz_mxngroup.3_0.xml`
 If the message A node group named <group> already exists in this system appears, log in to HP SIM and delete all node groups except for All Managed Systems and CMS, and repeat this step.
 If the message The name <node_name> does not represent a node in this system appears, then a node in the node group is missing, and processing on the file stops. Add the node

using `mxnode -a <node_name>`, or log in to HP SIM and add the node through Manual Discovery. Then repeat this step.

- g. Migrate authorizations by running the following command from the command line on the CMS:

```
mxauth -af /var/opt/mx/bak/3.0/zzz_mxauth.3_0.xml
```

If this command encounters any duplicate authorizations, it continues without displaying any messages.

Note: If the names contain characters such as underscore, space, and symbols, they might not be migrated because these characters are not supported.

- h. If, after taking the previous steps, items such as menus are still missing or out of place, run the following command:

```
sh /opt/mx/bin/fixmenu.sh scmtdefs.data /var/opt/mx/bak/3.0/tools  
/var/opt/mx/tools
```

10. Using the GUI, add the default WBEM user name and password to the **Global Protocol Settings** page.

Note: An account for at least one of the WBEM user name and password combinations must exist on the CMS.

- Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
- In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name and password.
- Click **OK**.

Note: After upgrading to HP Systems Insight Manager, you must run identification for all network devices, racks, and enclosures to appear on the **System Overview** page.

After this initial upgrade, follow the procedure to upgrade HP SIM 4.2 to 5.0. Refer to

Chapter 8. Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0 for more information.

Upgrading Existing Managed Systems

1. Install SSH on the managed systems:

On HP-UX:

- a. Set up a depot that includes the SSH product.
- b. Run the `Install Software` command on all HP-UX DTF managed systems.

```
mxexec -t "Install Software" -n <hpux_nodes>
```

This tool is MSA and requires a DISPLAY to run a GUI.

2. Upgrade the CMS. Refer to "Upgrading from SCM 3.0 to HP Systems Insight Manager 4.2" for more information.
3. On the CMS, copy the SSH-generated public key from the CMS to the managed system, and place it in the authorized keys file of the execute-as user (root or administrator).

Important: If the CMS is not an HP-UX system, on a non-English CMS, ensure that an administrator account exists on the CMS and that `mxagentconfig` has been run on the CMS for the created administrator account.

- a. Launch the **Manage SSH Keys** dialog box from the CMS command prompt:

```
mxagentconfig -a -n hostname -u username -p Password
```

- b. Click **Connect**.

Alternatively, you can configure SSH through the command line version of `mxagentconfig`. On the CMS, enter `mxagentconfig -?` for usage.



NOTE Using the `-p` option makes the password available in "ps" output, so HP recommends using the `-f` option (with a file only readable by root) when using `mxagentconfig -a`. When you use the `-p` option, enclose the password in single quotes if the password has any special characters like `&` or `$`.

8 Upgrading HP Systems Insight Manager 4.x to HP Systems Insight Manager 5.0

This chapter provides the steps to upgrade HP SIM 4.x to HP SIM 5.0



NOTE The "\" at the end of each command line indicates that the rest of the command is on the next line.

NOTE If you have MSDE installed on a previous version of HP SIM and are using MSDE, and are upgrading to HP SIM 5.0, HP SIM 5.0 requires that MSDE have the TCP/IP protocol enabled. Therefore, you must enable the TCP/IP protocol when upgrading from HP SIM 4.x to 5.0:

1. Select **Start>Run** and enter `svrnetcn.ext`.
2. In the **Disabled Protocols** box, select **TCP/IP**.
3. Click **Enable**.
4. Click **OK**.

NOTE HP SIM does not support upgrading to an Oracle database. Oracle is only supported on a fresh installation for a Custom install of HP SIM.

Upgrading HP SIM 4.x to HP SIM 5.0 - Windows

1. Verify that HP SIM 4.x or later is running on the system.
2. Download the software or install it from the HP Management CD.

To download the software, refer to <http://www.hp.com/go/hpsim>, and on the upper-left of the page under HP management software, click **Download**. The HP SIM **Download** Page appears. Under **HP Systems Insight Manager and related components**, select **HP SIM-Windows>Download latest version of HP SIM - Windows** for a full product install.

To use the Management CD, place the CD in the CD-ROM drive. The CD autorun feature launches a license agreement. Agree to the license agreement, and click the **Products** tab. Click **Install** under HP Systems Insight Manager or click **Explore CD** and run `setup.exe` located at `\hpsim\win_ia32\` to launch the installer.

The **HP Systems Insight Manager Setup** window appears. The **Setup** window displays links to the following documentation:

- ReadMe (Adobe format)
- Release Notes (Adobe format)
- Installation and User Guide (Adobe format)

3. Click **Install** to start the install process.

Note: The administrative account used to install HP SIM will be the initial login account.

The **HP Systems Insight Manager Setup** "Installation status" window appears with the following three stages:

- Pre-Installation

Examines this system for local instances of MSDE, or SQL Server 2000 and displays the **Optional MSDE 2000 SP3a installation** window if none are found.

Note: If the server reboots, the setup shell restarts automatically. If setup was initiated from a mapped drive and the mapped drive is not available on reboot, the setup shell fails to launch.

- Installation

Launches the Install Shell and installs HP SIM and other HP management software products.

- Post-Installation

Completes the import of PMP data when doing an upgrade.

Note: This window is immediately covered by the **HP Systems Insight Manager Setup Check** window. However, The **HP Systems Insight Manager Setup** Installation status window remains open, and when each stage is in progress, it states "In Progress." When each stage of the setup

is complete, it states "Done." After HP SIM and all components have been installed, click **Finish** to close the **HP Systems Insight Manager Setup** Installation status window and return to the desktop.

The **HP Systems Insight Manager Installer** window appears.

4. Click **Install** to begin. The **Select Installation Type** window appears.
For a Typical install, refer to [Typical install](#) for more information.
For a Custom install, refer to [Custom install](#) for more information.

Typical install

1. Click **Typical** to install the included components with minimal user interaction listed under the **Available Components for Install**.

Available components for install	Typical installation	Custom installation
System Management Homepage	Included	Included
OpenSSH for Windows 3.7.1p1-1	Included	Optional
WMI Mapper	Included	Optional
HP Systems Insight Manager	Included	Included
HP ProLiant Essentials Performance Management Pack	Included	Optional
HP Version Control Repository Manager	Included	Optional
HP ProLiant Essentials Virtualization Management Software	Included	Optional
HP Systems Insight Manager Installation Information	Included	Optional

Note: If a component is not listed as being available for installation on the CMS, then the HP SIM install shell has determined one of the following:

- The installation prerequisites for the component have not been met.
- The component is currently installed.

If the component that is present on the CMS is an older version than what is bundled with the HP SIM install shell and it supports an in-place upgrade, it will appear in the component list.

Note: SSH Server and Version Control Repository Manager components will not be listed if they were installed in version 4.0.

Note: If you choose not to install or upgrade a component during the upgrade of HP Systems Insight Manager, you can run setup.exe again and at that time select the components that are to be installed or upgraded.

The **Typical Install - Service Account Credentials** window appears. The Domain and Username fields default to the installing account credentials, and these credentials cannot be edited.

2. Enter the password for this account. Click **Next**. The **Typical Install - Database Configuration** window appears.
3. Enter the **account credentials** for the database server. The installing user account will be pre-populated in the Username field and cannot be edited. The Host field will also be pre-populated with the local host name, but it can be edited.
4. If using a local SQL Server or MSDE, provide the password for the installing user, and click **Next** to proceed. Typical install requires the installing user account to exist on the remote Database server. If your database is not local then you must supply the database server name and the password. Click **Next**.

Note: HP SIM does not support the following in a user name and password:

- A blank password
- A space followed by a double-quote
- A backslash (\)

If you use these characters in your user name or password, the HP SIM database initialization fails.

Note: In case of a reboot, if you just installed MSDE, the administrative credentials are those you used to log in before installing MSDE. Windows authentication is required to connect to the SQL server (whether locally or remotely). In addition, these credentials will also be your HP SIM administrative user login credentials. Any account that is a member of the administrator group will have administrator rights to MSDE. The local security policy will be modified to give you the following rights: log on as a service, create a token object, and replace a process level token. In addition, for Windows XP SP2 and Windows 2003 SP1 or later, Component Object Model (COM) security will be updated to allow remote access and activation by everyone and anonymous users. Refer to HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more details.

The **Typical Install-Software Selection** window appears. This window displays the complete list of the available components with a checkbox next to each one. If the checkbox is selected and disabled, the component is deemed a mandatory component and cannot be deselected. All the components that are under the Typical Install column of the **Select Installation Type** window should have disabled checkboxes. The amount of required disk space is also listed for each component.

5. Click **Next** to verify that enough disk space exists for the selected components, and if enough exists, the **Typical Install – Summary** window appears. The **Typical Install - Status** window appears. As each component is being installed, it states "In Progress" beside the component's name. After the component has installed, it states "Installed Successfully." When all of the HP SIM components have been installed, the **HP Systems Insight Manager Installation Information** window appears. This window has links for the Version Control Installation Guide, to help you configure Version Control and the System Management Homepage.
6. Click a link to view the Version Control Installation guide, or click **OK** and the **Typical Install - Status** window appears again. After all components have been installed, they have an installed status. The HP SIM Installation Information status states, "Success." Click **Finished**. Typical Installation is complete.



NOTE For more information regarding where the System Management Homepage default settings are stored during a typical installation and how to change them, refer to the System Management Homepage Installation Guide at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Custom install

1. Click **Custom** to select the individual components under the **Available Components for Install** and configure them during installation.

Available components for install	Typical installation	Custom installation
System Management Homepage	Included	Included
OpenSSH for Windows 3.7.1p1-1	Included	Optional
WMI Mapper	Included	Optional
HP Systems Insight Manager	Included	Included
HP ProLiant Essentials Performance Management Pack	Included	Optional
HP Version Control Repository Manager	Included	Optional
HP ProLiant Essentials Virtualization Management Software	Included	Optional
HP Systems Insight Manager Installation Information	Included	Optional

Note: If a component is not listed as being available for installation on the CMS, then the HP SIM install shell has determined one of the following:

- The installation prerequisites for the component have not been met.
- The component is currently installed.

If the component that is present on the CMS is an older version than what is bundled with the HP SIM install shell and it supports an in-place upgrade, it will appear in the component list.

Note: SSH Server and Version Control Repository Manager components will not be listed if they were installed in version 4.0.

Note: If you choose not to install or upgrade a component during the upgrade of HP Systems Insight Manager, you can re-run the setup.exe and at that time select the components that are to be installed or upgraded.

2. The **Custom Install-Software Selection** window appears. This window displays the complete list of the available components with a checkbox next to each one. If the checkbox is selected and disabled, the component is deemed a mandatory component and cannot be cleared. The amount of required disk space is also listed for each component.
3. Click **Next** to verify if enough disk space exists for the selected components. If enough space exists, the **Custom Install – Summary** window appears.
4. Select **Install** to initiate the installation process. This process installs all the products listed in the **Selected Components** table. The **Custom Install - Status** window appears. As you install each component, it states "In Progress" beside the component's name. After the component has installed, it states "Installed Successfully."
5. install System Management Homepage:

If the System Management Homepage is not installed, the **System Management Homepage Setup** window appears. This InstallShield Wizard guides you through the install of System Management Homepage. Click **Next**. The **Operating Systems Groups** window appears.

Note: If at any time during the install of System Management Homepage you click **Cancel**, the installation and setup of the System Management Homepage ends.

- a. Select **Administrator**, **Operator**, or **User** from the **Operating Systems Group Name** field.
- b. Enter the group name of an operating systems group in the **Group Name** field. Click **Add**. The group name is added. A maximum of five entries can be added for each group level. Click **Next** to continue.

Note: To delete a group name, select the group name, and click **Delete**.

- c. From the **User Access** window, configure the System Management Homepage for the following access types:

- Select **Anonymous Access** to enable anonymous access to unsecured pages.
- Select **Local Access Anonymous** or **Local Access Administrator** to set up the System Management Homepage to automatically grant local IP addresses at the selected access level.

Caution: Selecting **Local Access** with Administrator privileges provides any users with access to the local console full access without prompting them for a user name or password.

- d. Click **Next**. The **Trust Mode** window appears.
- e. Select the level of security you want to provide from one of the three trust modes:
 - Trust By Certificate
 - i. Select **Trust By Certificate**, and click **Next**. The **Trusted Certificates** window appears. The **Trusted Certificates** window allows trusted certificate files to be added to the **Trusted Certificate List**.
 - ii. Click **Add File** to browse and select any certificates to be included in the **Trusted Certificate List**. The **Select File** window appears. If an invalid file name is entered in the file name field, an error message appears, indicating the file does not exist. Click **OK** to select another file, or click **Open** to add the file to the **Trusted Certificate List**. The **Trusted Certificate List** appears. Click **Next**.

Note: If you click **Next** without adding any certificates to the list, and no certificates exist from a previous installation, a message appears, indicating that if you do not specify any trusted certificates, HP SIM cannot access the HP Insight Management Agent on this system. Click **OK** if you do not want HP SIM to access the Insight Management Agent on this system, or click **Cancel** to close the window and add the trusted certificates to the list.

Note: The **Trust By Certificates** option enables the System Management Homepage system and the HP SIM system to establish a trust relationship by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before enabling access.

or

- i. Click **Import**. The **Import Server Certificate** window appears.
- ii. Enter the name or IP address of the server whose certificate you want to import.
- iii. Click **Get Cert**. The certificate information appears.
- iv. Verify the certificate information. If you want to add this certificate to the **Trusted Certificate List**, click **Accept** and the certificate is added to the **Trusted Certificate List**, or click **Cancel** if you do not want to add it to the **Trusted Certificate List**. The **Trusted Certificate List** appears. Click **Next**.

Note: You can add an unlimited number of trusted certificates.

Note: To delete a certificate, select the certificate, and click **Delete**. The selected certificate is removed.

- v. From the **IP Binding** window, select the IP Binding checkbox if you would like to bind to IP addresses that match a specific subnet and mask. Click **Next**.
- vi. From the **IP Restricted Logins** window, select the Enable IP Restricted Logins checkbox if you would like to include or exclude specific IP addresses or IP address ranges. Click **Next**, and the **Summary Panel** appears.

- Trust By Name

- i. Select **Trust By Name**. Click **Next**.
- ii. The **Trusted Server** window appears. Enter the names of the servers you want to trust.

Note: Although the **Trust By Name** mode is a slightly stronger method of security than the **Trust All** mode, it still leaves your system vulnerable to security attacks. The **Trust By Name** mode sets up the System Management Homepage to only accept certain requests from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure and can prevent non-malicious access. For example, you might want to use the **Trust By Name** option if you have a secure network, but your network has two groups of administrators in two separate divisions. The **Trust By Name** option would prevent one group from installing software to the wrong system. This option does not verify anything other than the HP SIM server name submitted.

Note: The server name cannot contain the following characters:

~ ! ` @ # \$ % ^ & * () + = " : ' < > ? , | ;

- iii. Click **Add** to add the name of a server you want to trust. Click **Next**.

Note: If you click **Next** without adding any server names to the list, an error message appears, indicating that if you do not specify any trusted server names, HP SIM cannot access the Insight Management Agent on this system. Click **OK** to proceed without trusting any systems, or click **Cancel** to close the window and add server names to the list.

Note: To delete a certificate, select the certificate and click **Delete**. The selected certificate is removed.

- iv. From the **IP Binding** window, select the IP Binding checkbox if you would like to bind to IP addresses that match a specific subnet and mask. Click **Next**.
- v. The **IP Restricted Logins** window appears. Select the Enable IP Restricted Logins checkbox if you would like to include or exclude specific IP addresses or IP address ranges. Click **Next**, and the **Summary Panel** appears.

- Trust All

- i. Select **Trust All**. Click **Next**.
- ii. The **IP Binding** window appears. Select the IP Binding checkbox if you would like to bind to IP addresses that match a specific subnet and mask. Click **Next**.

Note: The **Trust All** option leaves your system vulnerable to security attacks and sets up the System Management Homepage to accept certain requests from any server. For example, you might want to use **Trust All** if you have a secure network, and everyone in the network is trusted.

Note: You can add up to five subnet IP address/netmask pairs.

Note: If you click IP Binding but do not specify the IP address/netmask then you might not be able to connect to the System Management Homepage.

The **IP Restricted Logins** window appears. The **IP Restricted Logins** window enables you to select specific IP addresses or IP address ranges to include or exclude from gaining login access. Although optional, the System Management Homepage can restrict login access based on the IP addresses of the machine attempting to gain access.

- iii. Select **Enable IP Restricted Logins**, and click **Next**. The **IP Addresses to Include** window appears. This window enables you to specify the IP address or IP address ranges to grant login access permission. If there are IP addresses in the **Inclusion** list, then only those IP addresses are enabled for login privileges. If there are no IP addresses in the Inclusion list, then login privileges are permitted to all IP addresses that are not in the **Exclusion** list.

Note: A single address and ranges of addresses can be accepted in the **IP Restricted Logins** window. Enter the single address in the first box.

- iv. In the **Include** field, enter a beginning IP address to which you want to grant login access. In the **To** field, enter an ending IP address to which you want to grant login access. All IP addresses that fall between the beginning and ending IP addresses are granted login access. Click **Add**. The IP address or IP address range is added to the **Exclusion** list. Select an IP address or IP address range, and click **Delete** to remove it from the **Exclusion** list. Click **Next**.

Note: If you entered an invalid IP address or IP address range, an error message appears indicating the IP address is invalid. Click **OK**. Enter a valid IP address or IP address range, and click **Add** again. The **IP Addresses to Exclude** window appears.

In the **Exclude** field, enter a beginning IP address to which you want to deny login access.

- v. In the **To** field, enter an ending IP address to which you want to deny login access. All IP addresses that fall between the beginning and ending IP addresses are denied login access.
- vi. Click **Add**. The IP address or IP address range is added to the **Inclusion** list. Select an IP address or IP address range, and click **Delete** to remove it from the **Inclusion** list. Click **Next**.

Note: If you entered an invalid IP address or IP address range, an error message appears, indicating the IP address is invalid. Click **OK**. Enter a valid IP address or IP address range, and click **Add** again.

Note: If **Next** is selected without adding any IP addresses to either the **Include** or **Exclude** lists, a warning message appears stating, IP Restricted Login checkbox will be marked as disabled. Do you want to proceed without adding any IP Address restrictions? If you select **OK**, the **IP Restricted Login** option on the **IP Restricted Login** window is cleared.

The **Summary Panel** appears. The **Summary Panel** lists the location where the System Management Homepage is installed, the amount of space the installation requires, and the summary of the options that you specified during the installation.

- f. Click **Next**. The installation process is started. Click **Finish** to exit the wizard.

Note: If HP SIM is installed after System Management Homepage is installed, the System Management Homepage 2048-bit key pair will be replaced with the HP Systems Insight Manager 1024-bit key pair.

6. Install OpenSSH:

On the **Welcome to the OpenSSH Services for HP Systems Insight Manager Setup Wizard**, click **Next**.

- a. The **Select Destination Location** window appears. Setup will install OpenSSH into the following folder C:\Program Files\OpenSSH. To change the location, use the **Browse** button. Click **Next**.
- b. The **OpenSSH Service Log On As User** window appears. Enter your account password. The user name and domain fields are prepopulated. Although these fields are prepopulated, you may change these values to specify any user you choose. However, the account credentials you do choose must have local administrator rights (be a member of the local "Administrators" group). Click **Next**.

Note: The **OpenSSH Service Log On As User** window appears only if installing on a Windows XP or Windows 2003 system. If you are installing on a Windows 2000 system, the OpenSSH Service runs as "localsystem" and does not ask for credentials.

- c. The **Ready to Install** window appears. Click **Install** to continue with the installation.
- d. After installing OpenSSH, if prompted, click **No, I will restart the computer later**.
- e. Click **Finish**.

Note: The local security policy will be modified to give you the following rights: log on as a service, create a token object, and replace a process level token. Refer to HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more details.

7. Install WMI Mapper:

On the **Welcome to the Pegasus WMI Mapper v2.1 Setup Wizard**, click **Next**.

- a. The **End-User License Agreement** window appears. After reading the license agreement, click **I accept the terms in the License Agreement**. Click **Next**.
- b. The **Choose Setup Type** window appears. Select the setup type. (The basic requirement for HP SIM is Typical installation. If you select Typical, omit step d.)
- c. Select the default location C:\Program Files\The Open Group\WMI Mapper or change the destination location using **Browse**. Click **OK**. Click **Next**.
- d. The **Ready to Install** window appears. Click **Install** to continue with the installation.
- e. Click **Finish**.

Note: For Windows XP SP2 or Windows 2003 SP1 or later, COM security will be updated to allow remote access and activation by everyone and anonymous users. Refer to HP Systems Insight Manager Read Me at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more details.

8. Install HP Systems Insight Manager:

When the **Welcome to the HP Systems Insight Manager Setup Wizard** appears, click **Next**. The **Service Account Credentials** window appears, with User name, Password, and Domain fields. The fields are pre-populated with the installing account credentials but can be edited if needed.

- a. Provide a valid password and proceed, or provide different account details. This account should have administrative privileges. Click **Next**.

Note: 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.

Note: This user account will be used to run the HP SIM service.

- b. The **Database Configuration** window appears. Specify **SQL Server** as your database server. Enter the requested information appropriately. Defaults are provided where possible.

Note: MSDE is selected by default.

For SQL Server 2000:

If your database is local, then the **Username**, **Domain**, **port (default is 1433)**, and **Database Server name** fields are pre-populated and can be changed if necessary. Provide the valid

password, and click **Next** to proceed. If your database is not local, supply the name of the remote **database server** and valid values for the **domain**, **port**, and **user credentials**, if different from what is already populated. HP SIM creates a database name with the format "Insight_V50_0_XXXXXXXX (timestamp)." For example, "Insight_V50_0_172541227." It then updates the database.props file, which can be found in C:\Program Files\HP\System InsightManager\Config. Click **Next**.

- c. The **Ready to Install** window appears. Click **Install** to install HP Systems Insight Manager. The **Install Progress** window appears.
- d. Click **Finish** when the installation is complete to close the **HP Systems Insight Manager Installer** window.

9. Install the HP ProLiant Essentials Performance Management Pack:

Note: PMP does not support a remote MSDE database.

Note: During the installation of the HP ProLiant Essentials Performance Management Pack, the following warning appears: "Warning: As part of PMP installation the HP SIM service must be stopped and restarted. Click **OK** to stop the service and continue PMP installation or click **Cancel** to abort the installation."

The Welcome to the HP ProLiant Essentials Performance Management Pack Setup Wizard appears. Click **Next**. The **Service Account Credentials** window appears.

- a. Enter your account password. Click **Next**.
- b. The **HP ProLiant Essentials Performance Management Pack Installing** window appears and installation begins. Click **Finish** to exit the HP ProLiant Essentials Performance Management Pack setup.

10. Install HP Version Control Repository Manager:

When the **HP Version Control Repository Manager Setup** window appears, click **Install**.

- a. The **HP Version Control Repository Manager Setup Repository Directory** window appears. Select the directory from which HP Version Control Repository Manager will retrieve support pack information using the **Browse** button. This directory must be manually created later if it does not exist. Click **OK**. Click **Next**.
- b. The **HP Version Control Repository Manager Automatic Update** window appears. Select the **Enable Automatic Update** checkbox to enable automatic downloading of ProLiant Support Packs and components at a specified interval and time.
- c. Click **Finish**. Installation of HP Version Control Repository Manager proceeds and completes.

Note: If the HP Version Control Agent is configured to use the HP Version Control Repository Manager, warning appears: "At least one HP Version Control Agent must be configured to use the HP Version Control Repository Manager." If none are configured, verify the HP Version Control Agent settings to ensure proper operation of the automatic update feature. Click **OK**.

- d. Click **Close**.

11. Install HP ProLiant Essentials Virtualization Management Software (VS):

Note: During the installation of the HP ProLiant Essentials Virtualization Management Software, the following warning appears: "The Virtualization Management Software installation requires HP SIM and database services to be running. During Installation, the HP SIM service will be restarted." Click **OK** to start the HP SIM status check.

- a. On the **Welcome to the HP ProLiant Essentials Virtualization Management Software Setup Wizard**, click **Next** to continue with the installation.
- b. The **Available Components** window appears with the following components to be installed:

- Virtual Machine Management Pack 2.0.1
- Server Migration Pack 2.0.1

Click **Next** to continue.

- c. The **Service Account Credentials** window appears. Enter your account password.

- d. Click **Next**. Installation begins.
- e. The **VMware VirtualCenter Settings** appears.

Select one of the following:

- Configure VMware VirtualCenter Setting Later
- Configure VMware VirtualCenter Setting now

If you select to configure VMWare VirtualCenter Setting now, enter your password.

Click **Next**.

Note: If you decide to configure at a later time, select **Options>Virtualization Management>Security>VMWare VirtualCenter Settings** from the HP SIM menu.

The **Completing the HP Virtualization Management Software Setup Wizard** window appears. Click **Finish** to exit setup.

Note: For Oracle, if you are installing the VS and want to connect to a local or remote Oracle database, enter your password and .jar file location on the Database Configuration screen. The HP ProLiant Essentials Virtualization Management Software must be installed in an empty Oracle database schema. VS database installation may be omitted if the VS database already exists in the specified schema. Click **Yes** to bypass VS database installation and use the current database. Click **No** to specify a different database name.

12. Install HP Systems Insight Manager information:

When all of the HP SIM components have been installed, the **HP Systems Insight Manager Installation Information** window appears. This window has links for the Version Control Installation Guide to help you configure Version Control and the System Management Homepage. Click a link to view the Version Control Installation guide or click **OK**, and the **Custom Install - Status** window appears again. After all components have been installed, they will have an installed status. The HP SIM Installation Information status states, "Success."

13. Click **Finished** to complete the component installation that you selected.
14. The **HP Systems Insight Manager Setup** window appears. Click **Finish** in the Initial Setup HP Systems Insight Manager window, to complete the installation.
15. If any of the components indicated that a reboot is necessary, reboot your system.
16. After upgrading to HP SIM 5.0, sign in to HP SIM, and run the Daily Device Identification task to ensure that all your associations are updated correctly.

To run the daily Identification task:

- a. Select **Tasks & Logs>View All Scheduled Tasks**. The **All Scheduled Tasks** page appears.
- b. Select the **Daily Device Identification** task.
- c. Click **Run Now**.

Upgrading HP SIM 4.x to HP SIM 5.0 - HP-UX

1. Verify that your system meets the minimum requirements.
2. Install the latest required and recommended HP-UX 11i patches. Refer to <http://www.hp.com/products1/unix/java/patches/index.html> for details.

Note: If you are running the 2002 release of HP-UX 11.11 (11i v1), apply the required and recommend patches to save time during the upgrade process. If you do not apply the patches, you could experience extended upgrade times of 2 hours before you can log in to the system after an upgrade. If initconfig.log shows 100% completion and you cannot browse into HP SIM on port 280, then stop and start the HP SIM service by running mxstop and mxstart respectively.

3. Download the software, or locate a copy of the software on a depot server.

To download the software, refer to <http://www.hp.com/go/hpsim>, and select **Download** under HP management software on the upper-left of the screen. The HP SIM **Download** Page appears. Under **HP Systems Insight Manager and related components**, select **HP SIM-HP-UX**, and select **Download latest version of HP SIM-HP-UX** for a full product install.

When installing HP SIM, Java Out-of-Box is required and will be automatically selected for installation. For additional information, refer to

<http://www.hp.com/products1/unix/java/java2/outofbox/index.html>. The kernel parameter values it adjusts are listed in the following table.

Java Out-of-Box Settings

Java Out-of-Box settings	Kernel parameter values
max_thread_proc	3000
maxdsiz	2063835136
maxfiles	2048
maxfiles_lim	2048
maxusers	512
nfile	4097
nkthread	6000
nproc	2048
tcp_conn_request_max	2048

Additionally, HP SIM will adjust the following kernel parameters:

Java Out-of-Box settings	Kernel parameter values
nfile	30000
semms	2048
semgni	1024

When you install HP Systems Insight Manager, the following software dependencies are required: hpSysMgmtDB, JAVA_OOB, and SSH. If you would like HP SIM to manage your CMS you must install WBEM, if it is not already installed. If you downloaded your software from the Web, these dependency packages are included in the depot file. The installation procedure will be described using this depot.

4. Install HP Systems Insight Manager:

```
swinstall -s /directory/depot -x autoreboot=true HPSIM-HP-UX
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot -x autoreboot=true HPSIM-HP-UX
```

Note: When upgrading your HP Systems Insight Manager installation on HP-UX to HP SIM 5.0, the HP-UX upgrade process includes an automatic reboot and can take up to two hours to complete. You can check the `initconfig.log` to determine if the upgrade has completed.

5. After upgrading to HP SIM 5.0, sign in to HP SIM, and run the Daily Device Identification task to ensure that all your associations are updated correctly.

To run the daily Identification task:

- a. Select **Tasks & Logs > View All Scheduled Tasks**. The **All Scheduled Tasks** page appears.
- b. Select the **Daily Device Identification** task.
- c. Click **Run Now**.

6. (Optional) If you plan to run the Mozilla browser on the CMS, verify that Mozilla 1.7.3 or later is installed. To verify which version is installed, open the Mozilla browser and select **Help>About Mozilla**. To browse to HP SIM start the HP SIM graphical user interface (GUI) using Internet Explorer or Mozilla at `http://localhost:280/`.



NOTE The HP Systems Insight Manager First Time Wizard appears when a user with full configuration rights logs in to HP Systems Insight Manager for the first time. The First Time Wizard configures only the basic settings. Other options are available. Refer to the HP Systems Insight Manager Technical

Next steps

Install and configure the required Management Agents on the systems that will be managed by the CMS. Next, complete the initial setup of HP Systems Insight Manager. Initial setup involves adding managed systems, adding users, setting up authorizations, and configuring event handling. Refer to Chapter 12. Initial Setup for details.

WARNING: After upgrading from HP SIM 4.x to HP SIM 5.0 for HP-UX, do not remove the SD bundles HPSIM-Migration or ixPostgreSQL. One of these bundles will be on your system (depending on whether you are upgrading from HP SIM 4.2.0.1.5 or a previous version respectively) in addition to the HP SIM bundle HPSIM-HP-UX. Either bundle will contain the SD product PostgreSQL. The web release of HP SIM 5.0 for HP-UX contains the custom version of the PostgreSQL database, which was packaged as a SD bundle with a name of hpSysMgmtDB, containing the SD product SysMgmtDB. However, this version of the database is only used with new installations of HP SIM. When upgrading from HP SIM 4.x, HP SIM 5.0 will continue to use the PostgreSQL program from the previous release of HP SIM. When upgrading from 5.0, HP SIM will continue to use the previously active database program. The hpSysMgmtDB bundle tag will be removed the SysMgmtDB product is now contained within the HPSIM-HP-UX bundle.



NOTE Serviceguard integration has changed with HP SIM 5.0. If you updated from HP SIM 4.2 with Serviceguard Manager 4.02, you can still launch Serviceguard Manager. To do this, select a cluster member from the Tools>Integrated Consoles menu. To update Serviceguard Manager to 5.0 refer to <http://www.hp.com/go/softwaredepot>. After you updated to 5.0, you can launch Serviceguard Manager by clicking a cluster name.

Upgrading HP SIM 4.x. to HP SIM 5.0 - Linux

1. Extract the .rpm files from the .bin file. Set the permissions to include the right to execute the .bin file by executing the following command:

```
./HPSIM-Linux_C.05.00.01.00.bin --keep --confirm
```

Note: Refer to Step 9 in the "Installing on Linux - Preparing the System" section for information on setting permissions.

2. Respond negatively to the prompt to run scripts for an Automatic install. The extracted files are placed in an mxserver subdirectory.
3. To change the directory to mxserver, execute the following command:

```
cd mxserver
```

4. Install HP SIM using the .rpm files:

```
rpm -Uvh hpsim-C.05.00.00.XXXXXXX.i386.rpm \  
hpsim-pgsql-config-C.05.00.00.XXXXXXX.i386.rpm
```

Note: Both files must be installed concurrently with a single command (no carriage return).

Note: The initialization of the upgrade is done in the background, which takes several minutes. To verify if the upgrade is 100% complete, view the file by executing the following command:

```
cat /var/opt/mx/logs/initconfig.log
```

5. Complete the upgrade by restarting the HP Systems Insight Manager daemons using mxstop and mxstart. HP SIM is now installed and initialized on the CMS. To browse to HP SIM, start the HP SIM graphical user interface (GUI) using Internet Explorer or Mozilla at <http://localhost:280/>.

Refer to Chapter 10. Using the Graphical User Interface for details.

6. After upgrading to HP SIM 5.0, sign in to HP SIM, and run the Daily Device Identification task to ensure that all your associations are updated correctly.

To run the daily Identification task:

- a. Select **Tasks & Logs > View All Scheduled Tasks**. The **All Scheduled Tasks** page appears.
- b. Select the **Daily Device Identification** task.
- c. Click **Run Now**.



NOTE Some tools in the *Monitor Tools* toolbox of previous versions of HP SIM have been removed from HP SIM 5.0. They either provide administrator-type functionality or access to administrator-level files to non-administrator users of HP Systems Insight Manager. If upgrading from a previous version, these tools remain in the Monitor Tools toolbox. You must review the contents of the Monitor Tools toolbox and any other toolboxes you have created, and remove these tools accordingly.

If upgrading from HP Systems Insight Manager 4.2 or later, the list of tools include:

Monitor tools	General tools
type	General Tools
cat	General tools
find	General tools

If upgrading from a version prior to HP Systems Insight Manager 4.2, the list of tools include:

Monitor tools	General tools
type	General tools
cat	General tools
find	General tools
cp	General tools
mv	General tools
rm	General tools
copy	General tools
del	General tools

1. To remove the tools, sign in to HP Systems Insight Manager as full configuration rights user.
2. Select **Options>Security>Users and Authorizations**, and then click the Toolboxes tab.
3. Select the **Monitor Tools toolbox**.
4. Click **Edit**.
5. In the **Toolbox contents** panel, select the tools you want to remove and click the << button.
6. Click **OK** to save.

NOTE After upgrading to HP Systems Insight Manager to ensure that all network devices, racks, and enclosures are properly identified, run Identification. Select Options>Identify Systems. The **Identify Systems** page appears. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

9 Uninstalling HP Systems Insight Manager

Uninstalling HP Systems Insight Manager from a Windows system

From the control panel, use the **Add/Remove Programs** feature in Windows, and complete the following steps to remove HP Systems Insight Manager and its dependencies:

1. Select **HP Systems Insight Manager**, and click **Remove**. If you want to uninstall HP Systems Insight Manager, click **Yes**. Click **Noto** to cancel the uninstall.

Note: Removing HP Systems Insight Manager does not remove its database files. If you plan to reinstall HP Systems Insight Manager, you do not have to rename or remove the old database.

If you clicked **Yes**, the **HP Systems Insight Manager Component Uninstall** window appears. This window lists some of the installed components each with a checkbox. The components listed for uninstall are: **OpenSSH Services for HPSIM 3.7.1p1-1**, **HP Performance Management Pack**, and **HP Virtualization Management Software**.

Note: The dependent components like **HP Performance Management Pack**, and **HP Virtualization Management Software** will be selected by default, and these selections cannot be edited. The **OpenSSH Services for HPSIM 3.7.1p1-1** might not be selected for uninstallation.

2. Click **Next**. Individual confirmation dialog boxes for each of the component selected for uninstall appear. If you want to cancel the uninstallation, click **Cancel**.

Note: The components listed in the **HP Systems Insight Manager Component Uninstall** window can also be uninstalled individually from the **Add/Remove Programs** feature. But **System Management Homepage**, **HP Version Control Repository Manager**, **Pegasus WMI Mapper**, and **MSDE** can be uninstalled only from the **Add/Remove Program** in the Control Panel.

3. The **HP Virtualization Management Software Uninstall** box appears with the following message: "The HP Virtualization Management Software uninstallation requires both HP SIM and database services to be running. During uninstallation, HP SIM services will be restarted. The HP SIM status check is in progress." Click **OK** to uninstall. The HP SIM status check is complete.
4. Click **Yes** to proceed with the HP Virtualization Management Software uninstallation. HP Virtualization Management Software was successfully removed from your computer.
5. After uninstalling the selected components, click **Next** on the **HP Systems Insight Manager Component Uninstall** window to proceed with the HP SIM uninstallation. The HP SIM uninstall progress screen appears. On completion of HP SIM uninstall, a window prompting for system reboot appears. HP recommends reboot the system to complete the uninstall process.

Uninstalling HP Systems Insight Manager from an HP-UX system



CAUTION Removing HP Systems Insight Manager permanently deletes the information in the database unless you back it up before removing the software.

1. Stop the HP Systems Insight Manager daemons:

```
mxstop
```

2. Verify that the daemons are no longer running:

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

If any of the HP Systems Insight Manager daemons are running, note their process IDs (PIDs) in the ps -ef output, and kill them:

```
kill -9 PID
```

where PID is the process ID of the daemon. For example, if the ps -ef | grep mx command displays a line that looks like:

```
root 18582 1 0 Jan 12 ? 00:13:18 /opt/mx/lbin/mxinventory
```

then the command to kill this daemon is:

```
kill -9 18582
```

3. (Optional) Back up the HP Systems Insight Manager database:
`mxrepositorysave -f filename`
where filename is the name of the backup file.
4. Remove the HP Systems Insight Manager software:
`swremove -x enforce_dependencies=false HPSIM-HP-UX`

Uninstalling HP Systems Insight Manager from a Linux system



CAUTION Removing HP Systems Insight Manager permanently deletes the information in the database unless you back it up before removing the software.

1. Stop the HP Systems Insight Manager daemons:
`/opt/mx/bin/mxstop`
2. Verify that the daemons are no longer running:
`ps -ef | grep mx`
If any of the HP Systems Insight Manager daemons are running, record the PID and kill the process:
`kill -9 pid`
where pid is the PID of the daemon. For example,
`kill -9 3456`
3. (Optional) Back up the HP Systems Insight Manager database:
`mxrepositorysave -f directory/filename`
where directory is a unique location for the file outside of the HP Systems Insight Manager directory structure and filename is the name of the back up file.
Note: If you plan to remove the HP Systems Insight Manager directories later in the process, save this backup in a location **outside** of the default product directories.
4. Remove the HP Systems Insight Manager software:
`rpm -qa | grep hpsim | xargs rpm -e`
5. (Optional) If other applications are not using PostgreSQL, you can remove it:
`rpm -qa | grep postgresql | xargs rpm -e`
To remove the PostgreSQL folder:
`rm -rf /var/lib/pgsql`

10 Using the Graphical User Interface

HP Systems Insight Manager provides a browser-based GUI.

Accessing the GUI

The **graphical user interface** (GUI) can be accessed from <http://localhost:280/> with any network client that is running a supported web browser.

▲ Required Web Browsers

- For HP-UX:
 - Mozilla 1.7.3 or laterTo download, refer to <http://software.hp.com>.
- For Linux:
 - Mozilla 1.7.3 or later
- For Windows:
 - Microsoft Internet Explorer 6 with Service Pack 1 or laterRefer to the following note about the required security options.

Note: For all Windows Internet Explorer browsers, you must have the SSL 3.0 or TLS 1.0 browser security options enabled for HP Systems Insight Manager to work properly.

Graphical User Interface Features

This section describes the **graphical user interface** (GUI) features. The following figure is a sample screen shot of the GUI.

The five regions in the GUI include:

1. Banner

The banner provides a link to the **Home** page, a link to **Sign Out** of HP SIM, and it displays the user that is currently signed in.

2. System Status panel

This panel provides uncleared event status, system health status information, and an alarm to notify you of certain events or statuses. The **System Status** panel can be customized for your environment. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign in the top right corner of the panel. To expand the panel, click the plus sign again. If the **System Status** panel is collapsed and an alarm is received, the panel expands to show the alarm.

3. Search panel

The search feature enables you to search for matches by system name and common system attributes. You can also perform an advanced search for matches based on selected criteria. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign in the top right corner of the panel. To expand the panel, click the plus sign again.

4. System and event collections

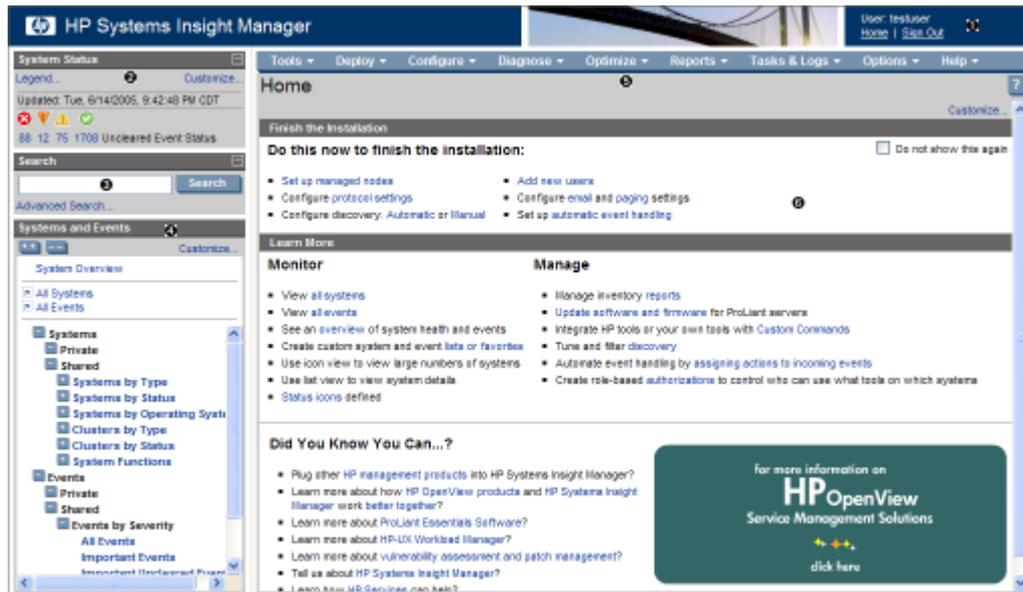
System and event collections enable you to view all known systems and events of a specific subset. Collections can be private, visible only to its creator, or shared, visible to all users. HP SIM ships with default shared collections only. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for information about customizing and creating new collections.

5. Menus

The HP SIM menus provide access to tools, logs, software options, and online help. The **Options** menu is primarily targeted for users who administer the HP SIM software. If you lack authorization to use these tools, you might not be able to access this menu.

6. Workspace

The workspace displays the results of your latest request. It can contain a collection, tool, or report. Some tools launch a separate browser window or X Window terminal instead of displaying in the workspace. This area contains the **Home** page when you sign in to HP SIM. By default, the introductory page appears as the **Home** page.



Default Home Page Features

The HP SIM introductory page is the default **Home** page for the GUI. The introductory page provides information and tips about HP SIM and links to frequently used features. You can customize HP SIM to display a different page as the **Home** page. Refer to "Customizing the Home Page" for information on selecting a different introductory page. The following figure is a sample screen shot of the introductory page.

The four default sections on the introductory page include:

1. Do this now to finish the installation:

This section only appears if the following conditions are met:

- The user has full configuration rights.
- The user has not disabled this section from the **Home Page Settings** page.

2. Monitor

This section provides links to common monitoring tasks, including locating and tracking systems and events. All monitoring tasks can be performed using the features and tools provided in the system and event collection area.

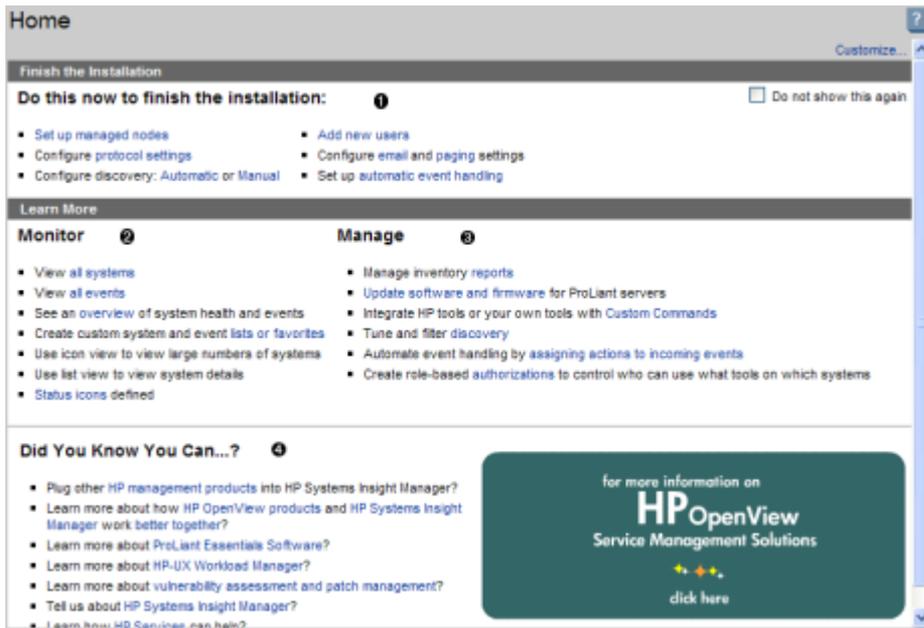
3. Manage

This section provides links to frequently used tools and features available from the menus above the workspace. These links provide access to inventory reports, software and firmware deployment, discovery, event handling, integrating custom commands, and authorizations.

4. Did You Know You Can...?

This section provides useful tips and shortcuts, where you can learn more about HP products, service offerings, and software.

This section appears if you have not disabled it from the **Home Page Settings** page.



Customizing the GUI

Customizing the Home Page

Customize the HP Systems Insight Manager **Home** page to select which page displays when HP Systems Insight Manager is first started and to disable sections in the default introductory page.

To customize the Home page:

1. Click **Home** in the banner to display the **Home** page in the workspace.
2. Click **Customize** in the upper-right corner of the introductory page.

Note: If the **Home** page has been set to something other than the default introductory page, you can access the **Home Page Settings** page by selecting **Options**→**Home Page Settings**.

3. Specify which page you want to use as **Home** page:
 - Introductory page (default)
 - System Overview page
 - Any specific system, cluster, or event collection

Note: The default introductory page is only available when it is set as the **Home** page. If you want to view this page when it is not set as your home page, reselect it as the **Home** page.

4. (Optional) If the introductory page is selected as your home page, customize the content on the page by selecting or deselecting the following options:
 - **Show "Do this now to finish the install" frame.** If selected, this section appears on the **Home** page.
 - **Show the "Did You Know?" image.** If selected, the image in the bottom right corner of the **Home** page appears.

Customizing the System Status Panel

Customize the **System Status** panel to display the following status information:

- Uncleared Event Status

A count that indicates the number of **uncleared event statuses** that are Critical, Major, Minor, and Normal for any given system collection. Each number is a hyperlink to a detailed list of events with that

particular status. By clicking the number, an event collection appears with those particular events and their corresponding systems.

- **Health Status**
A count that indicates the number of systems, in a given system collection, that have a **system health status** that is Critical, Major, Minor, and Normal. Each number is a hyperlink to a detailed list of systems with that particular status. By clicking the number, a system collection appears with those particular systems. Health status is not shown by default but can be configured to appear.
- **Alarm**
An alarm can be customized to appear for specific criteria for any given system collection. The alarm alerts you that a particular criterion has been met by one or more systems in that collection. Because the Status panel is continually updated, the alarm appears until the event is cleared, the system is removed from the collection, or the alarm customization is changed so that it no longer applies. If the **System Status** panel is collapsed, and an alarm occurs, it opens automatically so that the alarm is visible. You can collapse the panel, but it continues to open as long as the alarm is relevant. To have the panel remain collapsed, you must clear the offending event or system status or reconfigure the status display to no longer display alarms.
- **Legend of status icons**
To display a list of status icons, click **Legend** in the **System Status** panel. Legend information appears in a separate window and remains open until you close it.

To customize the System Status panel:

1. Click **Customize** in the upper-right corner of the **System Status** panel. The **Customize System Status** page appears.
2. Select the first **Show summary of**, and select **uncleared event status** or **health status**.
 - a. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - b. Edit the **Label** if desired.
3. Select the second **Show summary of**, and select **uncleared event status** or **health status**.
 - a. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - b. Edit the **Label** if desired.
4. Select to **Show an alarm when any system meets the condition**.
 - a. Select the **Condition**.
 - b. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - c. Edit the **Label** if desired.
5. Click **OK** to save changes.

Note: **Restore Defaults** returns the customization screen to its default condition: only the **uncleared event status** appears in the banner. Health status and the alarm are disabled. All personalized information is removed.

11 Using the Command Line Interface

HP Systems Insight Manager provides a [command line interface \(CLI\)](#) in addition to the [graphical user interface \(GUI\)](#). Many functions available in the GUI are also available through the CLI.

Logging in to the CLI

Access the HP Systems Insight Manager CLI directly on the CMS or from any network client using SSH client software.



NOTE Only administrators have command line access to HP Systems Insight Manager on a Windows CMS. For security reasons, administrators should not modify the access control settings put in place by the installer.

Logging in Directly on the CMS

1. Log in to the CMS using a valid user name and password (`SSH system name`).
HP SIM grants authorizations based on your operating system user login.
2. Open a terminal window or a command prompt window to execute HP SIM commands.

Remotely Using an SSH Client



NOTE The preferred way to log in remotely is using an SSH client. Telnet or rlogin work, but neither provides a secure connection.

1. Open an SSH client application on any network client.
2. Log in to the CMS through the SSH client software, using a valid user name and password.
HP SIM grants authorizations based on your operating system user login.

HP SIM Commands

HP SIM commands are installed in the following locations on the CMS:

- For HP-UX and Linux:
`/opt/mx/bin/`
- For Windows:
`C:\Program Files\HP\System Insight Manager\bin\`



NOTE The Windows path will vary if HP SIM was not installed in the default location.

To view the manpages from the command line on an HP-UX and Linux, use the following manpage sections:

- For HP-UX:
 - Commands manpages are section 1M.
 - Commands that are using XML file manpages are section 4.
- For Linux:
 - Commands that are using XML file manpages are section 4.
- For Windows:
 - Manpages are found in the following folder on Windows systems:
`HP\System Insight Manager\hpwebadmin\webapps\mxhelp\mxportal\en\manpages`

The following table provides a complete list of HP SIM commands. For a detailed explanation of these commands, view the associated manpages from a command prompt or refer to the *HP SIM Technical Reference Guide*.

Command	Functionality	Available manpages
mcompile	Compiles a SNMP Management Information Base (MIB) file into an intermediate format (.CFG) file for importing into HP SIM using the mxmib command.	mcompile(1M)
mxagentconfig	Configures the agent to work with a central management server (CMS).	mxagentconfig(1M)
mxauth	Adds, removes, or lists a toolbox-based authorization and copies authorizations from an existing user to another user.	mxauth(1M) and mxauth(4)
mxcert	Creates a new certificate, imports a signed or trusted certificate, removes a certificate, lists certificates, generates a certificate signing request, notes whether to require trusted certificates, upgrades certificate from HP SIM 4.x, and synchronizes public certificate with the System Management Homepage share directory.	mxcert(1M)
mxcollection	Adds, modifies, removes, and lists collections. Note: mxcollection XML file components and tags are case sensitive.	mxcollections(1M)
mxexec	Executes HP SIM tools, with associated arguments, on specific HP SIM managed systems, verifies the status of running tools, and enables a full configuration rights user to kill or cancel a running task.	mxexec(1M)
mxgetdbinfo	Displays information about the HP Systems Insight Manager database.	mxgetdbinfo(1M)
mxgethostname	Prints the name of the local host in HP SIM.	mxgethostname(1M)
mxglobalprotocolsettings	Used to managed global protocol settings, sets global protocol settings from XML, and lists global protocol settings in detailed format or XML format.	mxglobalprotocolsettings(1M)
mxglobalsettings	Used to manage the global settings in the globalsettings.props file.	mxglobalsettings(1M)
mxinitconfig	Performs initial configuration for the CMS.	mxinitconfig(1M) and mxinitconfig(4)

Command	Functionality	Available manpages
mxlog	Logs an entry to the log file or standard out.	mxinitconfig(1M) and mxinitconfig(4)
mxmib	Adds, deletes, and processes a list of MIBs for HP SIM and lists registered MIBs and traps for a specific registered MIB.	mxmib(1M)
mxngroup	Adds, modifies, removes, or lists system groups from HP SIM, adds and removes systems from system list, and copies systems from one system group to another.	mxngroup(1M) and mxngroup(4)
mxnode	Adds, modifies, identifies, removes, or lists systems in the HP SIM management domain	mxnode(1M) and mxnode(4)
mxnodesecurity	Adds, modifies, or removes security credentials for SNMP and Web-Based Enterprise Management (WBEM) protocols.	mxnodesecurity(1M)
mxoracleconfig	Configures HP SIM to use a newly created Oracle database after validating that HP SIM can connect to the Oracle database using the provided host name for the Oracle server, port number of the Oracle database listener, database name, user name, password, and location of the oracle thin driver .jar file. This command should be executed after the Oracle database administrator creates an instance of an Oracle database set to use the Unicode (AL32UTF8) character set for exclusive use by HP SIM and provides a user name and password to access the database after granting database administrator rights to the user name. The NSL Length setting of BYTE must be used.	mxoracleconfig(1M)
mxpassword	Adds, lists, modifies, or removes passwords stored in HP SIM.	mxpassword(1M)
mxquery	Adds, lists, modifies, or removes lists in HP SIM.	mxquery(1M) and mxquery(4)
mxreport	Lists report types, categories, and generates default and generic reports.	mxreport(1M)
mxstart	Starts daemons or processes used by the CMS.	mxstart(1M)
mxstm	Adds, removes, and lists System Type Manager rules.	mxstm(1M)
mxstop	Stops daemons or processes used by the CMS.	mxstop(1M)
mxtask	Lists, executes, removes, creates, and changes ownership for the HP SIM scheduled tasks.	mxtask(1M) and mxtask(4)
mxtool	Adds, modifies, and removes tools from HP SIM.	mxtool(1M) and mxtool(4)
mxttoolbox	Adds, modifies, or removes toolboxes from the HP SIM system.	mxttoolbox(1M) and mxttoolbox(4)
mxuser	Adds, modifies, removes, or lists users in HP SIM.	mxuser(1M) and mxuser(4)
mxwbemsub	Performs WBEM indication subscription functions on a set of systems, such as adding, deleting, listing, or moving subscriptions on each of the systems passed in as arguments.	mxwbemsub(1M)

12 Initial Setup

The initial setup involves steps for setting up managed systems, configuring discovery, configuring event handling, adding users, and defining authorizations. It assumes that you just completed the installation of your central management server (CMS).

The procedures in this process are common tasks that HP Systems Insight Manager (HP SIM) administrators perform on a regular basis. If you are a new administrator of an existing management domain, it might be useful for you to familiarize yourself with these procedures even though your CMS has already been through the initial setup.



NOTE All the information in this section is also available in the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

NOTE The HP SIM First Time Wizard appears the first time a user with full configuration rights logs into HP Systems Insight Manager. The First Time Wizard configures only the basic settings. There are other options available, refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

Setting Up Managed Systems

Overview

Setting up managed systems involves installing the required Management Agents and configuring the supported protocols to communicate with the HP Systems Insight Manager software. The following steps assume that HP Systems Insight Manager is installed on the CMS and the First Time Wizard has been completed.



NOTE Discovery must be run before setting up managed systems. Configuring Automatic Discovery is part of the First Time Wizard.

To set up managed systems, there are two overall steps:

1. Installing required and optional managed system software:
 - "Installing the ProLiant Support Pack on Windows systems for the first time"
 - "Installing the ProLiant or Integrity Support Pack on a Linux system for the first time"
 - "Installing the required software on an HP-UX system"
2. Configuring the managed system software
 - ▲ "Run the Configure or Repair Agents feature from the CMS"

Installing required and optional managed system software

Managed systems must have the HP VCA installed before you can use the Configure or Repair Agents feature to configure them.

Installing the ProLiant Support Pack on Windows systems for the first time

For Windows systems, install the latest ProLiant Support Pack with the preconfigured components to all managed systems using the HP Systems Insight Manager feature **Initial ProLiant Support Pack Install**.

When you are installing the ProLiant Support Pack for the first time, the Initial ProLiant Support Pack Install process enables you to install a ProLiant Support Pack to a Windows system because you do not have any HP Insight Management Agents, especially HP Version Control Agent, installed. This process also configures the systems to use the trust certificate from the HP Systems Insight Manager and the setting to use the desired HP Version Control Repository Manager. After you have run the Initial ProLiant Support Pack Install tool, then you can use the Install Software and Firmware tool to update systems.

The Install Software and Firmware feature in HP Systems Insight Manager requires that the HP Version Control Repository Manager be installed on servers containing a repository. Installing the HP VCRM is not part of this procedure. For more information regarding installing the HP VCRM, refer to the HP Version Control



NOTE You must have Windows administrator privileges on target systems to install a ProLiant Support Pack

NOTE The Install Software and Firmware and HP VCA features are only available after the Initial ProLiant Support Pack Install process has been run.

NOTE For more information regarding ProLiant Support Packs, refer to the *HP ProLiant Support Pack and Deployment Utilities User Guide* at <http://h18013.www1.hp.com/manage/psp.html>.

To install a ProLiant Support Pack:

1. Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Initial ProLiant Support Pack Install**. The **Initial ProLiant Support Pack Install** page appears.
2. Select the target systems.
3. Click **Next**.
4. From the **Enter Windows login credentials** page:
 - a. In the **User name** field, enter the Windows administrator user name for the target system.
 - b. In the **Password** field, enter the administrator password for the Windows user name entered above.
 - c. In the **Password (Verify)** field, reenter the Windows administrator password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain.

Note: This field can be left blank if the system is not part of a domain.
5. Click **Next**. The **Select a Windows Support Pack** page appears.
6. Under **Select a Version Control Repository**, select a source repository system from which to retrieve the catalog.

The following fields display:

- **Name**. This field displays the name of the system.
- **Status**. This field displays the status of the system.
- **Product Name**. This field displays the name of the product.
- **Trusted?**. This field indicates whether the system trust relationship has been configured. To configure a trust relationship, click **configure**.

Note: This section displays systems that are authorized by the current user name. If the current user is not authorized to view the systems, a message appears, indicating that the user does not have authorization rights on the system.

7. Under **Select a Support Pack to Install**, select a support pack to install. Click the  icon to drill down and view the contents of the Version Control Repository that you selected.

Note: To expand the **System Software Baseline** to display all contents, click the  icon located in the upper-left corner of the **Select a Support Pack to Install** section. Click the  icon to collapse the listings.
8. Select **Install and initialize SSH (Secure Shell)** if you want to install and configure OpenSSH on the target systems. This option is disabled by default.
9. (Optional) Select **Force downgrade or re-install the same version** if you are installing a ProLiant Support Pack that is older than or the same as the version currently installed. This option is disabled by default.
10. (Optional) If you do not want to reboot after the installation, clear the **Reboot systems if necessary after successful install** option, which is selected by default. However, the system must be rebooted for the new ProLiant Support Pack to be available.
11. Click **Next**. The **Configure Support Pack** page appears.

- If you select a ProLiant Support Pack 7.10, **Configure a Support Pack** appears. For example:

Note: If you select a ProLiant Support Pack that is earlier than 7.10, the following example varies.

To configure the 7.10 support pack:

- a. Click **Configure Support Pack** to set up the HP Version Control Agent in the selected Support Pack. The **HP VCA Setup** page appears.
Note: If the HP VCA has already been configured, you can omit this step.
- b. In the **Computer Name** field, enter the name of the system where the HP VCRM is installed.
- c. In the **Administrator Password** field, enter the password associated with the login name specified.
- d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **HP VCA Setup** page.
- e. Click **Next**. The **Download Support Pack** page appears.
- f. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial ProLiant Support Pack Install to run, or click **Run Now** to run the task immediately.

If you select a ProLiant Support Pack 7.20 or later, the following options display.

- Click **Configure System Management Homepage** to set up the Support Pack to establish a trust relationship with System Management Homepage when it is installed on target systems.
Note: If the Support Pack has already been configured, you can omit this step.
Note: the trust relationship is established, click **Last Update** to update the status to trusted.
 To configure the System Management Homepage:
 - a. From the **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page, click **Next**. The **Operating Systems Groups** page appears.
 - b. In the **Group Name** field, enter the name of an operating system group that you want to assign. For example, *vcadmin*.
 - c. In the **Operating Level** field, select the appropriate level for the new group from the dropdown list.
Note: The default **Administrators Groups** always have administrative access.
 - d. Click **Add** to assign the group. The new group appears under the operating system group to which it was assigned.
Note: You can add up to five entries per operating system group.
 - e. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 - f. Select the appropriate settings to include:
 - **Anonymous Access**
 Anonymous Access is disabled by default. Enabling **Anonymous Access** enables a user to access the System Management Homepage (SMH) without logging in. Select this option to allow anonymous access.
Caution: HP does not recommend the use of anonymous access.
 - **Local Access**
 Local Access is disabled by default. Enabling it means you can locally gain access to the System Management Homepage without being challenged for authentication. This means that any user with access to the local console is granted full access if **Administrator** is selected. If **Anonymous** is selected, any local user has access limited to unsecured pages without being challenged for a user name and password. Select this option to allow local access.
Caution: HP does not recommend the use of local access unless your management server software enables it.
 - g. Click **Next**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
 - h. Select the security required by your system. Some situations that require a higher level of security than others. Therefore, you are given the following security options:
 - **Trust by Certificate**
 Sets the System Management Homepage (SMH) to accept configuration changes only from HP Systems Insight Manager servers with trusted certificates. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before allowing access. If you do not want to enable any remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by avoiding importing any certificates.



NOTE HP strongly recommends using this option because it is more secure.

To trust by certificate:

1. Select **Trust by Certificate**, and click **Next**.
2. In the **Certificate Name** field, click **Browse** to select the certificate file. After the certificate file is selected, the certificate data is displayed on the screen.

3. Click **Add**. The certificate appears under **Certificate Files**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- Trust by Name
Sets the System Management Homepage to accept certain configuration changes only from servers with the HP Systems Insight Manager names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure. For example, you might use the trust by name option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP Systems Insight Manager server name submitted.



NOTE HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

The server name option must meet the following criteria:

- Each server name must be less than 64 characters.
- The overall length of the server name list is 1,024 characters.
- The following special characters should not be included as part of the server name: ~ ' ! @ # \$ % ^ & * () + = \ " : ' < > ? , |
- Semicolons are used to separate server names.

To trust by name:

1. Select **Trust by Name**, and click **Next**.
 2. In the **Trusted Server Name** field, enter the server name to be trusted.
 3. Click **Add**. The trusted system name appears under the **Trusted Servers** list. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- Trust All
Sets the System Management Homepage to accept certain configuration changes from any system.



NOTE HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

To trust all servers:

1. Select **Trust All**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
2. Click **Next**. The **IP Binding** page appears.

IP Binding specifies from which IP addresses the System Management Homepage (SMH) accepts requests from and provides control over which nets and subnets requests are processed.

Administrators can configure the System Management Homepage to only bind to addresses specified in the **IP Binding** page. A maximum of five subnet IP addresses and netmasks can be defined.

An IP address on the server is bound if it matches one of the entered IP Binding addresses after the mask is applied.



NOTE The System Management Homepage always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then the System Management Homepage is only available to 127.0.0.1. If IP Binding is not enabled, you bind to all addresses.

- i. Configure IP Binding:
 1. Select **IP Binding**. The **IP Binding** page appears.
 2. Enter the IP address.
 3. Enter the netmask.
 4. Click **Add**. The IP binding configuration is saved and appears under the **IP Binding List**.
 5. Click **Next**. The **IP Restricted Login** page appears.

- j. The IP Restricted Login enables the System Management Homepage (SMH) to restrict log-in access based on the IP address of a system.

You can set address restriction at installation time or by it can be set by administrators from the **IP Restricted Login** page

- If an IP address is excluded, it is excluded even if it is also listed in the included box.
- If there are IP addresses in the inclusion list, then only those IP addresses are allowed log-in access with the exception of *localhost*.
- If no IP addresses are in the inclusion list, then log-in access is allowed to any IP addresses not in the exclusion list.

To include or exclude IP addresses:

1. In the **From** field, enter the IP addresses to include or exclude. You can enter an IP address range to be included or excluded by entering a beginning IP address in the **From** field and an ending IP address in the **To** field.
2. From the **Type** field, select **Include** or **Exclude**.
3. Click **Add** to add the IP address or IP address range to the **Inclusion List** or **Exclusion List** below.
4. Click **Save**. The **HP System Management Homepage Login** page for the System Management Homepage system appears. For more information about System Management Homepage, refer to the System Management Homepage Online Help at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- Click **Configure HP VCA** to set up the HP Version Control Agent in the selected Support Pack.

Note: If the HP VCA has already been configured, you can skip this step.

To configure the HP VCA:

- a. In the **Computer Name** field, enter the name of the system where the HP VCRM is installed.
- b. In the **Login Account** field, enter the login name used to connect to the HP VCRM on the system specified.
- c. In the **Login Password** field, enter the password associated with the login name specified.
- d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **HP VCA Setup** page.
- e. Click **Next**.

12. Back in HP Systems Insight Manager, click **Next** to start the ProLiant Support Pack download. The **Download Support Pack** page appears.
13. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial ProLiant Support Pack Install to run or click **Run Now** to run the task immediately.

Installing the ProLiant or Integrity Support Pack on a Linux system for the first time

- ▲ For Linux systems, use the Linux Deployment Utility to install the latest support pack with the preconfigured components to the local system. For more information regarding installing a support pack using the Linux Deployment Utility, refer to <http://www.hp.com/servers/psp>.

Installing the required software on an HP-UX system

1. Understanding the basic managed system software for HP-UX.

For HP-UX, the following software, shown with minimum recommended versions, is required for essential HP Systems Insight Manager functionality to operate. This software is installed by default as part of the latest HP-UX 11i v2 operating environments, but may need to be installed or updated on HP-UX 11i v1 or older HP-UX 11i v2 systems.

- T1471AA A.04.00 HP-UX Secure Shell
- B8465BA A.02.00.05 HP WBEM Services for HP-UX

This WBEM Services bundle contains basic system instrumentation displayed in the HP SIM Property Pages as well as supporting collection and reporting by HP SIM Inventory functionality. To maximize the value of SIM for properties, inventory and events, the following should also be installed, available for HP-UX 11i v2 servers:

- LVMProvider R11.23 CIM/WBEM Provider for LVM
- WBEMP-LAN-00 B.11.23 LAN Provider for Ethernet/LAN Interfaces
- SysFaultMgmt A.02.00 HP-UX System Fault Management

The following, System Management Homepage for HP-UX, does not currently support the same level of functionality found in Windows and Linux servers. It is currently only required to support the latest version of Partition Manager.

- ▲ SysMgmtWeb A.2.2 HP-UX Web Based System Management User Interfaces

2. Ensuring the managed system software is installed

To see if the minimum required software is installed, login to the remote system and run the following command:

```
$ swlist -l bundle T1471AA B8465BA OpenSSL
```

To see if the optional providers and System Management Homepage are installed, run commands such as:

```
$ swlist -l bundle LVMProvider WBEMP-LAN-00 SysFaultMgmt
```

3. Acquiring and Installing managed system software

The SecureShell, WBEM and OpenSSL bundles are included on the HP-UX Operating Environment and Application Release media, as well as part of the HP Systems Insight Manager HP-UX depot downloaded from <http://www.hp.com/go/softwaredepot>.

For the WBEM providers, several are available from the latest HP-UX Operating Environment and Application Release media. Additionally, the LVMprovider and SysFaultMgmt are available from <http://www.hp.com/go/softwaredepot> by searching for the keyword *provider*.

Make sure that the OnlineDiag bundle is installed on your computer.

To verify that the OnlineDiag bundle is installed, enter the following command:

```
swlist | grep OnlineDiag
```

The OnlineDiag bundle is installed on the operating environments, so if you have a recent version of the operating environment, this should already be installed. However, if it is not installed, the OnlineDiagnostic bundle is available from <http://www.hp.com/go/softwaredepot> by searching for the keyword *B6191AAE*.

After the depots containing the providers have been acquired, they can be installed from the managed system using commands such as:

```
$ swinstall -s <depot_location> OpenSSL
```

Note:B8465BA depends on OpenSSL, so this must be installed first.

```
$ swinstall -s <depot_location> T1477AA
$ swinstall -s <depot_location> B8465BA
$ swinstall -s <depot_location> LVMPProvider WBEMP-LAN-00 SysFaultMgmt
```

4. Configuring Serviceguard provider:

A WBEM provider for Serviceguard can be optionally installed on HP Serviceguard clusters. This provider helps HP Systems Insight Manager create associations in its system lists between clusters and their members, as well as showing HP Serviceguard cluster status.

When using the First Time Wizard from HP Systems Insight Manager, the root user or a non-root user was specified for the WBEM default user. Alternatively a user may have been specifically set for this system.

To access the Serviceguard provider from HP Systems Insight Manager if a non-root user is the WBEM user, you must configure Serviceguard to allow that non-root user Serviceguard administrative access.

Configuring the Managed System Software

The HP Systems Insight Manager Configure or Repair Agents feature is a quick and easy way to configure managed systems, however it is possible to manually configure Linux and HP-UX systems.

Run the Configure or Repair Agents feature from the CMS

To run Configure or Repair Agents remotely against multiple systems simultaneously, you must have authorizations to run the Configure or Repair Agents tool.

You must have full CMS configuration privileges to modify the HP Systems Insight Manager community strings in the node security file. In addition, you must have administrator privileges for Windows systems or root privileges for Linux and HP-UX on the target systems to configure or repair the agent settings.

Note: It is recommended that you use like operating system to configure a managed system. For example, use a Linux-based CMS to run Configure or Repair Agents against Linux managed systems and HP-UX CMS to run Configure or Repair Agents against HP-UX managed systems. Windows systems can only be configured from a Windows CMS.

To configure agents remotely:

1. Select **Configure**→**Configure or Repair Agents** from the menu.

Note: The **Verify Target Systems** page appears if the targets are selected before selecting a tool.

2. To add targets, select a group from the dropdown list. The contents of the selected group appear and can be selected as targets or to select the collection itself, select **Select Name of Collection itself**.
3. Click **Apply**.The targets appear in the **Verify Target Systems** section.

Note: If the targets selected are not compatible with the tool, the **Tool Launch OK?** column provides a brief explanation for the problem. To remove a target, select the target and then click **Remove Targets**.

4. Select one of the following options:

- Click **Add Targets** to add more targets to the **Target System List**.
- To remove a target, select the target and then click **Run Targets**.
- Click **Next** to specify tool parameters and to schedule the task.

5. From the **Enter login credentials** page:

- a. In the **User name** field, enter the system administrator user name for the target systems.
- b. In the **Password** field, enter the system administrator password for the user name previously entered.
- c. In the **Password (Verify)** field, reenter the system administrator password exactly as it was entered in the **Password** field.
- d. For Windows managed systems only, in the **Domain** field, enter the Windows domain.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** or **root** credentials.

6. Click **Next**. Click **Prev** to return to the previous page. The **Configure or Repair Settings** page appears. The following options are available:
 - **Configure SNMP.** Select this option to configure SNMP settings.

If this option is selected, the following steps must be considered:

 1. Select **Set read community string**.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you may deselect this option. HP-UX allows read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed nodes do not always allow SNMP communication between themselves and a remote host. This setting is modified to allow the instance of the HP Systems Insight Manager system to communicate SNMP with these target systems.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over thirty characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP Systems Insight Manager over the network.
 2. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This allows the target systems to send SNMP traps to this instance of HP Systems Insight Manager.
 - **Trust relationship: Set to "Trust by Certificate".** Select this option to require systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP Systems Insight Manager system certificate to the target system's trusted certificate directory. This enables HP Systems Insight Manager users to connect to the System Management Homepage using the certificate for authentication.

Note: If you experience problems later setting the trust status to Linux, refer to the HP Systems Insight Manager Online Help **Troubleshooting** help file for assistance.
 - **Set administrator password for Insight Management Agents version 7.1 or earlier.** Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Deselect this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you can deselect this option.

If this option is selected, the following steps must be configured:

 1. In the **Password** field, enter the new administrator password.
 2. In the **Confirm Password** field, re-enter the new administrator password exactly as you entered it previously.
 - **Configure secure shell (SSH) access.**

If this option is selected, you must select one of the following options:

 - **Host based authentication for SSH** - For more information regarding SSH, refer to Secure Shell (SSH) in HP Systems Insight Manager white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
 - **Each user has to be authenticated on the managed system**

Note: If the selected systems include Linux or HP-UX systems, and options for Configure SNMP settings, Trust relationships and administrator password for HP Insight Management Agent 7.1 or earlier have been selected, then SSH authentication should be selected now unless already configured earlier.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** tool under **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install Open SSH**.

- **Create subscriptions for WBEM events.**

Note: This option is only applicable to Linux and HP-UX systems. If this option is selected, the target system is configured to send WBEM indications or events to HP Systems Insight Manager.

Note: Subscriptions for WBEM events can be created only if WBEM event providers are installed and running on the managed systems.

7. Click **Run Now** or you can click **Schedule** to run this task at a later time. Click **Prev** to return to the previous page. The **Task Results** page appears.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The information is used to display the information on the stdout tab. The results indicate whether the repair attempt was successful.

Note: Repair of SNMP settings, Trust relationships and administrator password for Insight Management Agents 7.1 or earlier on Linux systems is executed by a separate task, which can be viewed in the tasks log menu selection. Repair of SNMP settings, Trust relationships on HP-UX systems is executed by a separate task, which can be viewed in the tasks log menu selection. If Linux and HP-UX systems are selected, there are two Task IDs, one for Linux and one for HP-UX systems.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout Tab.** This tab displays the output text information.
- **The stderr Tab.** This tab displays information if the executable experienced an error.
- **Files Copied Tab.** This tab displays what files are in the process of being copied or have been copied to the target system.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

1. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.

2. Select which report to print.

3. Click **OK** to print the report, or click **Cancel** to return to the **View Task Results** page.

8. If Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Setting Up Managed Systems Manually

Using HP Systems Insight Manager's Configure or Repair Agents is the easiest way to configure managed systems. However, the steps to manually configure Linux and HP-UX managed systems are included in the event manual configuration is necessary.

The following sections detail how to configure managed systems on:

- "Setting Up HP-UX Managed Systems Manually"
- "Setting Up Linux Managed Systems Manually"

Setting Up HP-UX Managed Systems Manually

You can use the HP Systems Insight Manager Configure or Repair Agents tool to configure HP-UX managed systems simultaneously or you can configure each managed system manually.

Use these general steps to assist you with configuring an HP-UX system manually:

1. Install SSH (bundle T1471AA) if not previously installed.
2. Install WBEM (bundle B8465BA) if not previously installed.
3. (Optional) Configure SNMP to send traps to the CMS.
4. (Optional) Configure DMI on HP-UX 11.11 systems (this step is not needed if WBEM installed).

On the CMS:

5. Configure the SSH Keys for this system.
6. Configure the default WBEM user name and password if not previously done.



NOTE SSH and WBEM are installed on HP-UX 11.23 systems by default. For 11.11 systems, check if installed with this command:

```
swlist B8465BA T1471AA
```

7. Subscribe to WBEM Indications/Events

On each managed system:

1. Install SSH on the managed system if not previously installed.

```
swinstall -s /directory/depot T1471AA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot T1471AA
```

2. Install WBEM on the managed system if not previously installed.

```
swinstall -s /directory/depot B8465BA
```

where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot B8465BA
```

3. Configure SNMP to send traps to the CMS:

- a. Add the full hostname or IP address of the CMS as a trapdest in the following file:

```
/etc/SnmpAgent.d/snmpd.conf
```

```
trap-dest: hostname_or_ip_address
```

- b. Stop the SNMP Master agent and all subagents with the command:

```
/sbin/init.d/SnmpMaster stop
```

- c. Restart the SNMP Master agent and all subagents with the command:

```
/usr/sbin/snmpd
```

4. Configure DMI on the managed system by adding the DNS host name of the CMS.



NOTE DMI only needs to be configured for HP-UX 11.11 and only if WBEM is not installed.

- a. Stop the DMI daemon on the managed system:

```
/sbin/init.d/Dmisp stop
```

- b. Edit `/var/dmi/dmiMachines` by adding the host name of the CMS to the end of this file. Save the file.

- c. Start the DMI daemon:

```
/sbin/init.d/Dmisp start
```

5. On the CMS, copy the SSH-generated public key from the CMS to the managed system using the `mxagentconfig`:

Use one of the following commands:

- `mxagentconfig -a -n <hostname> -u root -f <file_with_root_password>`
or
- `mxagentconfig -a -n <hostname> -u root -p <root_password>`

Note: Using the `-p` option exposes the password through `ps` output, so use of the `-f` option (with a file only readable by root, and containing only the managed system root password) is highly recommended when using `mxagentconfig -a`. If the `-p` option is used, enclose the password in single quotes if the password has any special characters, such as `&` or `$`. For more information and options, see the `mxagentconfig` manpage with `man mxagentconfig`.

6. Log into the HP Systems Insight Manager GUI. For assistance with this, refer to . Chapter 10. Using the [Graphical User Interface](#) Using the GUI, add the default WBEM user name and password to the **Global Protocol Settings** page.

Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system.

Note: This step can be performed once for all the managed systems you are setting up.

- a. Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
- b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name, password, and confirmation password.
- c. Click **OK**.



NOTE An account for at least one of the WBEM user name and password combinations must exist on each managed system. If the user in the Global Protocol Settings does not exist on the managed node you can set per-system WBEM user names and passwords from the **System Protocol Settings** page.

7. Using the GUI, add the default WBEM user name and password to the **Global Protocol Settings** page.

Note: An account for at least one of the WBEM user name and password combinations must exist on the CMS.

- a. Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
- b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected and add the default WBEM user name and password.
- c. Click **OK**.

8. To subscribe to WBEM Indications/Events:

Note: For more information about OnlineDiagnostic, go to WBEM Subscriptions in HP Systems Insight Manager white paper at

<http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- a. From the managed system, make sure WBEM is already installed.

Note: Subscribing to WBEM Indications/Events on managed systems is optional.

- b. Verify that **SysFaultMgmt** provider is installed:

```
cimprovider -ls
```

You should see **EMSWrapperProviderModule**

From the CMS:

1. Verify that WBEM has root access:

```
mxnodesecurity -l -p wbem -n <systemname>
```

To subscribe to WBEM Events, you must have **root** access. If the Global Protocol Setting does not match the managed system or does not contain **root** access, the subscription for WBEM Indications fails. You can verify what access WBEM has by running the following command line:

```
mxnodesecurity -l -p wbem -n <systemname>
```

If the managed system does not have **root** access, you can change the individual system.

Note: You can use the Configure or Repair Agents tool to perform this step without permanently recording a **root** passwd.

To change the individual system:

- a. **Tools**→**System Information**→**System Page**.
 - b. From the **System Page**, select **Tools & Settings**→**System Protocol Settings**.
2. From the CMS, run the WBEM Indications/Events command line:

```
mxwbemsub -l -n <systemname>
```

Setting Up Linux Managed Systems Manually

You can use the HP Systems Insight Manager Configure or Repair Agents tool to configure Linux managed systems simultaneously or you can configure each managed system manually.

To manually configure Linux managed systems, perform the following on each managed system:

1. Install and configure SSH.
 - a. Verify that SSH is installed on the managed system:

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

If it is not installed, refer to your Linux provider for information on installing SSH.
 - b. On the CMS, copy the SSH generated public key from the CMS to the managed system and place it in the authorized keys file of the execute-as user (root or administrator).

Important: On a non-English CMS, ensure that an administrator account (spelled exactly as follows, administrator) exists on the CMS, and that `mxagentconfig` has been run on the CMS for the created administrator account.

 - i. Launch the **Manage SSH Keys** dialog box from the CMS command prompt:

```
mxagentconfig -a -n hostname -u username -p Password
```
 - ii. Click **Connect**.
2. Configure the system to send SNMP traps.

Note: These steps might vary slightly, depending on your version of Linux. Refer to your Linux provider for details if these file paths and file names do not exist on your system.

 - a. Verify that SNMP is installed:

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

If it is not installed, refer to your Linux provider for information on installing SNMP.
 - b. If you have not installed the HP Server Management Drivers and Agents from the ProLiant Support Pack for Linux, omit this step. Otherwise, stop the HP Server and Management Drivers and Agents daemons on the platform where you are installing HP Systems Insight Manager using the following command:

```
/etc/init.d/hpsasm stop
```

Note: If the HP Server Management Drivers and Agents daemon is not installed, omit this step and step F.
 - c. Stop the SNMP daemon:

```
/etc/init.d/snmpd stop
```
 - d. Edit the `snmpd.conf` file using any text editor.

For Red Hat Linux run the following command for opening this file in the vi editor: `vi /etc/snmp/snmpd.conf`

For SuSE SLES 8 run the following command for opening this file in the vi editor: `vi /usr/share/snmp/snmpd.conf`

 - i. Remove the comment symbol (`#`) from the trapsink line, and add the IP address of the CMS:

```
trapsink IPaddress
```

where `IPaddress` is the IP address of the CMS.
 - ii. Add the CMS to the read only community by adding the line:

```
rocommunity CommunityName IPaddress
```

where `CommunityName` is the SNMP community string used by the CMS and `IPaddress` is the IP address of the CMS.
 - iii. Save the changes to the file. To save and close this file using the vi editor, press the Esc key, enter `:wq!`, and press the Enter key.

- e. Start the SNMP daemon:


```
/etc/init.d/snmpd start
```
- f. Start the HP Server Management Drivers and Agents daemon if it is installed on your system:


```
/etc/init.d/hpsasm start
```
3. Install the Linux ProLiant Support Pack. To download this software and access installation information, go to <http://www.hp.com/support/files>.
4. Log into the HP Systems Insight Manager GUI. For assistance with this, refer to . Chapter 10. Using the Graphical User Interface .
5. Add the default WBEM user name and password to the **Global Protocol Settings** page in the HP Systems Insight Manager GUI.

Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system.

Note: This step can be performed once for all the managed systems you are setting up.

 - a. Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
 - b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name, password, and confirmation password.
 - c. Click **OK**.
6. Add the default WBEM user name and password to the **Global Protocol Settings** page in the HP Systems Insight Manager GUI.

Note: An account for at least one of the WBEM user name and password combinations must exist on the CMS.

 - a. Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
 - b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected and add the default WBEM user name, password, and confirmation password.
 - c. Click **OK**.

Examples

Setting up Windows managed systems

The following example describes how to setup remote Windows systems from a Windows CMS.

To configure remote Windows systems from a Windows CMS:

1. Login to the HP Systems Insight Manager on the Windows CMS with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already.
3. Run discovery if you have not already.
4. Preconfigure the System Management Homepage and version control components.
5. Install the ProLiant or Integrity Support Packs on remote systems:
 - ▲ Run the Initial ProLiant Support Pack Install to install the latest ProLiant Support Pack on Windows systems.
6. Run the Configure or Repair Agents feature. For more information, refer to "Run the Configure or Repair Agents feature from the CMS" .

Setting up remote Linux systems from a Linux CMS

The following example describes how to setup remote Linux systems from a Linux CMS.

To configure remote Linux systems from a Linux CMS:

1. Login to the HP Systems Insight Manager on the Linux CMS with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already.
3. Run discovery if you have not already.
4. Preconfigure the System Management Homepage and version control components.

5. Install the ProLiant or Integrity Support Packs on remote systems:
 - ▲ Run the Linux Deployment Utility to install the latest Integrity Support Pack on Linux and HP-UX systems. For more information, download the HP ProLiant Support Pack and Deployment Utilities User Guide at <http://www.hp.com/servers/psp>.
6. Run the Configure or Repair Agents feature. For more information, refer to "Run the Configure or Repair Agents feature from the CMS" .

Setting up remote HP-UX systems from an HP-UX CMS

The following example describes how to set up remote HP-UX systems from an HP-UX CMS.

To configure remote HP-UX systems from an HP-UX CMS:

1. Login to the HP Systems Insight Manager on the HP-UX with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already.
3. Run discovery if you have not already.
4. Ensure the managed system software is installed. For more information, refer to "Installing the required software on an HP-UX system" .
5. Run the Configure or Repair Agents feature to configure the managed system. For more information, refer to "Run the Configure or Repair Agents feature from the CMS" .

Configuring Protocol Settings

Configuring the protocol settings defines what systems are added to HP SIM using discovery.

To configure the protocol settings:

1. Click **Options**→**Protocol Settings**→**Global Protocol Settings**. The **Global Protocol Settings** page appears.
2. In the **Default ping settings** section, select **Use the ICMP protocol for system reachability (ping) check** or **Use the TCP protocol for system reachability (ping) check port number 80**. The **Use the ICMP protocol for system reachability (ping) check** is the default and recommended setting.

Select **Use the TCP protocol for system reachable (ping) check. port number 80** if your company has disabled ICMP on the corporate network or the corporate policy mandates system firewall software to filter out ICMP requests. For example, Windows XP has this feature built in and can result in systems not being automatically discovered. This option enables you to run HP Systems Insight Manager (HP SIM) and ping all available systems.

Note: This option only applies to IP-based systems and is available for global, system-wide settings that are used when managing all systems in HP SIM. It is used by automatic discovery, hardware status polling, the ping tool, and any other tool that must verify system availability. This option is not available on a single-system basis.

Note: If you select **Use the TCP protocol for system reachable (ping) check. port number 80**, even though HP SIM attempts a connection request to the current system, that system does not need any additional software running on it for this option to work. For example, HP does not require that a web server be running on port 80. Some networking systems might not respond to the TCP request, which is typically seen in low end networking equipment. Manual additions can be made if it is necessary. However, this system displays as Critical if hardware status polling is run.

3. Also in the **Default ping settings** section, set the **Default timeout** and the **Default retries**. If some systems are managed over a WAN or satellite link, use a larger timeout (for example, 5 seconds) with at least one retry. For a LAN, a shorter time-out can be used. This can be configured on a single-system basis.
4. In the **Default WBEM settings** section, select **Enable WBEM** to allow Web-Based Enterprise Management (WBEM) requests to be sent. Enabled is the default setting. Enter as many default user names and passwords as needed. If your network includes storage systems, enter the user name and password of each SMI CIMOM in this section. The identification process attempts each of these user name and password pairs until a successful response is obtained. Future WBEM requests to that system use the user name and password that succeeded. For Windows-based systems, the user name should include the domain name, for example, *domainname\username*.

Note: Order the name and password pairs such that root and administrator passwords are listed first and user and guest passwords are listed second. This order minimizes the search time.

5. In the **Default HTTP settings** section, select **Enable HTTP and HTTPS** if it is necessary to allow web-based agents and other HTTP port scans to be identified. HP recommends leaving this option enabled for proper management and discovery of systems.
6. In the **Default SNMP settings** section, select **Enable SNMP**, which is the system default, and set the **Default timeout** and **Default retries**. If some systems are managed over a WAN or satellite link, use a larger timeout (for example, 5 seconds) with at least one retry. For a LAN, a shorter timeout can be used. These settings can also be configured on a single-system basis.
7. Enter the **Default write community string**. This value is case-sensitive. Only a few tools need this option set. Community strings are case-sensitive.
8. Enter the **Read community string**. This value is case-sensitive. Enter as many as needed. The identification process attempts communication to the system, using each of these communities in succession until a successful response is obtained. Future SNMP requests then use the community string that provided a successful response.
9. In the **Default DMI settings** section, select **Enable DMI**, which is the default setting, to enable [Desktop Management Interface \(DMI\)](#) identification to run on systems. DMI is used to manage some older desktops, HP-UX servers, and some third-party servers. If you do not need to manage these kinds of systems, DMI can be disabled to improve discovery performance.

Note: DMI is not currently supported on Linux systems and is not shown in the user interface.

Note: If DMI is disabled and some systems no longer have a correct system type or product name, re-enable DMI.

Note: DMI identification is only supported on Windows and HP-UX-based [central management server \(CMS\)](#) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.
10. Click **OK** to accept the settings.

Configuring and Executing Discovery

Discovery is the process that HP SIM uses to find and identify the systems on your network to populate the database with that information. A system must first be discovered in order to collect data and track system status. There are two basic ways to discover new systems:

- **Automatic discovery.**
The process that HP SIM uses to find and [identify the systems](#) on your network to populate the database with that information. A [system](#) must first be discovered to collect data and track system status.
- **Manual discovery.**
The process that enables you to bypass a full automatic discovery and add single and multiple systems to the database, create or import the HP SIM database Hosts file, and create or import a generic Hosts file.

Configuring and Executing Automatic Discovery

1. Click **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Configure general settings**. The **General Settings** section appears.
3. Select **Automatically discover a system when an event is received from it**. This option allows systems to be discovered when a trap or some other supported event is received by [HP Systems Insight Manager \(HP SIM\)](#). It uses the discovery filters and IP address exclusion ranges for additional filtering of these events.
4. Select **Automatically discover a server blade when its [Integrated Lights Out management processor](#) is identified**. This option adds servers that were indirectly discovered through its management processor. When these servers are discovered, they are listed with a Disabled state on the system table view page and the only information displayed is the system serial number and the association to the iLO and the enclosure.

5. In the **Ping exclusion ranges, templates and/or hosts files** field, specify the IP addresses, templates, or hosts files containing IP addresses to exclude from the automatic discovery process. This applies to both range pinging and event based auto-discovery.
Important: When discovering clusters, the ping inclusion range must include the IP addresses of the cluster and the cluster members.
6. Select **Enable discovery filters**.
7. In the **Discover the following system types:** section, select the type of systems to be discovered.
Important: When discovering clusters, you must include the Server system type, or so that the cluster members are not filtered out.
Note: This is only available when you select **Enable discovery filters**.
8. In the **Limit discovery to systems that meet the following criteria** section, select from the following:
 - **Any system that matches the above filter**
 - **All manageable systems (WBEM, SNMP, DMI, WMI or HTTP support)**
 - **Manageable systems with HP agents only****Note:** This is only available when you select **Enable discovery filters**.
9. Click **OK** to save settings, or click **Cancel** to close the **General Settings** section without saving changes. If you click **OK** when discovery filters are enabled but have not selected any system types, the following error message appears:
You must make at least one system type selection when enabling filters.

Configuring and Executing Manual Discovery

1. Click **Options**→**Discovery** and select the **Manual** tab. The **System Information** section appears.
2. Select the **System name** radio button and enter the system name.
or
Select the **IP address** radio button and enter the IP address.
3. Click **Add System** to add the system to the database, or click **More Settings** to enter additional information.

System Information

Required field *

Enter either the system's name or IP address: *

System name:

IP address:

Specify additional system properties to use only if identification fails on this system

System type:

System subtype 1:

System subtype 2:

System subtype 3:

System subtype 4:

System subtype 5:

System subtype 6:

System subtype 7:

System subtype 8:

Product model:

The screenshot displays the configuration page for a system in HP SIM. It is divided into two main sections: **WBEM Settings** and **SNMP Settings**.

WBEM Settings:

- User name:** Two radio buttons are present: "Use default (currently:)" (selected) and "Use custom" followed by an empty text input field.
- Password:** Two radio buttons are present: "Use default" (selected) and "Use custom" followed by two empty text input fields labeled "Verify Password".

SNMP Settings:

- Timeout (in seconds):** Two radio buttons: "Use default (currently: 5)" (selected) and "Use custom" followed by an empty text input field.
- Retries:** Two radio buttons: "Use default (currently: 1)" (selected) and "Use custom" followed by an empty text input field.
- Read-only community string:** Two radio buttons: "Use default (currently: public)" (selected) and "Use custom" followed by an empty text input field.
- Write community string:** Two radio buttons: "Use default (currently: private)" (selected) and "Use custom" followed by an empty text input field.

At the bottom right of the form, there are two buttons: "Fewer Settings..." and "Add System".

- **Specify additional system properties to use only if Identification fails on this system.** Includes:
 - **System type**
 - **System subtype**
There are eight available System subtype fields that can later be changed on **System Attributes** page.
 - **Product model**
 - **WBEM Settings.** Includes:
 - **User name**
 - **Password**
 - **SNMP Settings.** Includes:
 - **Timeout (in seconds)**
 - **Retries**
 - **Read-only community string**
 - **Write community string**
4. If you clicked **More Settings**, click **Add System** to add the system immediately or click **Fewer Settings** to return to the previous brief display. If you clicked **Fewer Settings**, click **Add System** to add the system to the database.

Adding Users

Create a new [user](#) account to sign into [HP Systems Insight Manager \(HP SIM\)](#). The account must be valid on the operating system (includes Active Directory on Windows) on the [central management server \(CMS\)](#), and will be authenticated by the CMS. You must know the operating system user account name of the user you are adding, but you do not need to know the password.

To create a new user:

1. Click **Options**→**Security**→**Users and Authorizations**→**Users**, and click **New**. The **New User** section appears.
2. In the **Login name (on central management server)** field, enter the operating system login account name to be used to sign into HP SIM. This field is required.

Note: The user cannot sign into HP SIM if the account is not a valid login. The account is not validated until the user tries to sign into HP SIM.

3. In the **Domain (Windows domain for login name)** field, enter the Windows domain name for the login name if the CMS is running a Windows operating system. If left blank, the system name of the CMS is used as the domain.
4. In the **Full name** field, enter the user's full name.
5. In the **Phone number** field, enter the user's phone number.
6. In the **E-mail address** field, enter the user's e-mail address.
7. In the **Copy all authorizations of this user or [template]** field, select a template or login that already has the predefined authorizations that you want to assign to the login account you are creating.
8. In the **Central management server configuration rights** section, select the level of authority to assign to the new user from the following options:
 - **full, allowed to modify all central management server settings.** Allows the user total control of the database. Users can run discovery of systems and data collection define users and authorizations; set Cluster Monitor configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.
 - **limited, allowed to create/modify/delete all reports and their own tools.** Allows the user to create new reports, edit any reports, and delete any reports (including the predefined reports).
 - **none, no configuration of central management server allowed.** Allows the user to view and run predefined reports on the CMS and all managed systems. However, the user has no configuration rights on the CMS or on the managed systems.
9. Under the **Login IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems that you want this user to be able to use as a client browsing into this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted form, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in dotted form. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Important: If browsing from the central management server, ensure all IP addresses of the CMS are properly included. If browsing to `localhost` ensure the loopback address 127.0.0.1 is also included.
10. In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from this user as clients browsing into this CMS. Use the same format in the previous step for **Inclusion ranges**.

Note: Be sure to verify that your inclusion and exclusion ranges do not overlap.

Note: Steps 11 through 15 are only for a CMS running Windows.
11. Under the **Pager Information** section, in the **Phone number** field, enter the pager phone number of the user associated with this user account if you are using a Windows operating system. If the **Phone number** field is left blank, the paging information is not saved.
12. In the **PIN number** field, enter the PIN number associated with the pager phone number.
13. In the **Message length** field, select how many characters can be accepted in the paging message from the dropdown list.
14. In the **Baud rate** field, select the appropriate baud rate for the pager from the dropdown list.
15. In the **Data format** field, select the appropriate data format for the pager from the dropdown list.
16. Click **OK** to save and close the **New User** section. You can click **Apply** to save and keep the **New User** section open, or click **Cancel** to cancel the creation of this user.

The new user account is created.

User groups must exist in the operating system. For Windows, this includes Active Directory. Members of the user groups in the operating system can sign into [HP Systems Insight Manager \(HP SIM\)](#) and will inherit the group's attributes for configuration rights and login IP address restrictions, as well as the group's authorizations. When a group's configuration rights, login IP address restrictions, or authorizations are changed, this change is immediately reflected in all current members of the group.

To create a new user group:

1. Click **Options**→**Security**→**Users and Authorizations**→**Users**, and click **New Group**. The **New User Group** section appears.
2. In the **Group name (on central management server)** field, enter the operating system group name to be used for logging into HP SIM. This field is required.
3. In the **Domain (Windows domain for login name)** field, enter the Windows domain name for the group if the central management server (CMS) is running a Windows operating system.
4. In the **Full name** field, enter the full name for the group. This is displayed in the table on the **Users** tab.
5. In **Copy all authorizations of this user or [template]** dropdown list, select a template or login that already has the predefined authorizations that you want to assign to the group you are creating.
6. In the **Central management server configuration rights** section, select the level of authority to assign to the new user group from the following options. Users that login into HP SIM as members of this group inherit these configuration rights.
 - **full, allowed to modify all central management server settings.** Allows the user total control of the database. Users can run discovery of systems and data collection define users and authorizations; set Cluster Monitor configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.
 - **limited, allowed to create/modify/delete all reports and their own tools.** Allows the user to create new reports, edit any reports, and delete any reports (including the predefined reports).
 - **none, no configuration of central management server allowed.** Allows the user to view and run predefined reports on the CMS and all managed systems. However, the user has no configuration rights on the CMS or on the managed systems.
7. Under the **Login IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems that you want members of this user group to be able to use as a client browsing into this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted form, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in dotted form. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Important: If browsing from the central management server, ensure all IP addresses of the CMS are properly included. If browsing to `localhost` ensure the loopback address 127.0.0.1 is also included.
8. In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from members of this user groups as clients browsing into this CMS. Use the same format in the previous step for **Inclusion ranges**.

Note: Be sure to verify that your inclusion and exclusion ranges do not overlap.
9. Click **OK** to save and close the **New User Group** section. You can click **Apply** to save and keep the **New User Group** section open, or click **Cancel** to cancel to close the **New User Group** section without saving the new group.

Configuring Email Settings

Configuring e-mail settings enables users to receive e-mail notification of certain events.

To configure e-mail settings:

1. Click **Options**→**Events**→**Automatic Event Handling**→**E-mail Settings**. The **E-mail Settings** page appears.
2. Specify the SMTP host in the **SMTP Host** box.
3. Specify the e-mail address that the management server uses when sending e-mail notifications in the **Sender's Email Address** box.
4. To authenticate your SMTP server, select **Server Requires Authentication**.
5. Specify the account name in **Account name** box.
6. Specify the password in the **Password** box.
7. Click **OK** to save changes.

Configuring Paging Settings

Configuring paging settings enables users to receive pages to notify them of certain events.

To configure paging settings:

1. Click **Options**→**Events**→**Automatic Event Handling**→**Modem Settings**. The **Modem Settings** page appears.
2. From the **COM port** field, select the appropriate COM port. Refer to your modem documentation for details.
3. Click **OK** to save the setting.

Setting Up Automatic Event Handling

Automatic event handling enables you to define an action that HP SIM performs when an **event** is received. Automatic event handling can be set up to use the e-mail and paging settings that you specified in the previous sections.

To set up automatic event handling with **events** and system attributes that you specify now:

1. Click **Options**→**Events**→**Automatic Event Handling**→**New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with event and system attributes that I will specify**.
3. There are six steps to complete to define a new task. Under **Step 1 of 5, Select name** is selected. Enter a name for the task in the **Task name** field.
4. Click **Next**. The step 2, **Select existing event collection** page appears.
5. Select the event search criteria for defining the task:

- List criteria
- Comparison option
- Value for the criteria or comparison options selected

To add additional search criteria, click **Add**.

6. When you have entered the information, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 3, **Select systems** appears .
7. Select the system criteria for defining the task from the dropdown lists:
 - List criteria
 - Comparison option
 - Value for the criteria or comparison options selected
8. To add additional criteria, click **Add**.
9. When you have entered the information, click **Next** to continue with the next step or click **Previous** to return to the previous step. Step 4, **Select actions** page appears.
10. Select from the following:

- Send page (Windows only)

Add users to be paged from the dropdown list of users by clicking >>. Click << to remove users from the list of users to be paged. The pager number for an HP Systems Insight Manager (HP SIM) user is set on the **Users and Authorizations** page. If a user name in the **Users** list is inactive, the pager information for the user has not been configured. You can add the user to the list of users to be paged, but pager messages are not sent to this user until the pager information is provided on the **Users and Authorizations** page.

- Send e-mail

In the **To** field, enter the list of e-mail addresses that should receive the notification, separating each entry with a comma.

In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each entry with a comma.

In the **Subject** field, enter a note describing the subject of the e-mail.

In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:

- **Standard.** A default message format that sends a text e-mail message to the recipients
- **Pager/SMS.** An e-mail message formatted with the same information and format as a pager message is sent to the recipients
- **HTML.** An e-mail message that looks like the **HTML Event Details** page is sent to the recipients

In the **Encoding** field, select from the following formats:

- **Western European (ISO-8859-1)**
 - **Unicode (UTF-8)**
 - **Japanese (ISO-2022-JP)**
 - **Japanese (Shift_JIS)**
 - **Japanese (EUC-JP)**
- Run custom command
Select a custom command from the **Name** dropdown list. Custom commands are created under the **Tools**→**Custom Commands**→**New Custom Command** option.
 - Assign
Enter the name of the person to whom to assign the task. The event is assigned to this user when received.
 - Forward as **SNMP trap**
Enter a system name or IP address in the **Name or IP** text field, and click >> to add it to the **Trap recipients** box.
Click **Delete** if you want to delete a recipient after first highlighting the name in the **Trap recipients** box. Use the up and down arrows to scroll to the recipient to delete.
 - Write to system log
On Windows NT and Windows XP systems, the event details are written to the Application Log, and the **Source** column of the Event Log is listed as **HP SIM** for the logged event. On Linux and HP-UX systems, the event details are logged to the system log, which is usually located in the file `/var/log/messages` on Linux and in `/var/adm/sysLog/syslog.log` on HP-UX.
 - Clear event
Received events are cleared based on the criteria selected when task executes.
11. After you have made your selections, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 5, **Select time filter** appears.
 12. Select the box if you want to use time filters, and select an option from the dropdown list.
 - a. Click **Manage Filters** if you want to set user defined filters.
 - b. Select the **View time filter** box. A time filter popup window appears, showing the times selected.
If the **Use time filter** checkbox is not selected, actions are triggered whenever the events matching the selected criteria are received.
If the **Use time filter** checkbox is selected, actions are triggered **only** when they occur during the days and times specified by the selected time filter.
 - c. When you have entered the information, click **Next** to continue with the next step or **Previous** to return to the previous step. Step 6, **Review summary** page appears. The **Task name**, the **events**, **system criteria**, and **Action(s)** information are displayed. If a paging or e-mail option was selected, the modem and e-mail settings are displayed, along with buttons to change the settings.

13. Click **Edit Modem Settings** to edit the modem settings, or click **Edit e-mail Settings** to edit the SMTP settings.

Note: The event and system search criteria are displayed at the bottom of the page. This information can be extremely complex and long. Therefore, you might need to scroll down to view all of the criteria.

14. Click **Finish** to create the new task, or click **Previous** to go back to the previous step.

To set up automatic event handling with an existing event list:

1. Click **Options**→**Events**→**Automatic Event Handling**→**New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with an existing event collection**. The step 1 **Select name** appears.
3. Enter a name for the task in the **Task name** box.
4. Click **Next**. The step 2, **Select existing event collection** page appears.
5. Select the event collection from the dropdown list. This step enables you to select an event collection and its associated system collection. Click **View** to view a read-only view of the event and system collection criteria. Click **Previous** to return to the previous step, or click **Next** to continue with the next step. The step 3, **Select actions** page appears.
6. Select actions for this task. Select from the following:

- Send page (Windows only)

Add users to be paged from the dropdown list of users by clicking >>. Click << to remove users from the list of users to be paged. The pager number for an HP SIM user is set on the **Users and Authorizations** page. If a user name in the **Users** list is inactive, the pager information for the user has not been configured. You can add the user to the list of users to be paged, but pager messages are not sent to this user until the pager information is provided on the **Users and Authorizations** page.

- Send e-mail

In the **To** field, enter the list of e-mail addresses that should receive the notification.

In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each with a comma.

In the **Subject** field, enter a note describing the subject of the e-mail.

In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:

- **Standard**. A default message format that sends a text e-mail message to the recipients
- **Pager/SMS**. An e-mail message formatted with the same information and format as a pager message is sent to the recipients
- **HTML**. An e-mail message that looks like the **HTML Event Details** page is sent to the recipients

In the **Encoding** field, select from the following formats:

- **Western European (ISO-8859-1)**
- **Unicode (UTF-8)**
- **Japanese (ISO-2022-JP)**
- **Japanese (Shift_JIS)**
- **Japanese (EUC-JP)**

- Run custom command

Select a custom command from the **Name** dropdown list. Custom commands are created under the **Tools**→**Custom Commands**→**New Custom Command** option.

- Assign

Enter the name of the person to whom to assign the task. The event is assigned to this user when received.

- Forward as **SNMP trap**
Enter a system name or IP address in the **Name or IP** text field, and click >> to add it to the **Trap recipients** box.
Click **Delete** if you want to delete a recipient after first highlighting the name in the **Trap recipients** box. Use the up and down arrows to scroll to the recipient to delete.
 - Write to system log
On Windows NT and Windows XP systems, the event details are written to the Application Log, and the **Source** column of the Event Log is listed as **HP SIM** for the logged event. On Linux and HP-UX systems, the event details are logged to the system log, which is usually located in the file `/var/log/messages` on Linux and in `/var/adm/sysLog/syslog.log` on HP-UX.
 - Clear event
Received events are cleared based on the criteria selected when task executes.
7. After you have made your selections, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 4, **Select time filter** pages appears.
 8. Select the **Use time filter** box if you want to use time filters, and select an option from the dropdown list.
 - a. Click **Manage Filters** if you want to set user defined filters.
 - b. Click **View time filter**. A time filter popup window appears, showing the times selected.
If the **Use time filter** checkbox is not selected, actions are triggered whenever the events matching the selected criteria are received.
If the **Use time filter** checkbox is selected, actions are triggered **only** when they occur during the days and times specified by the selected time filter.
 - c. When you have entered the information, click **Next** to continue with the next step or **Previous** to return to the previous step. The step 5, **Review summary** page appears. The **Task name**, the **selected event collection**, the **events**, **system criteria**, and **Action(s)** information are displayed. If a paging or e-mail option was selected, the modem and e-mail settings are displayed, along with buttons to change the settings.
 9. Click **Edit Modem Settings** to edit the modem settings, or click **Edit e-mail Settings** to edit the SMTP settings.
 10. Click **Finish** to create the new task, or click **Previous** to go back to the previous step.

Adding Toolboxes

Create a **toolbox** to configure a group of tools to which a user has access.

To add a toolbox:

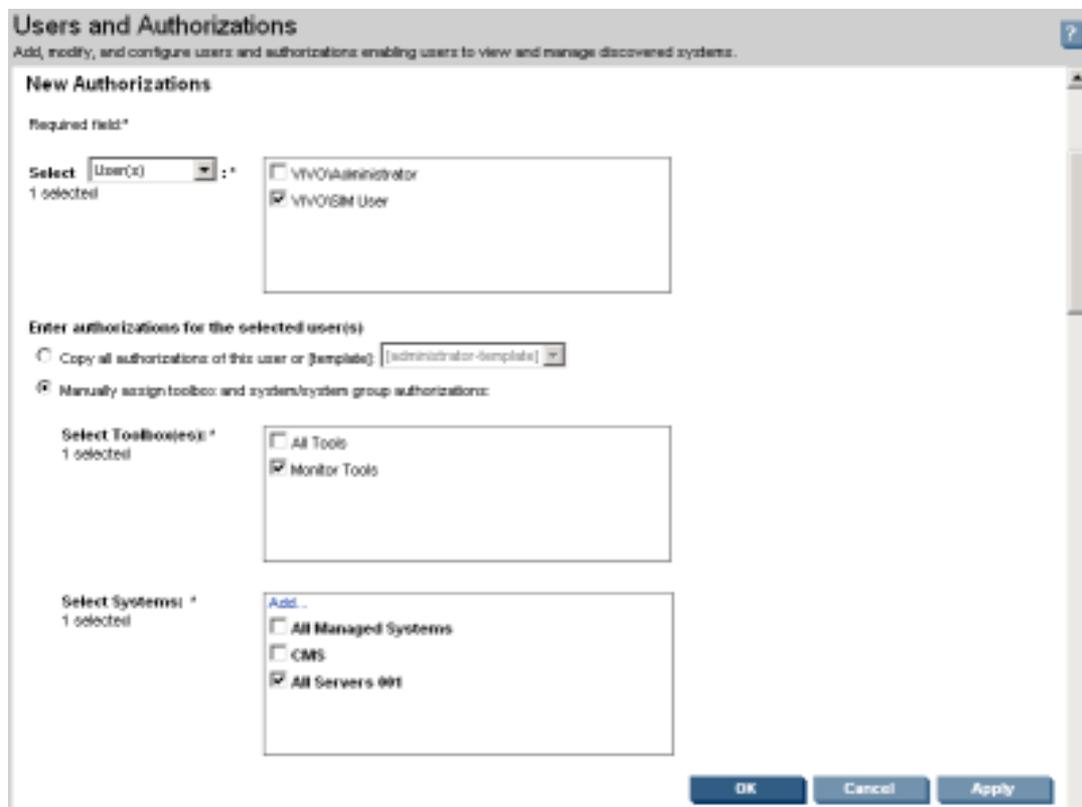
1. Click **Options**→**Security**→**Users and Authorizations**→**Toolboxes**, and then click **New**. The **New Toolbox** section appears.
2. In the **Name** field, enter a name for the new toolbox. This field is required.
3. In the **Description** field, enter a description for the toolbox.
4. Select **Toolbox is enabled** to enable the toolbox and all authorizations created with this toolbox.
5. In the **Show tools in category** field, select the category to display a list of tools in the available tools list. Select the tools to be assigned to this toolbox in the available tools list, and click >>.
The selected tools appear in the **Toolbox contents** list. You can select a tool displayed in the **Toolbox contents** list, and click << to remove it from the assigned tools list.
6. Click **OK** to save the new toolbox and close the **New Toolbox** section. Click **Apply** to save the settings without closing the **New Toolbox** section, or click **Cancel** to cancel the new toolbox creation and return to the **Toolboxes** section.

Adding Authorizations

Authorize your users for a toolbox on a system or group of systems.

To add authorizations:

1. Click **Options**→**Security**→**Users and Authorizations**→**Authorizations**, and then click **New**. The **New Authorizations** section appears.
2. In the **Select** dropdown list, select **User(s)** or **UserGroup(s)**, and select the users or groups in the box. This field is required.
3. In the **Enter authorizations for the selected user(s)** section, select one of the following options:
 - **Copy all authorizations of this user or [template]:**
Select a user or template from the dropdown list.
 - **Manually assign toolbox and system/system group authorizations**
 - a. In the **Select Toolbox(es)** section, select the toolboxes to include.
 - b. In the **Select Systems** list box, the two default system groups are displayed. Select one of these groups or click **Add** to display the **Add Systems** section to select systems for the authorization.
 1. Click the down arrow in the **Add targets by selecting from** dropdown list and select a collection.
 2. If you want to use the entire collection as your selection, select **Select "collection name" itself**; this creates a system group based on the currently displayed contents of the collection.



3. If you want to select all individual systems from the collection, select the checkbox at the top of the table view to select all systems.
Note: This creates a separate authorization for each selected system.
4. If you want to select individual systems from the collection, select the systems from the table view.
Note: This creates a separate authorization for each selected system.
5. Click **Apply** to save system selections and return to the **New Authorizations** section, or click **Cancel** to return to the **New Authorizations** section without saving changes.
Note: A system group is a group of systems based on a system collection and used for authorizations. It is a static snapshot of the contents of the collection at the time the system group was created. There are two default system groups that are not based on collections.

The **All Managed Systems** system group contains every managed system, except the **central management server (CMS)**. The CMS is excluded so that users are not mistakenly assigned the authorization to manage the CMS system itself. There is a CMS group created explicitly for the CMS. These default system groups cannot be edited, updated, or deleted.

- c. If you selected individual systems of a collection, each selection populates the list box and is selected for inclusion in the authorization. If you selected a collection and the collection has been used previously in an authorization, a message appears stating that a system group for the collection exists and will be updated with current source collection content. This affects all authorizations associated with that collection. When a collection is used for the first time, no message appears. A system group with the name of the collection followed by three numbers, usually 001, is displayed in the **Select Systems** dropdown list and is selected.
- d. Click **OK** to save the new authorization and close the **New Authorizations** section, or if you do not want to save changes, click **Cancel** to cancel the creating process.

Setting Up Managed Storage Systems

Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices. HP SIM uses this standard to discover and manage the **storage systems** it supports.

You must have a storage system's **WBEM SMI-S provider** installed and configured in order for HP SIM to discover it. This includes storage devices such as Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).

Refer to the HP SIM SMI-S Provider webpage <http://www.hp.com/go/hpsim/providers> to view the latest information regarding HP SIM support for a particular device. This webpage offers information on obtaining, installing, and configuring SMI-S providers.

Installing SMI-S Providers

Each storage vendor is responsible for the delivery and installation of the **SMI-S provider** for its storage system. The webpage referenced previously provides information on obtaining non-HP SMI-S providers. Also, consult the storage vendor's website or representative for more information regarding their SMI-S providers. For each storage system:

1. Verify that the applicable SMI-S provider is installed.
2. If the SMI-S provider is not installed, obtain and install it per the vendor's installation instructions.

Verifying SSL

HP SIM requires that **Secure Sockets Layer (SSL)** is enabled for the SMI-S provider in order to discover and manage the storage system that the provider supports. Verify that is enabled for each SMI-S provider.

This represents HP SIM's default global setting for SSL; however, you can modify this setting so that SSL is disabled. When this global setting is set to disabled, all SMI-S providers must be configured to have SSL disabled.



NOTE This is a global setting for HP SIM. All SMI-S providers must be configured to match the global setting. If a provider does not match this setting, the storage system it supports will not be discovered or managed by HP SIM.

Configuring SMI-S providers

Occasionally, it might be necessary to modify an SMI-S provider's port number or password. Use the provider's documentation to perform these modifications.

For example, if two SMI-S providers are installed on the same host but they do not share the same CIMOM, then you must configure the providers to use different ports to communicate with the CMS. The CIMOM is the part of the SMI-S provider that communicates with the CMS.

Configuring HP SIM to discover storage systems

After verifying that each storage system's SMI-S provider is installed and configured, configure HP SIM to discover the storage systems.

1. Enter the user name and password for each provider's SMI CIMOM in the Default WBEM settings section on the "Setting Global Protocol's page.
2. Add each SMI CIMOM IP address to the **System Automatic Discovery** task or to the **Creating a New Discovery** task. Refer to the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

HP SIM discovers the storage systems after the next automatic discovery task. If you want to discover your storage systems immediately, run the discovery task as described in the "Running a Discovery Task" section of the the HP Systems Insight Manager Technical Reference Guide at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

13 Configuration options

There are several configurable parameters in HP Systems Insight Manager (HP SIM) that are not available from the GUI. These parameters can only be configured by editing a configuration file on the CMS.



NOTE All HP SIM parameters have been set to predefined values that are appropriate for most situations. These parameters should only be changed if you are experiencing issues with the default values.

There are two main default locations where configuration files are stored.

For HP-UX and Linux:

- `/etc/opt/mx/config`
- `/opt/hpwebadmin/lib`

For Windows:

- `C:\Program Files\HP\System Insight Manager\config\`
- `C:\Program Files\HP\System Insight Manager\hpwebadmin\lib`

The Windows directory paths vary if HP SIM is not installed in the default location.

These files follow the format of a Java properties file. Therefore, the keys in these files are case-sensitive. In addition, the backslash (\) must be represented by a double-backslash (\\). For more information about the Java property file format, refer to <http://java.sun.com/>.

This chapter provides information on the following configuration options:

- "CPU utilization during data collection"
- "GUI time-out policy"
- "HP SIM Audit Log configuration"
- "Lifetimes for Entries on the Task Results Page"

CPU utilization during data collection

Overview

The data collection task runs many threads in parallel to overlap computing and database operations with the wait for managed systems to respond. On slower systems, this could potentially saturate the CPU for some time, depending on the processor speed of the CMS system and the number of systems being collected. Therefore, HP SIM provides some strategies to lessen the CPU usage.

Implementation

To lessen the CPU usage during data collection on the CMS:

- Limit the number of systems that are being collected at one time. For example, create separate data collection tasks for different groups of systems and schedule them to run at different times.
- Configure the CMS to use a remote database on a system other than the CMS. A substantial portion of the CPU load is consumed by the database during data collection. This option is only supported with a Windows CMS.
- Lower the `DataCollectionThreadCount` parameter in the `globalsettings.props` file. This parameter defaults to 3. Lowering it to 2 or 1 reduces the CPU demand of data collection tasks, but it increases the time required to complete the tasks.

GUI time-out policy

Overview

HP SIM provides two alternative time-out policies. The first time-out policy is for environments in which HP SIM is used to monitor system status, which is called the monitor time-out policy, and it is similar to the policy

used by Insight Manager 7. The second time-out policy is more strict and will time-out inactive users. This is called the active time-out policy and it is similar to the policy used by Servicecontrol Manager.

Monitor time-out policy

The monitor time-out policy keeps sessions alive provided the user has a Web browser window open displaying the HP SIMGUI. Closing the browser or navigating to another Web page starts the timer for the time-out period. The default time-out period is 20 minutes. Users must use some other means to protect an unattended session from illegal use, such as password-protected screen savers.

Active time-out policy

The active time-out policy only keeps sessions alive if the user is actively using the GUI, such as clicking on links and buttons. Display and refresh of the banner is not sufficient to keep the session alive. The user is timed-out either by inactivity, closing the browser, or navigating to another site. The default time-out period is 20 minutes.

Implementation

- To configure the time-out policy, edit the `globalsettings.props` file. You can switch between these modes or change the time-out period. The default time-out policy is the monitor policy. The monitor policy is enabled when:

```
EnableSessionKeepAlive=true
```

To enable the active time-out policy, change this value to `false`.

```
EnableSessionKeepAlive=false
```

- To change the default time-out period, edit the `web.xml` file. The default location for this file is:

- For HP-UX or Linux:

```
/opt/mx/jboss/server/hpsim/deploy/jbossweb-tomcat50.sar/conf/web.xml
```

- For Windows:

```
CC:\Program Files\HP\System Insight
```

```
Manager\jboss\server\hpsim\deploy\jbossweb-tomcat50.sar\conf\web.xml
```

Locate the `session-timeout` element and set it to a new value in minutes.

```
<session-timeout>20</session-timeout>
```

HP SIM Audit Log configuration

Overview

Several features of the HP SIM Audit Log are configurable. For example, you can specify which tools log data and the maximum Audit Log file size. The HP SIM Audit Log is configured through the `log.properties` file and tool logging is enabled or disabled through the XML tool definition files.

Tool behaviors

The XML tool definition file provides an option to disable logging of [single-system aware \(SSA\)](#) and [multiple-system aware \(MSA\)](#) command tools. The `log` attribute for the command element specifies whether the results of the command are output to the HP SIM log file. Command output is logged by default.

Audit Log parameters

In the `log.properties` file, you can configure the following Audit Log parameters:

- File name
- File extension
- Maximum file size in megabytes
- File extension of the roll-over name
- Amount of memory allocated for queuing items to be written to the Audit Log

Audit Log location

The location of the Audit Log can be configured using the `path.properties` file.

Implementation

Changes made to the `log.properties` file do not take effect until the log manager daemon or service is restarted. For Linux and HP-UX, restart the HP SIM daemons using `mxstop` and `mxstart`. For Windows, restart the HP SIM service.



CAUTION The queue size should be changed only with extreme care. If the queue is set too high, the log manager consumes too much system memory.



NOTE When the Audit Log file reaches the maximum file size, the log is renamed with `MX_LOGROLLFILEEXT` extension and a new file is started. If a previous version of the file has already been renamed with the `MX_LOG_ROLLFILEEXT` extension, it will be an automatic roll-over of an audit log file. A roll-over will not occur until a task running is completed. However, after one hour of exceeding the maximum file size, if the task is not finished, then the audit log file will roll over to another file.

To configure the location of the Audit Log:

1. For Windows, create a file named `path.properties` under `C:\Program Files\HP\System Insight Manager\config`.
For Linux and HP-UX, create a file named `path.properties` under `/etc/opt/mx/config`.
2. Add the following entry in the `path.properties` file: `LOG= \\Auditlog\Logs` or `LOG=C:/Auditlog/Logs`.
Note: `C: \\Auditlog\Log` is listed here as an example. This path is user defined.
3. For Linux and HP-UX, restart the HP Systems Insight Manager (HP SIM) daemons (`mxstop` and `mxstart`). For Windows, restart the HP SIM service. After restarting the service, a new log file named `mx.log` resides in the directory specified in `path.properties` file.

Lifetimes for Entries on the Task Results Page

Overview

HP SIM enables you to set how long entries remain on the **Task Results Page** after a task completes its results.

Short and long task lifetimes

Some task results are kept for a short time, while other task results are kept for a longer time. Tasks fall into one or the other category based on the type of tool associated with them. Tasks for the following tools have a short lifetime:

- Web-launch tools
- Tools that run from the `mxexec` command line using the `-o` or `-O` options to save the command output
- Tools that run X-Window commands
- Tools that specify in their tool definition the "job-log" flag as disabled including:
 - Hardware Status Polling
 - Data Collection
 - Identify Systems
 - Software Status Polling
 - Delete Events
 - System Protocol Settings
 - Automatic Discovery
 - Hardware Status Polling

Tools in this category have no task output, have task output that is saved outside of HP Systems Insight Manager, or have task results that are unlikely to be of long-term interest. Tasks for all other tools have the long lifetime.

Frequently scheduled tasks

Task results can also be removed from the **Task Results Page** if a certain number of task results for a scheduled task accumulate. This setting defaults to 10 instances of a single task. If more than 10 accumulate on the results page, then the oldest task result for this scheduled task is removed.

Last result tasks

A task result is kept indefinitely if it is the last result for a scheduled task. For example, if a scheduled task is disabled, its final task result is kept indefinitely, or until the task is enabled and more task results accumulate.

Implementation

To configure the short and long task lifetimes, edit the `mx.properties` file.

- The short lifetime defaults to 30 minutes. To change that time, edit:

```
MX_JOB_CACHE_TIME_COMPLETED_JOBS=30
```

- The long lifetime defaults to 30 days. To change that time, edit:

```
MX_JOB_MAX_COMPLETED_JOB_AGE=30
```

- Task results for frequently scheduled tasks start to drop off after 10 instances. To change this value, edit:

```
MX_JOB_MAX_COMPLETED_JOBS_PER_TASK=10
```



NOTE The limit of 10 task results applies to scheduled tasks with the "job-log" flag enabled in the tool definition. Scheduled tasks for the tools with the "job-log" flag disabled have a limit of 1. This value is not configurable.

- By default, the last task results for a scheduled task is kept indefinitely. If you want to keep more than 1 job, edit:

```
MX_JOB_MIN_COMPLETED_JOBS_PER_TASK=1
```



NOTE This many job instances per task is kept regardless of the `MX_JOB_MAX_COMPLETED_JOB_AGE` setting.

14 Troubleshooting

GUI Issues

Parts of the GUI do not show up on my Linux system, such as the devices in the system list, or the System and Events Lists area on the left.

Solution: You need to remove everything and re-install. You may have a previous version of PostgreSQL or HP Systems Insight Manager (HP SIM) on your system that you failed to remove before installing the new version.

Installation Issues

I am unable to load HP SIM on Windows NT 3.51 or Windows NT 4.0.

Solution: Windows NT 3.51 and Windows NT 4.0 are not a supported platform.

During a Windows install at the database credentials screen the installer fails with an invalid credentials error, I am unable to enter my password.

Solution: A user name and password cannot contain the following:

- A space followed by a double-quote
- An Oracle username cannot contain the following: a backslash (/) or a forward slash (\).

If you use these characters in your user name or password, you will receive an "Invalid character" error and not be allowed to sign in.

I receive the error "Database Connection Error" during the Java-based database installation portion of HP SIM installation.

Solution: Verify that the target Microsoft SQL Server service (MSSQL) is running (select **Control Panel**→**Services**→**MSSQLSERVER**).

When installing HP SIM on a Linux or HP-UX system with long hostnames, the installation fails.

Solution: HP SIM 5.0 supports discovery and management of systems with long hostnames on Linux and HP-UX (up to 256 characters), but does not yet support being installed on systems with long hostnames.

During the installation, the system reboots, and then the installation launches the browser. Internet Explorer displays a message saying that it could not establish a connection with the local host. The browser is being launched before the service has had time to start.

Solution: Try to access the URL again by placing the cursor in the URL field and pressing the Enter key. Keep trying until the application loads in the browser.

During the installation, the system reboots, and then the installation launches the browser. Internet Explorer displays a message saying that it could not establish a connection with the local host. The browser is being launched before the service has had time to start.

Solution: Try to access the URL again by placing the cursor in the URL field and pressing the Enter key. Keep trying until the application loads in the browser.

Login Issues

I am unable to log into HP SIM or to managed systems browsing from HP SIM using Internet Explorer 6.0.

Reason 1: Internet Explorer has a problem with underscores in system names, which prevents the authentication cookie from working properly.

Solution 1A: For HP SIM, if you are using Internet Explorer 6.0 and your HP SIM server has an underscore in the name, use the IP address of the HP SIM server instead of the name in the Internet Explorer address field.

Solution 1B: For managed systems, if the names of the systems have an underscore, use the IP address of the system. Configure HP SIM to create links to the system using the IP address instead of the name:

1. Browse and sign into HP SIM.
2. Select **Options**→**Security**→**System Link Configuration**. The System Link Configuration page appears

3. Select Use the system IP address.
4. Click **OK**.

Note: By using IP addresses instead of names, you might encounter security alerts, if the name in the managed system certificate does not match the name in the link. The default certificate for managed systems uses the system name, not the IP address.

Reason 2: For managed systems, the privacy policy setting in Internet Explorer 6.0 is blocking the authentication cookies from the managed systems.

Solution 2A: Change the browser privacy security policy setting. From the Internet Explorer browser menu, select **Tools**→**Internet Options**, then select the **Privacy** tab. The privacy setting can be modified in one of the following ways:

- ▲ Set the privacy setting to **Accept all Cookies** by sliding the slider bar to the bottom. This setting allows a browser to accept all cookies for both first-party and third-party sites. When browsing to HP SIM or directly to a managed system, it is considered a first-party site. When navigating to a managed system through HP SIM, the system is considered a third-party site.

or

- ▲ Customize the handling of cookies by clicking **Advanced** and enabling **Override automatic cookie handling**. Then select the appropriate radio buttons for first-party and third-party cookies to **Accept** or **Prompt**. If you select **Prompt**, the browser prompts you on how to handle a cookie each time a cookie is received. You can choose to block or allow the cookie each time, or for all times. Enabling **Always allow session cookies** does not resolve the problem because the Web Agents do not use session cookies.

or

- ▲ Individually specify the handling of cookies for each system. Click **Edit** in the **websites** section and add the address of the system in the specified field. Click **Allow** to always allow cookies to that system. Repeat this for all systems.

Solution 2B: Remove the systems from the Internet Zone. The privacy policy only affects systems in the browser Internet Zone, so by removing systems from that zone, you prevent the privacy policy from affecting those systems. This can be accomplished in one of the following ways:

- Browsing to systems by IP address instead of by name can cause the browser to consider those systems to be in the Internet Zone. Instead, browse by name. You can configure HP SIM to use system names when creating links to systems by selecting **Options**→**Security**→**System Link Configuration** and selecting **Use the system name**.
- If your browser is configured to use a proxy server, you can configure your browser to bypass the proxy server for specific systems, which removes those systems from the browser **Internet Zone**. From the browser menu, select **Tools**→**Internet Options**, then select the **Connections** tab. Click **LAN Settings**, and if you are configured to use a proxy server, click **Advanced**. In the **Exceptions** list, you can specify a list of addresses that should bypass the proxy server. These addresses are no longer be in the **Internet Zone** and are not affected by the privacy settings policy.

Servicecontrol Manager and HP SIM Issues

If you are upgrading your system from HP-UX 11i v1 to HP-UX 11i v2, and HP SIM 4.X is installed and you do not want to run HP SIM in the future, you can remove the HP SIM product.

To remove HP SIM execute the following command:

```
swremove - xenforce__dependencies=false T2414BA
```

If you are upgrading your system from HP-UX 11i v1 to HP-UX 11i v2, and HP Servicecontrol Manager 3.0 is configured on your system or HP SIM is installed on your system, and you want to continue to run HP SIM in the future, you must upgrade to HP SIM using one of the following upgrade scenarios:

- If HP Servicecontrol Manager 3.0 is configured on your system and you do not want to lose your data, you must upgrade Servicecontrol Manager 3.0 to HP SIM 4.2. before upgrading your system from

HP-UX 11i v1 to HP-UX 11i v2. Refer to [Chapter 7. Upgrading from HP Servicecontrol Manager to HP Systems Insight Manager](#) for more information.

- If you do not want to keep any of the data from HP Servicecontrol Manager, you can remove Servicecontrol Manager before starting the upgrade. Determine if HP Servicecontrol Manager is installed on your system by using the following commands:

```
swlist -l bundle B8337BA B8339BA B8338BA
```

```
swlist -l product ServControlMgr AgentConfig SysMgmtServer SysMgmtAgent
```

Uninstall HP Servicecontrol Manager using the following command:

```
swremove ID
```

where ID is the product or bundle ID. For example:

```
swremove -x enforce__dependencies=false B8339BA
```

or

```
swremove -x enforce__dependencies=false \ SysMgmtServer SysMgmtAgent
```

Remove the old product subdirectories by executing the following command:

```
rm -fr /opt/mx /etc/opt/mx
```

- If Servicecontrol Manager is not configured or if HP SIM 4.x is installed, and you want to continue to use HP SIM, you must select HP SIM 5.0 for upgrade.

Execute the following command:

```
-x match_target=true
```

option or by using the interactive mode to select HPSIM-HP-UX.

You can also specify HPSIM-HP-UX on the command line. The HP SIM 5.0 installer will upgrade both a configured and an un-configured HP SIM 4.X. If you chose to remove either HP Servicecontrol Manager or HP SIM, you must execute the following command to remove subdirectories that were used in the product:

```
rm -fr /opt/mx /etc/opt/mx
```

If these subdirectories are not removed, you might encounter database errors when trying to run `mxinitconfig -a` when installing HP SIM 5.0.

Servicecontrol Manager and HP-UX 11i Issues

If HP Servicecontrol Manager version 2.5 or earlier is installed on your HP-UX 11i v1 operating system, you must remove Servicecontrol Manager before upgrading your system to HP-UX 11i v2. If you do not remove HP Servicecontrol Manager version 2.5 or earlier from your system, the upgrade process to HP-UX 11i v2 will fail.

If you are upgrading your system from HP-UX 11i v1 to HP-UX 11i v2 and have never run HP Servicecontrol Manager and do not plan to use HP SIM, you can remove the HP Servicecontrol Manager product after upgrading your operating system to HP-UX 11i v2.

Solution: Determine if version 2.5 or earlier of HP Servicecontrol Manager is installed on your system by typing the following commands:

```
swlist -l bundle B8337BA B8339BA B8338BA
```

```
swlist -l product ServControlMgr AgentConfig SysMgmtServer SysMgmtAgent
```

Note whether the version number is A.02.05.xx or earlier. If the version number is A.02.05.xx or earlier, then you must remove Servicecontrol Manager from your HP-UX 11i v1 system. Also note if the file `/var/opt/mx/dta/.inititalization` exists. If this file exists on your system, then you must remove Servicecontrol Manager from your HP-UX 11i v1 system before upgrading to HP-UX 11i v2. Uninstall HP Servicecontrol Manager using the following command:

```
swremove ID
```

where ID is the product or bundle ID. For example:

```
swremove -x enforce__dependencies=false B8339BA
```

```
swremove -x enforce__dependencies=false SysMgmtServer SysMgmtAgent
```

Remove the old product subdirectories by executing the following command:

```
rm -fr /opt/mx /etc/opt/mx
```

Upgrade Issues

When upgrading from previous versions of HP SIM to HP SIM 5.0, tools that are now obsolete can remain in the Monitor Tools toolbox.

If upgrading from HP SIM 4.2 or later, the list of tools include:

type	General Tools
cat	General tools
find	General tools

If upgrading from a version prior to HP SIM 4.2, the list of tools include:

type	General tools
cat	General tools
find	General tools
cp	General tools
mv	General tools
rm	General tools
copy	General tools
del	General tools

Solution:

1. To remove the obsolete tools, sign in HP SIM as a full configuration rights user.
2. Select **Options > Security > Users and Authorizations**, and then select the Toolboxes tab.
3. Select the **Monitor Tools toolbox**.
4. Click **Edit**.
5. In the **Toolbox contents** panel, select the tools to remove and click the <<button.
6. Click **OK** to save.

glossary

A

- agent** A program that regularly gathers information or performs some other service without the user's immediate presence. HP Systems Insight Manager (HP SIM) agents provide in-depth hardware and software information and subsystem status to HP SIM and numerous third-party management applications.
See Also management agent.
- alarm** A user-configurable notification displayed in the **System Status** panel of HP SIM when certain events occur. For instance, if a monitored item changes, an alarm notifies the user that a change has occurred.
See Also trap, event.
- all events** Systems where any event types have occurred.
- All Tools toolbox** A default toolbox that provides complete access to all tools for the authorized system or system group.
- attribute** A single characteristic of a manageable product or component, as in an attribute of a Management Information Format (MIF) file. A set of related attributes constitutes a group. For example, the clock speed of a processor chip is an attribute of a group that describes that chip.
See Also Management Information Format.
- authentication** The process of identifying an individual, based on a user name and password. Authentication is distinct from authorizations and ensures that the individual is who they claim to be.
- authorizations** A mapping of a relationship between a user, a toolbox, and a system or system group.
- automatic discovery** The process that HP SIM uses to find and identify the systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status.
- available software** A listing of the software components available in the repository to which the HP VCA has been configured to point. When browsing directly into a HP VCA, these additional components can be selected for installation.

B

- banner** The section of the GUI at the top of the screen that includes the user name and links to the **Home** page and sign out functions.

C

- caution** A note to indicate that failure to follow directions could result in damage to equipment or loss of information.
- central management server ()** A system in the management domain that executes the HP SIM software. All central operations within HP SIM are initiated from this system.
- central processing unit polling rate** The rate for how often the Cluster Monitor CPU Resource checks CPU utilization as reported by HP Insight Management Agent on monitored systems.
- certificate** An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together.
See Also certificate authority.
- certificate authority ()** A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual they claim to be.
- cleared status** A status condition that indicates a system is cleared.
- clearing events** Changing the event status from uncleared to cleared.
- clients** HP desktop, portable, and workstation systems.

cluster	A parallel or distributed computing system made up of many discrete systems that form a single, unified computing resource. Clusters vary in their features, complexity, and the purposes for which they are best suited.
cluster IP address	The IP address of the cluster.
cluster monitor	A core component of HP SIM. Cluster Monitor adds the ability to monitor and manage multi-node clusters. Cluster Monitor also manages multiple cluster platforms in a heterogeneous environment.
cluster monitor resource	A program that provides a monitoring or management function for clustered nodes in a cluster.
cluster system identification	Information about cluster systems. This information is stored in the database.
collections	The method for grouping system or event searches.
command line interface ()	A program interface where commands can be executed directly from the command shell of the operating system command shell.
common information model ()	An object-oriented schema defined by the Desktop Management Task Force (DMTF). CIM is an information model guide that describes and shares management information enterprise-wide. CIM is designed for extending each management environment in which it is used.
common information model object manager ()	A CIMOM acts as the interface for communication between web-based enterprise management (WBEM) providers and management applications such as HP Systems Insight Manager. A CIMOM that provides an interface for an SMI-S provider is called an SMI CIMOM.
communications protocol	See management protocol.
component	A component is a single, self-describing, installable (interactive or silent) binary file containing a single piece of software, such as firmware image, driver, agent, or utility, that is supported by the management and update tools.
configuration history report	The Survey Utility that contains reports that show configuration details for server and compares configuration history files for differences.
Configure or Repair Agents	An HP SIM plug-in feature that enables you to repair credentials for SNMP settings and trust relationships that exist between HP SIM and target systems. You can also update Web Agent passwords on target systems that have 7.1 agents or earlier installed.
control tasks	Sequences of instructions that are associated with a search, event, or both, such as Delete Events, Remove Disk Thresholds, Set Disk Threshold, and Set Device Access community strings.
critical status	A state generated when HP SIM can no longer communicate to a managed system.
custom commands	Tasks that launch an application on the server that is running HP SIM.

D

data collection reports	Data collection reports include information about discovered systems in a single instance or a historical trend analysis report. HP SIM supports Overwrite existing data set (for detailed analysis) , formerly known as Single Instance Data Collection task in Insight Manager 7, and Append new data set (for historical trend analysis) , formerly known as Historical Data Collection task in Insight Manager 7. With Overwrite existing data set (for detailed analysis) , data is collected from a system at a single instance. With Append new data set (for historical trend analysis) , data detailing the system history is collected.
data collection tasks	Procedure that involves gathering information from a group of managed systems and storing that information in the database. HP SIM uses Hardware Status Polling and Data Collection Tasks to implement collection.
Desktop Management Interface ()	An industry-standard protocol, primarily used in client management, established by the DMTF. DMI provides an efficient means of reporting client system problems. DMI-compliant computers can send status information to a central management system over a network.
Desktop Management Taskforce ()	An industry standard body that defines DMI and WBEM standards for the industry. HP is an active sponsor and participant in the DMTF body.

digital signatures	A technology used to validate the sender of a transaction. This technology uses private keys to digitally sign the data and public keys to verify the sender.
discovery	A feature within a management application that finds and identifies network objects. In HP management applications, discovery finds and identifies all the HP systems within a specified network range.
discovery filters	Enables users with full configuration rights to prevent or allow certain system types from ever being added to the database.
discovery template	Files that can be used by automatic discovery in lieu of typing the addresses directly in to the Ping inclusion ranges or Exclusion ranges fields on the Automatic Discovery - General Settings page and are designed to be used as a quick way to change the scope of automatic discovery.
Distributed Component Object Model ()	An extension of the Component Object Model (COM) that enables COM components to communicate between clients and servers on the same network.
distributed task facility ()	A management application that manages the remote execution of tasks on managed systems.
DMI	See Desktop Management Interface.
Domain Name Service ()	A service that translates domain names into IP addresses.

E

e-mail notification	One of the notification tasks in HP SIM that sends notifications through e-mail.
edit collection	To modify existing collections to add or remove search criteria.
enclosure	A physical container for a set of blades servers. It consists of a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies.
event	<p>Information sent to certain users that something in the managed environment has changed. Events are generated from SNMP traps and are preconfigured in this release. HP SIM receives a trap when an important event occurs. Events are defined as:</p> <ul style="list-style-type: none"> • Warning. Events of this type indicate a state that might become a problem. • Informational. Events of this type require no attention and are provided as useful information. • Normal. Events of this type indicate that this event is not a problem. • Minor. Events of this type indicate a warning condition that can escalate into a more serious problem. • Major. Events of this type indicate an impending failure. • Critical. Events of this type indicate a failure and signal the need for immediate attention.
event overview	A chart that summarizes the uncleared events by product type.
external sites	Third-party application URLs.

F

full configuration rights user	A user who is automatically authorized for the All Tools toolbox on all systems, including the CMS. This type of user has been given special privileges to administer the HP SIM software.
---------------------------------------	---

G

graphical user interface () A program interface that takes advantage of the graphics capabilities of the computer to make the program easier to use. The HP SIM GUI is web-enabled and displays in a web browser.

H

hosts files A file that includes all critical system information from the HP SIM database, such as IP addresses.

HP Insight Management Agent A program that regularly gathers information or performs some other service without the user's immediate presence.

HP ProLiant Essentials Virtual Machine Management Pack () Provides central management and control of Virtual Machines on Microsoft Virtual server, Vmware's GSX and ESX. Integrated with HP SIM, VMM provides unified management of HP ProLiant host servers and Virtual Machines.

HP ProLiant Essentials Vulnerability and Patch Management Pack The all-in-one vulnerability assessment and patch management tool integrated into HP SIM, simplifying and consolidating the proactive identification and resolution of issues that can impact server availability into one central console.

HP Systems Insight Manager System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables.
HP SIM; combines the strengths of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms. HP SIM can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins for rapid deployment, performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets.

HP Systems Insight Manager database () The database that stores vital information about HP SIM, including users, systems, and toolboxes.

HP Version Control Agent () An agent that is installed on a server to enable you to see the HP software installed on that server. The HP VCA can be configured to point to a HP VCRM agent, enabling easy version comparison and software update from the repository.

HP Version Control Repository Manager () An HP agent that enables a customer to manage HP provided software stored in a user-defined repository.

HyperText Transfer Protocol () The underlying protocol used by the World Wide Web.

I

identification An aspect of the discovery process that identifies the management protocol and type of system.

installed version A particular HP software component that is installed on the server the HP VCA is installed on.

Instant Support Enterprise Edition () Provides proactive remote monitoring, diagnostics, and troubleshooting to help you enhance the availability of HP-UX, Microsoft Windows, Linux, OpenVMS, Tru64 Unix, NonStop, and Sun Solaris servers, as well as storage and network systems in your data center.

Internet Protocol () Specifies the format of datagrams (packets) and the addressing scheme on a network. Most networks combine IP with Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

Internetwork Packet Exchange () A networking protocol used by the Novell NetWare operating systems and is a datagram (packet) protocol used for connectionless communications.

IP range	Systems with an IP address that falls in the specified range.
J	
Java database connectivity ()	Similar to ODBC, this set of application program interfaces (APIs) provides a standard mechanism to allow Java applets access to a database.
Java Remote Method Invocation ()	A set of protocols that enable Java objects to communicate remotely with other Java objects.
K	
key	A value used alone or with an encryption decoder (corresponding public or private key) for cryptography. In traditional private key cryptography, the communicators share a key or cipher so that each can encrypt and decrypt messages. The risk in this system is that if any party loses the key, the system is broken. In public key cryptography, the private key is associated with a public key, so each person in the system has a personal private key that is never shared.
keystore	A database that maintains a list of keys. The keystore can contain a subject's own private key. A keystore can also contain a list of public keys, as published in certificates. See Also key.
L	
limited configuration rights user	A user who has limited capability to configure the CMS. Limited-configuration-rights users have permission to create, modify, and delete all reports and their own tools.
M	
Major status	Aggregate status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken immediately.
managed systems	Any system managed by HP SIM, such as servers, desktops, and Remote Insight Boards (RIBs).
management agent	A daemon or process running on a managed system. It receives and executes requests from the CMS on the managed system.
management domain	A collection of resources called managed systems that have been placed under the control of the HP SIM. Each central management server is responsible for a management domain. The managed systems can belong to more than one management domain.
Management HTTP Server	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software. This version is available in the ProLiant Support Pack 7.10 or earlier.
Management Information Base ()	The data specification for passing information using the SNMP protocol. An MIB is also a database of managed objects accessed by network management protocols.
Management Information Format ()	An ASCII text file in the DMI architecture that describes the manageable features and attributes of a product. The DMI maintains this information in a MIF database and makes it available to operating systems and management applications. The DMTF has specified MIF formats for a variety of system types and peripheral systems.
management instrumentation	Agents running on systems that provide management information for HTTP, DMI, or SNMP protocols.
management LAN	A LAN dedicated to the communications necessary for managing systems. It is typically a moderate bandwidth (10/100 BaseT) and secured through limited access.
management protocol	A set of protocols, such as WBEM, HTTP, SNMP, or DMI, used to establish communication with discovered systems.
management scope	A set of systems within the set of all discovered systems that HP SIM manages.

management services	The provider of a core set of capabilities such as auto-discovery, data collection, a central repository for system and event information, event management, basic notification, and secure access. These functions are used by add-ins from HP, a Management Solutions Partner, and HP SIM users.
management tasks	Procedures you set up to search systems or events.
manual discovery techniques	Processes that enable you to bypass a full discovery for the following tasks: <ul style="list-style-type: none"> • Adding a single system • Editing the system • Creating or importing an HP SIM database hosts file • Creating or importing generic hosts files
Microsoft Clustering Service status page	A page that summarizes cluster status as defined by Microsoft Cluster Server and lists the status and values of MSCS-defined cluster attributes. The Cluster Monitor uses color to display status based on MSCS condition values (Normal, Degraded, Failed, and Other).
Minor status	Aggregate status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken as soon as possible to prevent further failure.
Monitor Tools toolbox	A default toolbox that contains tools that display the state of managed systems but not tools that change the state of managed systems.
multiple-system aware ()	A run type that supports multi-system operations. Tools with this run type operate on the target systems using their own internal mechanisms instead of using the distributed task facility. The MSA run type uses the distributed task facility to launch the tool on a single system before the tool interacting with the other managed systems.
N	
no configuration rights user	A user who cannot configure the CMS. However, the user can view and run predefined reports on the CMS and all managed systems.
O	
Open Service Event Manager ()	Enables you to collect, filter, and send problem reports for supported systems (ProLiant and Integrity) running Insight Management Agents. In addition, OSEM automatically sends service event notifications to HP SIM when a problem is detected on the system.
overall software status	This section indicates whether the software on the server that the HP VCA is installed on has any updates available within the repository in which it has been configured to monitor.
P	
HP ProLiant and Integrity Support Pack	An ProLiant and Integrity Support Pack is a set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An ProLiant and Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.
Performance Management Pack ()	A software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers. PMP tools consist of Online Analysis, Offline Analysis, Comma Separated Value (CSV) File Generator Report, System Summary Report, Status Analysis Report, Configuration, Licensing, and Manual Log Purge.
ProLiant Essentials license key	The contractual permissions granted by HP to the customer in the form of a coded embodiment of a license that represents a specific instance of a license. A single license can be represented by a single key or by a collection of keys.
ProLiant Support Pack	A set of HP software components that have been bundled together by HP and verified to work with a particular operating system. A ProLiant Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.

R

racks	A set of components cabled together to communicate between themselves. A rack is a container for an enclosure.
Red Hat Package Manager ()	The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.
Reference Support Pack	A baseline bundle of HP software components that the HP VCA can be configured to point to in the repository. This setting enables users to indicate that they want to keep all of their software up to a certain Support Pack level.
remote wakeup	<p>Sometimes referred to as Wake-On-LAN (WOL). The remote powering up of a system through its resident WOL network card, provided that the system has been enabled to be so awakened using the ROM or F10 Setup.</p> <p>This is a capability on which HP SIM relies to turn on the systems for scheduled Software Updates or Replicate Agent Settings.</p>
remove all disk thresholds	A task provided by HP SIM to remove disk thresholds for systems in an associated collection. This task only removes disk thresholds that were set by HP SIM or by browsing directly to the Web Agent. Any thresholds set by HP SIM for Windows 32, including disk thresholds, are not removed by this task.
Replicate Agent Settings	A tool that can be used to copy web-based agent settings to a group of systems.
repository	A directory containing ProLiant Support Pack or Integrity Support Packs and Smart Components.
Resource Partition	<p>A subset of the resources owned by an operating system instance. The use of those resources is controlled through technologies such as the Fair Share Scheduler, pSets, and Memory Resource Groups.</p> <p>A resource partition also has a set of processes associated with it, and only those processes can use the resources within the resource partition. Policies established by tools such as Process Resource Manager (PRM), Workload Manager (WLM), or Global Workload Manager (gWLM) control how resources are allocated to the set of resource partitions within an operating system instance.</p>
role	See toolbox.
rule set	Conditions, policies, or criteria applied to system information to determine what it is.

S

search criteria	A set of variables (information) used to define a requested subset of information from the set of all information. The information set that can be filtered includes action information, some of the system information, and so on. A filter is composed of an inclusion filter followed by an exclusion filter. The result of these two filtering operations is called a group. An example of a filter is an SQL statement that creates viewable information or causes management operations to be performed.
Secure HTTP ()	An extension to the HTTP protocol that supports sending data securely over the web.
Secure Shell ()	A program to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.
Secure Sockets Layer ()	A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common usage of SSL is to provide authentication of the server, so clients can be assured they are communicating with the server it claims to be. It is application protocol independent.
Secure Task Execution ()	A feature of HP SIM that securely executes a task from a managed system. STE ensures that the user requesting the task has the appropriate rights to perform the task, and encrypts the request to protect data from snooping.

security roles	A feature that enables administrators to restrict system access and manage access on a per-user or per-group basis. This capability enables systems administrators to delegate tasks to junior staff without providing access to advanced or dangerous features. It also enables systems administrators to delegate management of systems to specific organizations or customers without providing access to systems owned by other organizations or customers.
self-signed certificate	A certificate that is its own Certificate Authority (CA), such that the subject and the CA are the same. See Also certificate, certificate authority.
server blade	Typically a very dense server system containing microprocessors, memory, and network connections that can be easily inserted into a rack-mountable enclosure to share power supplies, fans, switches, and other components with other server blades. Server blades tend to be more cost-efficient, easier to deploy, and easier to adapt to growth and change than traditional rack-mounted or tower servers. See Also enclosure, racks.
server blade visual locator	A feature designed to provide visual representation of ProLiant BL e-Class and p-Class servers within their respective enclosures and racks. See Also enclosure, racks.
Service Advertising Protocol (SAP)	A NetWare protocol used to identify the services and addresses of servers attached to the network.
set disk thresholds	A task provided by HP SIM to set a disk threshold for systems in an associated collection. This threshold is set on all disk volumes on the target system.
Shared Resource Domain (SRD)	A collection of compartments—all of the same type—that share system resources. The compartments can be nPartitions, virtual partitions, processor sets (pSets), or Fair Share Scheduler (FSS) groups. A server containing nPartitions can be an SRD—as long as nPartition requirements are met. A server or an nPartition divided into virtual partitions can be an SRD for its virtual partition compartments. Similarly, a server, an nPartition, or a virtual partition containing pSets can be an SRD for its pset compartments. Lastly, a Server, an nPartition, or a virtual partition containing FSS groups can be an SRD for its FSS group compartments. A complex with nPartitions can hold multiple SRDs. For example, if the complex is divided into nPartitions, named Par1 and Par2, Par1's compartments could be virtual partitions, while Par2's compartments are pSets. Each compartment holds a workload. gWLM manages the workload by adjusting the compartment's resource allocation.
Short Message Service (SMS)	A convenient way to send brief text messages directly to a wireless phone. There is a maximum message length of 140 characters.
Simple Network Management Protocol (SNMP)	One of the management protocols supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. MIB-2 is the standard information available consistently across all vendors.
Single Login	Permission granted to an authenticated user browsing to HP SIM to browse to any of the managed systems from within HP SIM without re-authenticating to the managed system. HP SIM is the initial point of authentication, and browsing to another managed system must be from within HP SIM.
single-system aware (SSA)	A run type that does not support multi-system operations. Tools with this run type are only aware of the system on which they are running.
SMI CIMOM	See common information model object manager.
SMI-S provider	An industry-standard WBEM provider that implements a well defined interface for storage management. The manufacturers of host bus adapters (HBAs), switches, tape libraries, and storage arrays can integrate SMI-S providers with their systems, or provide them as separate software packages. See Also Web-Based Enterprise Management.
SNMP communication setting	Default SNMP community string used when communicating with systems supporting SNMP communications.
SNMP trap	Asynchronous event generated by an SNMP agent that the system uses to communicate a fault.

software inventory	A listing of the HP software installed on the system where the HP VCA is installed.
software update	A task to remotely update software and firmware.
spoofing	The act of a website posing as another site to gather confidential or sensitive information, alter data transactions, or present false or misleading data.
standard error ()	The default place where the system writes error messages. The default is the terminal display.
standard output ()	The default place to which a program writes its output. The default is the terminal display.
status message list	A list created by Cluster Management Resources to collect entries found in the bottom left area of the Cluster Monitor page to bring your attention to cluster attributes that are in an abnormal state.
status message summary header	The list header summary of the total number of status messages in the list and, in parentheses, the number of status messages that have not been examined.
status type	The classification of status messages (for example, Critical, Major, Minor, Normal, Warning, and Unknown).
Storage Management Initiative Specification ()	A standard management interface developed by the Storage Networking Industry Association (SNIA). SMI-S provides a common interface and facilitates the management of storage devices from multiple vendors. SMI-S uses industry-standard common information model and Web-Based Enterprise Management technology.
storage systems	SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).
subnet	On TCP/IP networks, subnets are all systems whose IP addresses have the same prefix. For example, all systems with IP addresses that start with 10.10.10. would be part of the same subnet.
Survey Utility	An agent (or online service tool) that gathers and delivers hardware and operating system configuration information. This information is gathered while the server is online.
symmetric key	A common key that both the server and receiver of a message share and use to encrypt and decrypt a message.
system	Systems on the network that communicate through TCP/IP or IPX. To manage a system, some type of management protocol (for example, SNMP, DMI, or WBEM) must be present on the system. Examples of systems include servers, workstations, desktops, portables, routers, switches, hubs, and gateways.
system default searches	Requests for data about aggregate system health status, proactive subsystem status, and detailed component information on servers, workstations, desktops, and portables, irrespective of management protocol.
system group	A group of systems based on a system collection; a static snapshot of the source collection at the time the system group was created. Used for authorizations.

system health status	<p>This is the overall status gathered from protocols (DMI, SNMP, WBEM, Insight Management Agents, and so on) that are supported on a target system. Status is defined as:</p> <ul style="list-style-type: none"> • Critical HP SIM can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems. • Major A major problem exists with this system. It should be addressed immediately. For systems running an HP Insight Management Agent, some component has failed. The system might no longer be properly functioning, and data loss can occur. • Minor A minor problem exists with this system. For systems running Insight Management Agent, some component has failed but the system is still functioning. • Warning The system has a potential problem or is in a state that might become a problem. • Normal The system is functioning correctly. • Disabled The system is disabled from monitoring but is not necessarily turned off. • Unknown HP SIM cannot obtain management information about the system. • Informational The system might be in a transitional or non-error state.
system identification	<p>Identifying information about systems. This information is stored in the database. The following information is identified:</p> <ul style="list-style-type: none"> • Type of management protocol on the system (SNMP, DMI, WBEM, HTTP, and SSH) • Type of HP system (server, client, switch, router, and so on) • Network name of system
system information	<p>Information that is provided on the System Page under the Identity tab. The system information includes:</p> <ul style="list-style-type: none"> • Network address • Network name • Description • Contact • Location • System links
system information using DMI	<p>Agents that conform to the DMI V2 standard and have passed testing. The list of compliant DMI V2 agents can be found on http://www.dmtf.org.</p>
system information using SNMP	<p>Agents that conform to SNMP MIB-2 standards.</p>
system links	<p>A summary information page for a specific system that has a management agent.</p>
System Management Homepage ()	<p>An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.</p>

system overview report	A report indicating the state of systems that is available at the time that HP SIM is first opened. A system search result contains the number of systems that are registered with the HP SIM databases. Systems are grouped by their status conditions. Each number in a column is a hyperlink to a more detailed list of systems, which displays the systems that correspond to the number in the overview.
system search	Logical grouping of systems into a collection based on information in the HP SIM database. After a search is defined, you can display the results from the system view page or associate it with a management task.
system search results	The result of a system search.
system status panel	The section of the GUI on the left of the screen that displays status information and system or event alarms.
system type	One of 12 supplied types. You can add your own based on one of these types. For example, use Server type to create MyServer type. It is still a server and is reported on in the same way, but it has your designation.
System Type Manager ()	A utility that enables you to modify the default behavior of discovery and identification of objects classified as Unknown or as another category of systems are discovered and identified precisely as you require. HP SIM discovers and identifies the system and applies the new information when an Unknown system matches a rule set that you specify as the primary rule set. Furthermore, creating the new system type provides a System Link page for viewing the information returned from the system agent or from the communication protocol of SNMP or DMI.
T	
task	An executed instance of an HP SIM tool, on one or more systems or systems groups, with a specific set of arguments.
task scheduling	A master scheduling tool for the scheduling of polling, control, and notification tasks.
threshold	A preset limit that produces an event when the limit is reached or exceeded.
timed event	An action that schedules necessary events. Examples of events include backups, disk storage cleanup, and so on. The user defines the tools in this category.
Tomcat	An open source implementation of Java Servlet and JavaServer Pages technologies that is used by HP SIM as a web server.
tool	An application, command, or script that can be executed by HP SIM on one or more systems to perform a task.
tool category	An organizational structure for grouping tools. A tool must belong to one and only one category. Tool categories can only contain tools. They cannot contain other tool categories.
toolbox	A defined set of tools that a user might need for a particular task, such as database administration or software management. Each HP SIM toolbox is associated with a set of tools.
trap	An unsolicited message generated by a management agent that indicates that an event has occurred. For example, a monitored item has exceeded a set threshold or changed status. Previously called alarm. See Also event.
trap categories	Event collection systems found by event type. SNMP traps categorized by HP SIM into logical groups according to their functions.
trap forwarding address	The IP address of a system that has been specified to receive trap notifications forwarded by the HP SIM systems.
type	The classification of a system, which identifies it as a standard system type. The system types are client, cluster, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and other.

U

uncleared event status	<p>Events that have a Critical, Major, Minor, Normal, or Informational severity.</p> <ul style="list-style-type: none">• Critical. A failure has occurred, and immediate attention is required.• Major. A failure is impending.• Minor. A warning condition exists that can escalate into a more serious problem.• Normal. These events are not a problem.• Informational. No attention required. This status is provided as useful information
unknown status	<p>HP SIM cannot obtain management information about the system using SNMP or DMI. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting.</p>
user	<p>A network user with a valid login on the CMS that has been added to HP SIM.</p>
user accounts	<p>Accounts used to sign into HP SIM. These accounts associate a local Windows user account or a domain account with privilege levels and paging attributes inside HP SIM.</p>
user configuration page	<p>A page in HP SIM that provides the ability to create and define users that have access to the management application and associated rights.</p>
user group	<p>A group of users defined on the CMS operating system that has been added to HP SIM. Members of the user group in the operating system can sign into HP SIM.</p>

V

HP VCA log	<p>A listing of all the software maintenance tasks completed by the HP VCA and reports resulting from those tasks.</p>
version control	<p>Referred to as the HP VCRM installed on a Windows system for Windows and Linux ProLiant systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software Distributor can be launched from an HP SIM CMS against one or more installed HP-UX systems.</p>
Virtual Server Environment ()	<p>An integrated server virtualization offering for HP-UX, Linux, and Windows servers that provides a flexible computing environment maximizing usage of server resources. VSE consists of a pool of dynamically sizeable virtual servers; each can grow and shrink based on service level objectives and business priorities. For more information, go to http://hp.com/go/vse.</p>

W

WBEM Services	<p>HP WBEM Services for HP-UX is an HP product that uses WBEM and DMTF standards to manage HP-UX system resources.</p>
Web-Based Enterprise Management ()	<p>An Industry initiative to provide management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM compliant applications.</p>
Web-Based Enterprise Services ()	<p>A tool suite that is aimed at preventing or reducing the downtime of a system.</p>
Web-launch aware ()	<p>A run type for tools that are launched in a web browser using a web server. WLA tools can be designed to deal with multiple systems.</p>

Windows Management Instrumentation () workspace	An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled. The section of the GUI where tools are displayed.
X	
X client	An application or tool that appears on an X server. X clients can also be called X applications.
X server	A local application that accepts X client requests and acts on them.
X Window System	A cross-platform windowing system that uses the client/server model to distribute services across a network. It enables applications or tools to run on a remote computer.
XML document	A collection of data represented in XML.

Index

A

- access the graphical user interface, 68
- active time-out, 104
- add authorizations, 100
- add toolboxes, 100
- add users, 94
- All Tools toolbox, 11
- audit log, 13
 - configure, 105
- authorizations, 11
 - add, 100
- automatic discovery, 92
- automatic event handling, 97

B

- banner
 - customize, 70

C

- central management server
 - Custom install HP Systems Insight Manager on Windows, 27, 56
 - HP-UX system preparation, 35
 - install HP SIM on HP-UX, 36
 - install HP Systems Insight Manager on Linux, 41
 - Linux system preparation, 39
 - overview, 6
 - remove HP Systems Insight Manager on HP-UX, 66
 - remove HP Systems Insight Manager on Linux, 67
 - remove HP Systems Insight Manager on Windows, 66
 - requirements, 17
 - Typical install HP Systems Insight Manager on Windows, 25
 - Windows system preparation, 24
- certificate authority, 16
- CMS (see central management server)
- command line interface
 - log in, 72
 - security, 14
- commands, 72
- communication protocols (see management protocols)
- configuration
 - add authorizations, 100
 - add toolboxes, 100
 - add users, 94
 - audit log, 105
 - automatic event handling, 97
 - data collection CPU utilization, 104
 - discovery, 92
 - email settings, 96
 - lifetimes for Task Result entries, 106
 - managed system, 75
 - paging settings, 97
 - protocol settings, 91
 - time-out policy, 104

- configuration options, 104
- configuration rights
 - full, 12
 - limited, 12
 - no, 12
- configure email settings, 96
- configure paging settings, 97
- conventions, typographic, 2
- CPU utilization, 104
- custom install, 24
- customization options, 104
- customize the graphical user interface, 70

D

- data collection
 - performance, 104
- database, 13
 - remote for improved performance, 104
- default time-out period, 104
- default toolboxes, 11
- Desktop Management Interface, 15
- discovery, 92
- Distributed Task Facility, 15
- DMI, 15
- DTF, 15

E

- email
 - configure, 96
- event handling, 97

F

- features, 6
- firewalls, 16
- firewalls ports, 16
- first setup (see initial setup)
- frequently scheduled task lifetimes, 106
- full configuration rights user, 12

G

- getting started, 75
- graphical user interface
 - customize, 70
 - log in, 68
 - overview, 68
 - security, 14
- GUI (see graphical user interface)

H

- health status section, 68
- Home page
 - customize, 70
 - overview, 68
- HP Systems Insight Manager
 - commands, 72
 - features, 6

- HP Systems Insight Manager database, 13
- HP Systems Insight Manager Windows Installation, 24
- HP-UX CMS
 - installation and configuration, 36
 - remove HP Systems Insight Manager, 66
 - system preparation, 35
- HTTPS, 15

I

- in-place migration, 46
- initial setup, 75
 - add authorizations, 100
 - add toolboxes, 100
 - add users, 94
 - automatic discovery, 92
 - automatic event handling, 97
 - configure e-mail settings, 96
 - configure paging settings, 97
 - discovery, 92
 - managed systems, 75
 - manual discovery, 93
 - protocol settings, 91
- Insight Manager 7 comparison, 6
- install
 - central management server requirements, 17
 - managed system requirements, 20
 - process overview, 17
- install HP Systems Insight Manager
 - HP-UX CMS, 36
 - Linux CMS, 41
 - Windows CMS, 25

L

- last result task lifetimes, 106
- legend, 68
- lifetimes for Task Result entries, 106
- limited configuration rights user, 12
- Linux CMS

- installation and configuration, 41
- remove HP Systems Insight Manager, 67
- system preparation, 39

log in

- command line interface, 72
- graphical user interface, 68

M

- managed node (see managed system)
- managed system
 - discovery of, 92
 - overview, 6
 - protocol settings on the CMS, 91
 - requirements, 20
 - setup, 75
- management domain
 - overview, 6
- management protocols, 15
 - DMI, 15
 - HTTPS, 15
 - SNMP, 15

- SSH, 15
- WBEM, 15
- manpages, 72
- manual discovery, 93
- Microsoft SQL Server 2000, 13
- Microsoft SQL Server Desktop Engine (MSDE), 13
- monitor time-out, 104
- Monitor Tools toolbox, 11

N

- network client
 - overview, 6
- new features, 6
- no configuration rights user, 12
- node (see managed system)
- node group (see system group)

O

- Oracle, 13

P

- paging
 - configure, 97
- parameter
 - DataCollectionThreadCount, 104
 - EnableSessionKeepAlive, 104
 - LOG, 105
 - MX_JOB_CACHE_TIME_COMPLETED_JOBS, 106
 - MX_JOB_MAX_COMPLETED_JOB_AGE, 106
 - MX_JOB_MAX_COMPLETED_JOBS_PER_TASK, 106
 - MX_JOB_MIN_COMPLETED_JOBS_PER_TASK, 106
 - MX_LOG_FILEEXT, 105
 - MX_LOG_FILENAME, 105
 - MX_LOG_FILESIZE, 105
 - MX_LOG_QUEUE_SIZE, 105
 - MX_LOG_ROLLFILEEXT, 105
 - session-timeout, 104
- ports, 16
- PostgreSQL, 13
- protocol settings, 91
- protocols, 15

R

- remote migration, 46
- remove HP Systems Insight Manager
 - HP-UX CMS, 66
 - Linux CMS, 67
 - Windows CMS, 66
- repository (see database)
- requirements
 - central management server, 17
 - managed system, 20

S

- search, 68
- Secure HTTP, 15
- Secure Shell, 15
- security
 - access, 14

- certificate authority, 16
- command line interface, 14
- firewalls, 16
- graphical user interface, 14
- ports, 16
- self-signed certificates, 16
- Web server, 16
- X applications, 16
- self-signed certificates, 16
- Servicecontrol Manager 3.0 comparison, 6
- setup
 - add authorizations, 100
 - add toolboxes, 100
 - add users, 94
 - automatic event handling, 97
 - configure email settings, 96
 - configure paging settings, 97
 - discovery, 92
 - initial, 75
 - managed systems, 75
 - protocol settings, 91
- short and long task lifetimes, 106
- Simple Network Management Protocol, 15
- SNMP, 15
- spoofing, 16
- SSH, 15
- Storage Management Initiative Specification
 - storage, 102
- system group
 - overview (see)
- system key, 68

T

- Task Results Page
 - entry lifetime configuration, 106
- time-out policy
 - configuration, 104
- toolboxes, 11
 - add, 100
- tools, 12
 - command line, 12
 - Web, 12
 - X Window, 12
- types of tools, 12
- typical install, 24
- typographic conventions, 2

U

- Upgrading Insight Manager 7
 - data migration tool, 46
- users
 - add, 94
 - add authorizations, 100

W

- WBEM, 15
- Web Based Enterprise Management, 15
- Web server security, 16
- Windows CMS

- installation and configuration, 25
- remove HP Systems Insight Manager, 66
- system preparation, 24
- Windows Installation, 24

X

- X application security, 16