Getting started with HP SIM 5.2 in a smaller Windows environment

Introduction 3

HP SIM basics 4
- Product architecture 4
  - Central management server 4
  - Managed systems 5
  - Network clients 5
  - Systems and event collections 5
- Setting up custom collections 6
- Authorizations 6
- Secure access using a web browser 7

Managing HP ProLiant 100 series servers 7

Managing storage 7

Managing HP printers 8

Managing clients 8

Managing systems running HP-UX or Linux 8

Additional HP SIM capabilities 9
- Version Control 9
- Reporting 9
- Tool Definition Files 9
- HP SIM plug-ins 10

Installation overview and requirements in a Windows environment 10

Installing HP SIM on the CMS for the first time 17
- Installing HP SIM 17
- Populating the HP VCRM 19
- Signing in to HP SIM 19
- Using the First Time Wizard 20
- Setting up Windows managed systems 25
  - Configuring the managed system software using the Configure or Repair Agents feature from the CMS 26
- Setting up managed storage systems 34
  - Installing SMI-S providers 34

Verifying SSL 34
Configuring SMI-S providers 34
Configuring HP SIM to discover storage systems 34
Summary 35
Glossary 36
Additional resources 37

Introduction

HP Systems Insight Manager (HP SIM) is HP's unified server and storage management application that assists you in managing all HP servers, storage, and system hardware within your IT environment. HP SIM brings enterprise-level benefits to IT environments ranging from small networks to large corporate networks. Regardless of the size or complexity of your organization, HP SIM can help you be more efficient and proactive in identifying, diagnosing, and fixing potential issues for all of your HP hardware. For example, you can receive notification of drive issues that enable you to replace the drive under warranty before it fails.

HP SIM ships with all HP ProLiant 300, 500, and 700 series servers, HP XP, EVA, and MSA storage arrays, and is included in the HP-UX media releases, or it can be downloaded from http://www.hp.com/go/hpsim and implemented quickly. The default management capabilities enable you to auto-discover systems, monitor system health, deploy system software and firmware updates, and setup paging or e-mail notifications for pro-active notification of potential problems. HP SIM also includes a set of fully enabled licenses for value-added options such as patch management and performance management, which enable you to evaluate these additional capabilities on ProLiant systems. If you are responsible for managing printers, storage, and clients in addition to servers, HP SIM provides additional value through consolidated access to specialized tools for managing these systems.

HP SIM is easy to install and use. This paper guides you through the steps to install a basic HP SIM configuration in a Microsoft® Windows® environment. For more information about using HP SIM in other environments, visit the Information Library at:

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

This paper also describes some of the advanced capabilities of HP SIM that you can implement based on the needs of your organization.

Five things you should know about HP SIM:

- It is the only unified server and storage manager platform in the industry – it can manage servers, storage, desktops, printers, and networking equipment and interfaces with management tools for those systems.
- It can be installed and configured on a Windows XP desktop in less than one hour.
- The graphical user interface (GUI) is intuitive and easy to learn (no extensive training needed.)
- It provides fault and inventory management for a handful of systems up to thousands of systems.
- It includes free licenses for HP ProLiant Essentials Vulnerability and Patch Management Pack (VPM) and other HP ProLiant Essentials value-added plug-ins.

By default, HP SIM provides unified server and storage management including fault, inventory, and configuration management of all your HP servers and storage. Even if you have little or no experience using management tools, HP SIM can immediately help you become more proactive in detecting and solving system problems. HP SIM provides tangible benefits in a wide range of IT environments. For example:

Sam is an IT administrator in a small firm of lawyers. He manages 5 servers, 50 desktops, 2 storage arrays, 10 printers, and miscellaneous networking systems. He does not currently use management tools. If the lawyers have a problem with their systems, they quickly pick up the phone and call him. Sam does not think that his firm will invest in management tools and he is not sure that he has the time to learn the software. If Sam used HP SIM, he would receive an e-mail or pager notification of potential problems with server and storage components such as drives, CPU, and memory, enabling him to fix issues before the lawyers noticed and phoned him. Answering fewer crisis phone calls could save Sam much more than the time he would spend learning HP SIM. HP SIM would also help Sam to quickly locate information on his systems such as serial numbers, model numbers, and operating system levels as well as enable him to centrally track and update server BIOS, firmware, and agents. With the addition of the HP ProLiant Essentials Vulnerability and Patch Management Pack, he can even scan systems for security vulnerabilities, update operating system and application patches, and ensure that patches remain installed on the systems.

Wilma is an IT administrator in a small department within a large enterprise. She is responsible for managing the 20 Windows servers and 1 storage array in her local environment. She understands the benefits of HP SIM for the larger IT environment, but she thinks that it might be too complex and expensive for her small department. In fact, she prefers to use the old Windows console even though she knows that it does not support the newest ProLiant servers. First, Wilma needs to know that HP SIM can be installed on a desktop running Microsoft Windows XP Professional, and she can use Microsoft SQL Server Desktop Engine® (MSDE) as her database. MSDE ships with HP SIM at no additional charge and can be installed along with HP SIM. Because HP SIM is browser-based, Wilma is not tied to her Windows management console to get information on her servers and storage. She can sign in from any machine on the network and get secure access to her systems. This means that even if she is out of the office, she can still manage her servers and storage. Wilma will also be pleased to know that it is easy to update HP SIM. Instead of having to install a new console with every agent release, she only has to update event definitions in the console. She will save time and increase her efficiency as she learns how to make the best use of HP SIM features for updating her system software, running regular inventory reports, and more.

HP SIM basics

Product architecture

HP SIM can be described by a simple distributed architecture comprising three types of systems – a central management server (CMS), managed systems, and network clients. Authorized users can access the CMS through a web browser graphical user interface (GUI) from any network client running Internet Explorer or Mozilla. It also provides a command line interface (CLI) to allow scripted operations.

Central management server

Each management domain has a single CMS. The CMS runs the HP SIM software and initiates all central operations within the domain. The CMS can be a Windows, HP-UX, or Linux machine. However, this paper assumes that you install the HP SIM software on a Windows system. The CMS can be a server or a desktop PC that meets the hardware requirements specified in Installation overview and requirements in a Windows environment later in this paper.

HP SIM uses a database to store vital management domain information, including authorizations, systems, users, and more. HP SIM in a Windows environment supports MSDE or Microsoft SQL 2000®, Microsoft SQL 2005, and Oracle databases. SQL Server 2005 Express Edition is shipped standard with HP SIM and is usually sufficient to support an environment of up to 500 managed servers and storage devices. You do not need a Microsoft SQL server license to use SQL Express Edition.

Managed systems

A managed system is any system in the management domain that communicates with the CMS. Managed systems can include servers, desktops, workstations, storage, printers, laptops, hubs, storage systems, SANs, management processors, or routers with an IP or IPX address. To get the full capabilities from HP SIM, ProLiant servers should have one or more management agents installed. You can install the ProLiant Windows management agents onto ProLiant PL300 series servers and above directly from HP SIM (refer to Populating the HP VCRM). ProLiant 100 series servers and non-HP platforms can be managed using standards-based management protocols such as Windows Management Instrumentation (WMI) and SNMP. HP storage arrays/infrastructure and non-HP storage arrays are managed using standards-based management protocols such as SNMP, SMI-S (Storage Management Initiative Specification) and WBEM (Web-Based Enterprise Management.)

Network clients

You can access HP SIM from any network client. The network client can be part of the management domain and must be running a compatible browser to access the GUI or an SSH client application to securely access the CLI.

Systems and event collections

HP SIM enables you to group systems and events by attributes or by selecting individual systems using system collections. HP SIM comes with a standard set of system collections that logically group systems and events based on information in the HP SIM database, such as operating system, hardware platform, status, event type, and other criteria. In addition, you can create your own collections that enable you to automatically select systems or events from the database for specific tasks and monitoring actions. System collections are dynamic; anytime a system reflects the criteria of an existing collection, it becomes available in that collection.

To create a custom collection:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.

2. The **Customize Collections** page enables you to delete, copy, move, or edit existing collections or create new collections.

3. Click **New**.

4. Collection criteria are defined by logical operators and system properties, such as IP address range, total system memory, operating system type, system type, member, and so on. You can add as many criteria as needed to define your collection.

5. After you define the collection, click **Save As Collection** to save your collection in the appropriate location.

6. Test your new collection by selecting it from the **System and Event Collections** panel.

To successfully monitor and control managed systems, it is important to properly configure SNMP and agent security settings. The Configure or Repair Agents task makes it easy to configure these settings across groups of Windows, Linux, or HP-UX systems.

Click **Configure→Configure or Repair Agents**. Then configure SNMP and security settings as follows:

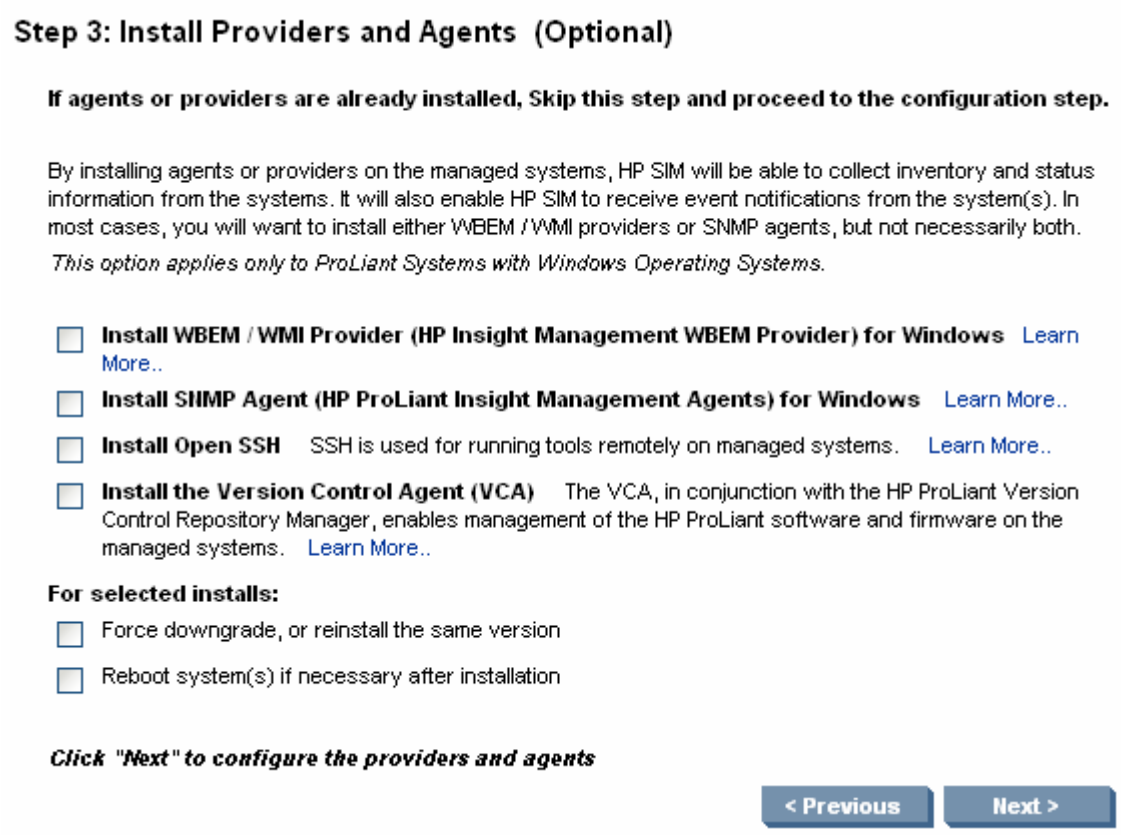
1. Select the collection or individual systems to be configured. If you created a custom collection in step 1 of the previous section, select the same collection.

2. Enter Windows login credentials. You must input a user name and password that allows HP SIM to login to the target systems. Click **Next**.

3. Input the required SNMP and security configuration information as indicated in Figure 1.

4. Click **Run Now**. After the task is completed, the **Task Results** page identifies which configuration operations have succeeded and which have failed.

Figure 1



Setting up custom collections

You can also create private collections (optional) by manually selecting systems. For example, you might want to group systems by location (servers on the seventh floor) or by owner (finance department systems). Each private collection displays a status icon representing the most critical status within the group, enabling administrators to identify problem areas at a glance.

Authorizations

Only users with a valid user ID and password on the CMS can access and perform tasks on a particular managed system or group of systems. Each user can perform tasks using the tools in a toolbox authorized for that particular user. There are four default toolboxes in HP SIM including the **All Tools** toolbox and the **Monitor Tools** toolbox. Users who are authorized to use the **All Tools** toolbox can perform all administrative tasks and can change the state of managed systems. Occasional users or non-experts should be authorized to use only the **Monitor Tools** toolbox. This paper assumes that you have a small number of authorized users and use only the default toolboxes. Note that toolboxes and authorizations can be customized for environments with larger numbers of users and different security needs for different managed systems.

Secure access using a web browser

When you access HP SIM from a web browser, you must sign in using a secure sockets layer (SSL) connection. Your user name and password for HP SIM is the same as your login credentials for the Windows operating system running on the CMS. HP SIM uses operating system security and SSL to ensure strong authentication and data encryption and to minimize the risk of unauthorized access to the management console.

Managing HP ProLiant 100 series servers

The HP ProLiant 100 series servers do not support HP Insight Management Agents. Therefore, HP SIM collects data from ProLiant 100 series servers through Windows Management Instrumentation (WMI), which provides basic system inventory reporting. Not all data available in standard WMI is shown or reported in HP SIM.

You should be able to view the following information:

- ROM-based SMBIOS tables populated by the ROM during Power On Self Test (POST)
- Operating system-based information including MAC addresses, IP addresses, domain, operating system version and serial number, last boot time, current running processes, and disk information
- Standard operating system driver information including network, and logical and physical drive storage (from the operating system point of view)
- HP SIM also provides status polling of ProLiant 100 series servers

Managing storage

HP SIM has been significantly upgraded to manage storage devices it supports through the SMI-S (Storage Management Initiative Specification) standards-based interface. SMI-S complemented with SNMP enables HP SIM to detect and configure storage systems including Fibre Channel-based storage arrays and tape libraries, hosts with HBAs, and Fibre Channel switches. Storage devices and Fibre Channel infrastructure devices are discovered, events are monitored, and data is gathered for proactive management and asset reporting.

Specific storage data collection includes vendor, model, device status, array capacity, disk RAID type, port information, LUN information, firmware level, network addresses, part numbers, and component serial ID's.

HP SIM in conjunction with the HP Insight Management Agents discovers and monitors Modular Smart Array (MSA) series storage attached to ProLiant servers. HP SIM tracks physical and logical configurations and receives prefailure alerts in a manner consistent with internal storage resources. HP SIM also discovers and launches Command View EVA and Command View XP storage arrays and launches the array management software running on hosts managed by HP SIM.

In addition, the HP ProLiant Essentials Performance Management Pack (PMP) 4.x (where x is the minor PMP version, for example, 4.1 or 4.2) integrates seamlessly with HP SIM to provide hardware bottleneck analysis for MSA storage. PMP provides the required tools to receive proactive notification of developing bottleneck conditions, and debugs existing performance issues on MSA500/MSA1000 shared storage devices. PMP 4.x is automatically installed with HP SIM 5.0 and later.

For value-added storage management functionality such as automated storage provisioning, application management, and chargeback, the HP Storage Essentials suite offers a full set of modules which can be deployed individually or as a set. Each of the modules is tightly integrated with HP SIM, ensuring single sign-on, UI integration, common discovery and reporting. For more information on HP Storage Essentials visit www.hp.com/go/storageessentials.

Managing HP printers

You can integrate HP Web Jetadmin with HP SIM to extend its management capability to include printers. The integration of HP Web Jetadmin and HP SIM provides:

- Integrated server and printer discovery with printer drill down. HP SIM enables you to easily discover a wide variety of printers, drill down on a specific printer, and launch the HP Web Jetadmin device status page to troubleshoot or manage a printer.
- Easy access to the HP Web Jetadmin console from HP SIM. You can launch the full HP Web Jetadmin application from the HP SIM menu, enabling quick and seamless access between the tools.

For links to more information, including a technical white paper and an overview to HP Web Jetadmin, go to http://h10010.www1.hp.com/wwpc-JAVA/offweb/vac/us/en/en/network_software/wja_sysinsight_manager.html.

Managing clients

The HP Client Manager Connector for HP SIM enables you to consolidate deployment and management of HP clients and servers within a single HP SIM console. This software extends the core functionality of HP SIM with HP client hardware management and provides access to additional Altiris client lifecycle management functionality.

- You can use the HP Client Manager Connector to:
- Discover and monitor the health of HP clients
- Manage system software updates for HP clients
- Deploy new client systems through an integrated deployment wizard
- Remotely troubleshoot HP client problems using in-depth diagnostic reports

Note: You cannot install the Altiris Notification Server and the HP Client Manager Software on a system running the Vulnerability and Patch Management Pack due to conflicting IIS settings. The Altiris Notification Server and the Vulnerability and Patch Management Pack can be installed on systems other than the HP SIM system.

For more information, go to HP Client Management Solutions.

Managing systems running HP-UX or Linux

This paper focuses on the management of Windows systems but HP SIM can also manage HP-UX and Linux systems.

For more information about HP-UX management capabilities and Integrity systems, refer to www.hp.com/go/integrityessentials . For information about HP-UX CMS and managed system software for Virtual Server Environment (VSE) technologies refer to http://hp.com/go/vse.

For more information on the Linux agents for managed systems, go to http://h18004.www1.hp.com/products/servers/linux/value-add-software.html.

Additional HP SIM capabilities

HP SIM provides a rich set of functionality to help you be more effective in the management of your IT environment. After you have completed the basic setup described later in this document, consider adding the capabilities described below. For more information, refer to the HP SIM User Guide at http://www.hp.com/go/hpsim or on the HP ProLiant Essentials Foundation Pack Management CD (Management CD).

Version Control

Version Control can save time and support costs by ensuring the consistency of your server system software. HP SIM catalogs HP system software such as BIOS, system drivers, Insight Management Agents, HP utilities, and firmware on managed systems, and compares them to the latest available from HP or with a standard baseline set that you define. The system software and the baseline definitions are stored in a Version Control Repository on the CMS. You can configure the HP Version Control Repository Manager (HP VCRM) to automatically retrieve the latest software and firmware from http://hp.com. You can also schedule regular updates and regular automatic comparisons of the system software on a managed system with that in a selected baseline set. You are alerted of discrepancies so that you can use HP SIM to schedule an update of a system or groups of systems. For more information, refer to the HP SIM User Guide at http://www.hp.com/go/hpsim or on the Management CD. For more information regarding Version Control, refer to the manuals at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

Note: This paper describes how to install and populate the Version Control Repository Manager to assist in the initial deployment of the ProLiant Support Pack for Windows to multiple managed systems. To learn how to set up version control in its entirety, refer to the User Guide mentioned previously.

Reporting

HP SIM collects comprehensive system data, enabling you to quickly produce detailed inventory reports on an ad-hoc or regular basis. Reports can be saved in HTML, XML or exported to CSV format for easy incorporation into popular reporting packages, making those monthly reports to management a snap! And, HP SIM makes it easy to identify systems that might need CPU or memory upgrades before migrating to the latest operating system. For more information, refer to the HP SIM User Guide at http://www.hp.com/go/hpsim or on the Management CD.

Tool Definition Files

Tool definition files enable you to launch tools on a managed system from the HP SIM menu. Tool definition files are useful if you have developed your own scripts or in-house applications to assist in administrative tasks. Tool definition files are simple XML documents that describe the type of tool to be run, such as command line or web launch, and the title and location of the new menu item. A tool definition file can also specify any restrictions such as device filters or operating system filters. For more information, see the HP SIM User Guide at http://www.hp.com/go/hpsim or on the Management CD

HP SIM plug-ins

HP SIM plug-in applications improve lifecycle management of HP hardware resources and extend the breadth of device coverage of HP products in your IT environment. Choose from a growing list of HP management tools that plug into HP SIM enabling you to:

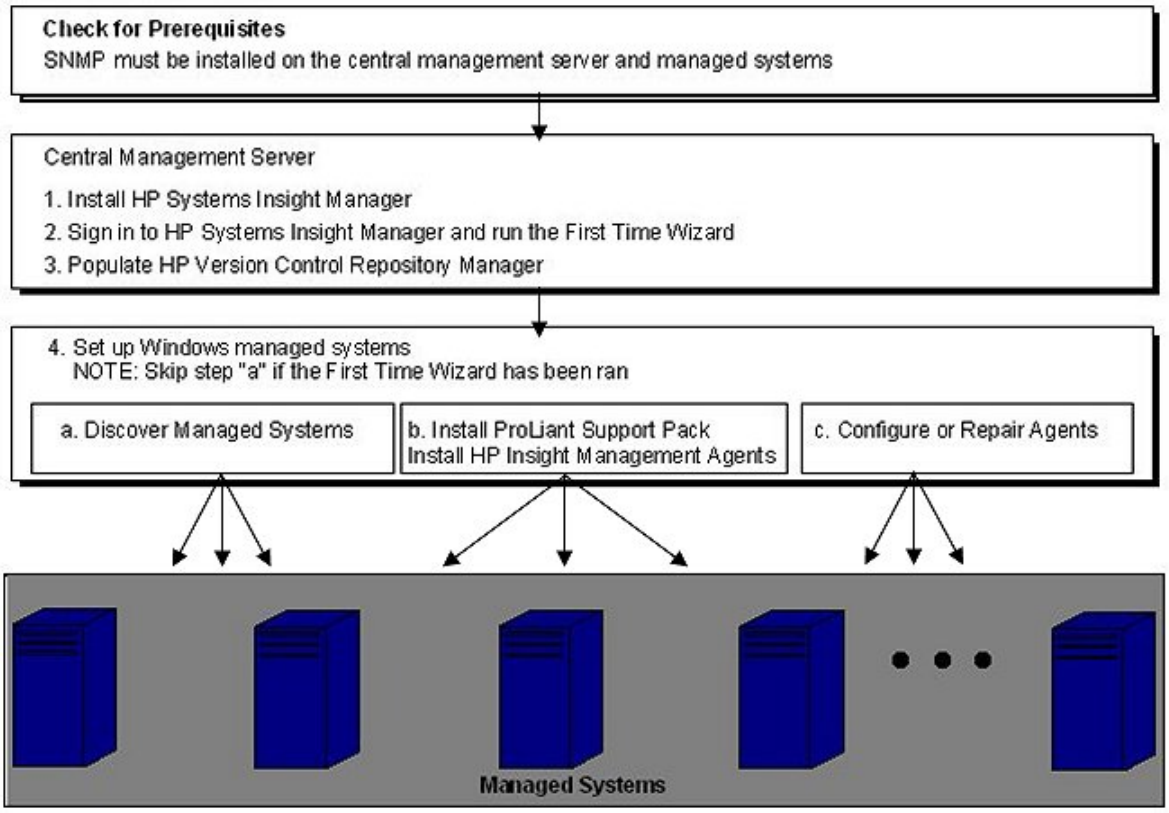
- Access HP infrastructure management tools from a single console
- More efficiently deploy and manage HP systems
- Consolidate event management and notification services for HP servers, storage, printers, clients, power and other devices in a single management tool.
- Have more control and flexibility through modular, extensible, and standards-based management that can be adapted to meet the needs of your environment. For more information about plug-ins, go to:
    - www.hp.com/go/hpsim
    - www.hp.com/servers/proliantessentials
    - http://h18006.www1.hp.com/products/storage/software/e-suite/index.html

Installation overview and requirements in a Windows environment

HP SIM is available for download from the HP (hp.com) website and ships at no extra charge with all ProLiant 300, 500, and 700 series servers, and StorageWorks products. The GUI is intuitive and easy to learn so you do not need extensive training to start using it.

Figure 2 shows a representation of the HP SIM installation process. First, you must ensure that SNMP, MDAC2.7 SP1 and TCP/IP is installed on the system that hosts HP SIM and on all managed devices. After you install the HP SIM software on the host system, this system becomes the CMS. Next, install and configure management protocols and desired Management Agents on managed systems. The only management protocol required on managed systems for HP SIM to function properly is SNMP. Management protocols such as WMI and SSH are not required but can augment the capabilities of HP SIM.

Figure 2



The hardware, software, and networking requirements for HP SIM in a Windows environment are shown in **Error! Reference source not found.**. These requirements are separated by system type for the CMS, managed systems, and network clients. See HP SIM basics for more information.

System requirements

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

Windows Central Management Server

- This section contains the minimum requirements for the Windows operating system that is used for the CMS.

Operating system	Hardware	Software	Networking
Microsoft Windows Server 2008 Standard and Enterprise for x86 and x64 (32-bit mode) Microsoft Windows Server(TM) 2003 Standard and Enterprise for x86 and x64 (32-bit mode) with Service Pack 2	Any HP ProLiant x86 or x64 system with the following configuration: Minimum: 1.5-GHz processor with 1 GB RAM 500 MB free disk space recommended Recommended: 2.4-GHz	Database software: SQL Server 2005 Express Edition with Service Pack 2 **Note:** SQL Server 2005 Express Edition	Static or dynamic host name resolution TCP/IP SNMP

Operating system	Hardware	Software	Networking
Microsoft Windows Vista Microsoft Windows Server 2003 R2 Enterprise for x86 and x64 (32-bit mode) with Service Pack 2 Microsoft Windows 2003 SMB for x86 with Service Pack 2 Microsoft Windows XP Professional with Service Pack 2 VMware ESX v3.0.01 or later running guest on x86 The Central Management Server supports Microsoft Windows 2000 and 2003 International Server - French, German, Italian, Spanish, and Japanese (latest service pack available for each language).	processor with 1.5 GB RAM **Note:** If Microsoft SQL Server is installed on the CMS, an additional 500 MB of RAM should be installed. **Note:** HP Netserver platforms can be used for the Central Management Server as long as the Instant Toptools software is not installed and all other requirements are met.	requires .NET 2.0 Framework installed. **Note:** SQL Server 2005 Express Edition supports 500 systems and 5,000 events. Microsoft SQL Server 2005 with Service Pack 2 (remote or local) **Note:** Microsoft SQL Server 2005 supports 5,000 systems and 50,000 events. Microsoft SQL Server 2000, Standard or Enterprise Edition with Service Pack 4 (remote or local) Oracle 9i Standard or Enterprise Oracle 10g Browser software: Microsoft Internet Explorer 7.0 Microsoft Internet Explorer 6.0 with Service Pack 2 Firefox 1.5.0.12 Firefox 2.0.0.4	

Note: HP SIM 5.2 can run on a Windows Virtual Machine (VM) provided the following requirements are met. The VM must be hosted on an ESX 3.0.1 or later server and the VM configuration must meet HP SIM hardware requirements and the CPU and Memory resources allocated to this VM must be always available to this VM (by reserving CPU and Memory resources).

Note: HP Integrity VMs do not support running an application at the same level as the host.

Note: HP Service Essentials Remote Support Pack, including the Remote Support Software Manager, is NOT supported on Virtual Machines.

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

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: Service Essentials Remote Support Pack (Remote Support Pack) is not supported on Windows XP Professional. If you install HP SIM on Windows XP Professional, you cannot use Remote Support Pack.

Note: Microsoft SQL Server 2005 is only supported if HP SIM is running on Windows Server 2003.

Note: You cannot run Internet Explorer 6.0 and Internet Explorer 7.0 simultaneously. However, if you uninstall Internet Explorer 7.0, Internet Explorer 6.0 is restored.

Managed system requirements and recommendations

This section contains requirements and recommendations for managed systems.

Operating systems

Windows managed systems

- Microsoft Windows Server 2008 Standard or Enterprise for x86 and x64 (32-bit mode)
- Microsoft Windows Server 2008 Standard or Enterprise Core for x86 and x64 (32-bit mode)
- Microsoft Windows Server 2008 Datacenter, Datacenter Core, Web Edition, and for Itanium-based systems
- Microsoft Windows Server(TM) 2003 R2 Standard or Enterprise for x86 with Service Pack 2 and x64
- Microsoft Windows Server 2003 R2 DataCenter with Service Pack 1 or later
- Microsoft Windows 2003 Standard with Service Pack 1 or later
- Microsoft Windows 2003 Standard for x64 with Service Pack 2
- Microsoft Windows 2003 Standard and Enterprise for x86 and x64 with Service Pack 2
- Microsoft Windows 2003 Web Edition for x86 with Service Pack 1 or later
- Microsoft Windows 2003 Small-Medium Business for x86 with Service Pack 1 or later
- Microsoft Windows 2003 SMB Business for x86
- Microsoft Windows 2000 Datacenter for x86

- Microsoft Windows 2000 Server with Service Pack 1 or later for x86
- Microsoft Windows 2000 Server and Advanced Server with Service Pack 4 for x86
- Microsoft Windows NT4 with Service Pack 6
- Microsoft Windows Vista Client
- Microsoft Windows XP with Service Pack 1or later
- Microsoft Windows Virtual Server
- VMware ESX v3.0.01 or later running guest on x86
- Integrity Virtual Machine for Windows running guest on Windows
- VMware GSX

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

HP-UX managed systems

- HP-UX 11i v3 (IA/PA)
- HP-UX 11i v2 Update 2 (IA/PA)
- HP-UX 11i v2 (IA only)
- HP-UX 11i
- Integrity Virtual Machine HP-UX running guest on HP-UX 11i v2 and v3

Linux managed systems

- Red Hat Linux 9
- Red Hat Linux 8
- Red Hat Linux 7.3 Workstation
- Red Hat Enterprise Linux 5 for x86 with Update 1, AMD64 and EM64T with Update 1, and Itanium-based systems
- Red Hat Enterprise Linux 4 x86 with Update 6, AMD64 and EM64T with Update 6, and Itanium-based systems
- Red Hat Enterprise Linux 3 x86 with Update 9, AMD64 and EM64T with Update 9, and Itanium-based systems
- SUSE Linux Enterprise Server 10 for x86, AMD64 and EM64T with Service Pack 1, and Itanium-based systems
- SUSE Linux Enterprise Server 9 for x86 with Service Pack 4, AMD64 and EM64T with Service Pack 4, and Itanium-based systems

- SUSE Linux Enterprise Server 8 for United Linux 1.0 and Itanium-based systems
- Integrity Virtual Machine Linux running guest on Linux
- VMware GSX
- VMware ESX 3.5

Note: Operating systems with only IPX enabled are not identified by an HP-UX or Linux Central Management Server.

Novell managed systems

- Netware 6.5
- Netware 6.0

SUN managed systems

- Solaris 9 Intel Platform
- Solaris 8 Intel Platform

IBM managed systems

- OS/2

HP managed systems

- Tru64
- NSK
- OpenVMS

Hardware

- For HP-UX:
- Any HP PA-RISC system
- Any HP Itanium®-based system
- For Windows:
- Any HP x86 system
- Any HP x64 system
- For Linux:
- Any HP x86 system
- Any HP x64 system
- Any HP Itanium-based system

Software

- This software is not required, but if you want improved management capabilities, HP recommends that you install these components.
- For Windows:
- OpenSSH Services 4.3p2
- ProLiant Support Pack 6.30 or later
- WBEM/WMI
- SNMP (recommended as an alternative to WBEM)
- WBEM (for Integrity systems only)
- 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

Required web browsers

For Windows:

- Microsoft Internet Explorer 6 (with Service Pack 2) or later
- Firefox 1.5.0.12
- Firefox 2.0.0.4

  Note: For optimum performance, the minimum resolution for the browser should be 1024 x 768.

For HP-UX:

- Firefox 1.5.0.12
- Firefox 2.0.0.4

For Linux:

- Firefox 1.5.0.12
- Firefox 2.0.0.4

  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), see 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 local installation on the CMS.

- Custom tools on the Tools menu require SSH on the Central Management Server to run properly. These commands run on the Central Management Server with environment variables set to the context of specific events or devices. SSH on the Central Management Server is also used by the Initial ProLiant Support Pack Install on the Deploy->Deploy Drivers, Firmware and Agents menu.

- You can 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 OpenSSH 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. If SSH is not configured on the client, then command line tools, any HP SIM plugins that require SSH, and Configure or Repair Agents do not work properly.

Installing HP SIM on the CMS for the first time

You can install HP SIM from the Management CD or download a self-extracting file available from http://www.hp.com/go/hpsim. The following procedure is for installing HP SIM from the HP ProLiant Essentials Foundation Pack Management CD that ships with HP ProLiant servers.

Installing HP SIM

By default, the Typical installation includes HP SIM, the SSH Server, the WMI Mapper, HP Performance Management Pack, System Management Homepage (HP SMH), Virtual Machine Management Pack , HP Server Migration Pack and HP VCRM (see Table 1). If you do not want to install a particular component at this time, use the Custom installation. You can re-run setup.exe at any time and use the Custom installation to load the component.

Table 1

Installation Component	Typical Installation	Custom Installation
System Management Homepage	✓	✓
OpenSSH for Windows 3.7.1p1-1	✓	Optional
WMI Mapper	✓	Optional
HP Systems Insight Manager	✓	✓
HP ProLiant Essentials Performance Management Pack	✓	Optional
HP Version Control Repository Manager	✓	Optional

HP ProLiant Essentials Virtualization Management Software	✓	Optional
HP SIM Installation Information	✓	Optional

Note**:** Before you proceed with the custom install, if you are going to install ProLiant Essentials Performance Management Pack, HP ProLiant Essentials Virtual Machine Management Pack, or the HP SMH, refer to the following documents for specific username requirements for the product administrator, service account and DB administrator.

For more information refer to the:

- HP 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

General steps to install components:

1. Insert the HP ProLiant Essentials Foundation Pack Management CD in the CD-ROM drive. The installer autorun screen appears listing the contents in the Products tab.
2. Click **Install** on the HP SIM page. Then select **Install** located next to the HP SIM (Windows) listing to launch the Installer.
3. The **HP SIM Installer** screen appears. Click **Install**. This portion of the installation checks for previous versions of HP SIM running on the system and initiates an upgrade process if one is found.
4. If no previous versions of HP SIM are found, the core HP SIM installer starts. Click **Next** to begin the HP SIM installation.
5. If no database is detected on the local system, the installer provides an option to install SQL Server Express 2005. If you plan to install the database locally, select the **Install SQL Express** option, enter password for the administrator, and click **Next**. If you plan to connect to a remote database, enter the database host name, domain name of the database host, database name, and password for accessing the database. Click **Next**.
6. After the SQL Server Express 2005 installation has completed, **Select installation Type** is displayed.
7. Under **Select Installation Type**, select **Custom** if you want to deselect a component or change individual component settings for the drive, installation directory, or program group. If you perform a **Typical** installation, the packages selected by the installer by default will be installed. Refer to the HP SIM Installation and Configuration Guide for Microsoft® Windows on the Management CD for assistance.
8. When you are prompted for your account credentials, enter your login password. Click **Next**.
9. The **Install Summary** screen appears. Click **Install**.

   The components are installed sequentially, and the status of each component installation appears. Installation times vary depending on the speed of the host server processor. After all components have been installed, they have an installed status. See the section Populating the

HP VCRM below for more information on configuring the Version Control Repository Manager during installation. Click **Next**. The **Registration** page appears. Enter the product key for HP SIM in the given fields and click **Register Now**. Click **Register Later** if you want to register later.

10. The **Installation Complete** page appears. The page includes a link attached with the page to view more information regarding Version Control. You must reboot the server after installation. Select **Yes, reboot this system now** and click **Finish** to reboot the server, or select **No, I will reboot later** and click **Finish** to reboot later..

11. In the **HP Systems Insight Manager Setup** screen, click **Finish**.

12. Restart the HP Systems Insight Manager host system.

Populating the HP VCRM

The HP VCRM is a repository that stores the software and firmware components used to support ProLiant servers on Windows and Linux platforms. By default, the HP VCRM is installed on the HP SIM central management server; however, you can specify a custom directory or server location.

You can use the HP VCRM as a central point to define software baselines and to automate the installation and change management of HP software and firmware updates to production systems.

The automatic update feature of the HP VCRM is the preferred solution for updating repositories automatically. The automatic update feature of the HP VCRM keeps servers connected to HP for proactive delivery of the latest HP ProLiant and Integrity Support Packs and components directly to a specified repository. You can configure the automatic population of the repository during the HP VCRM installation or after installation. In the event you cannot use the automatic update feature, you can populate the repository from the HP SmartStart CD.

Signing in to HP SIM

1. After the system restarts, test the installation by signing in to HP SIM using one of the following methods:

   - If you are browsing locally, double-click the **HP SIM** icon on the Windows desktop.

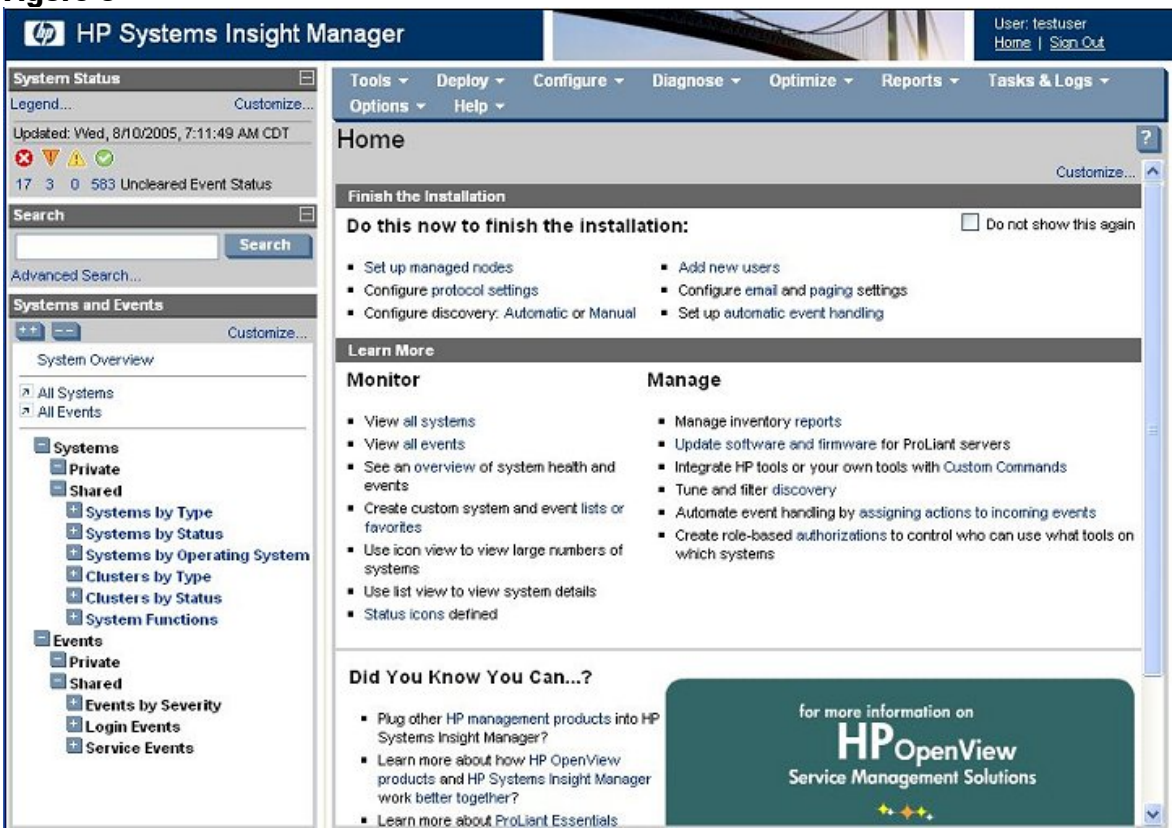
   - If you are browsing remotely, type **HTTPS://CMSMachineName:50000** in the Address bar (where CMSMachineName is the name of your CMS).

   Note: After you restart the CMS, it might take a few minutes for the HP SIM HTTP server to initialize.

2. Enter the user credentials that you provided during the installation; the HP SIM GUI (Figure 3) appears. The **System and Event Collections** panel on the left side of the user interface is pre-populated with a number of default system and event collections. For a complete description of these collections, refer to the HP SIM User Guide in the HP SIM Information Library at http://www.hp.com/go/hpsim.

[3] During the installation of MSDE, you might be asked to restart the system. If so, restart the system and restart the HP SIM installation process. You are not asked to install MSDE when you re-start the installation process.

Figure 3



Using the First Time Wizard

The First Time Wizard is automatically launched the first time a user with administrative privileges signs in to HP Systems Insight Manager (HP SIM). The administrative account used to install HP SIM is the initial administrative account. If the wizard is canceled before completion, it restarts each time an administrative user signs in. You can cancel and disable the wizard from starting automatically by selecting the Do not automatically show this wizard again checkbox and clicking Cancel. The wizard can be started manually by selecting Options->First Time Wizard.

The First Time Wizard provides step-by-step instructions for performing the initial configuration of HP SIM. Additional configuration options are available in the HP SIM GUI.
The First Time Wizard helps you configure the following settings on the Central Management Server (CMS). After configuring a setting, click Next to continue the First Time Wizard setup procedure. The First Time Wizard does not apply any changes until you click Finish on the Summary page.

Note: The default settings in Firefox block the First Time Wizard. You must disable the pop-up blocker in Firefox to see the First Time Wizard.
Note: The selections you make in the First Time Wizard are not applied until you click Finish on the summary page.

The First Time Wizard includes the following options:

- **Introduction**. Describes the purpose of the First Time Wizard. You can cancel the First Time Wizard and disable the wizard from automatically starting when an administrative user signs in.
- **Managed Environment.** Specifies all operating systems to be managed by the Central Management Server (CMS). The selections made here configure HP Systems Insight Manager

(HP SIM) to show collections, tools, and reports only for managed environments that are selected.

- **WBEM.** . Enter the default Web-Based Enterprise Management (WBEM) user names and passwords. This information is used to discover systems that use the WBEM management protocol.
- Enter the mapper proxy system host name and port number to communicate with Windows systems using Windows Management Instrumentation (WMI).
- **SNMP.** Enter the read community strings to use for all newly discovered systems. Community strings establish the authentication that enables communication between HP SIM and a managed system. This information is required to discover systems that use the SNMP management protocol.
- See the HP Systems Insight Manager 5.2 User Guide at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html for more information about WBEM and SNMP.
- **Discovery.** Use the wizard to enable discovery, set up the discovery schedule, and enter the IP address ranges or host names of the systems you want to discover. Discovery is the process HP SIM uses to find and identify systems on your network and populate the database with that information. A system must be discovered to collect data and track system health status.
- **Configure Managed Systems.** Configure managed systems as they are discovered, by configuring WBEM and Windows Management Instrumentation (WMI), SNMP, Secure Shell (SSH) access, and trust relationship.
- **E-mail.** Enter the e-mail settings that the CMS will use to send e-mail notifications. You can set up Automatic Event Handling tasks that prompt HP SIM to send e-mails when the CMS receives a specific event.
- **Summary.** Displays all First Time Wizard settings with the option to modify settings or to finish the First Time Wizard.

  Note: The First Time Wizard configures only the basic settings of HP SIM.

Configuring the managed environment

From this page, select the operating systems that the Central Management Server (CMS) will manage. There are four options: Windows, Linux, HP-UX, and Other. The selections made here configure HP Systems Insight Manager (HP SIM) to hide collections, tools, and reports for operating systems you do not use. By default the CMS operating system is selected on this page.

Note: These settings can be changed at any time, and the hidden collections, tools, and reports can be made visible again. To change these settings from the HP SIM menu, select Options-> Managed Environment.

1. Select the operating systems for the CMS to manage.
2. Click **Next** to go to the next First Time Wizard step, or click **Previous** to return to the previous step.

Entering WBEM settings

HP Systems Insight Manager (HP SIM) uses the C:\hpsim\Peabody\doc\docs\source\en\winUG\single-nonhp\hpsim-WindowsuserGuide.html - d0e18802#d0e18802Web-Based Enterprise Management (WBEM) protocol to communicate with managed systems. You can enterWBEM settings in the First Time Wizard or from the HP SIM

menu bar. To disable WBEM communication or enter settings in the GUI, select Options->Protocol Settings->Global Protocol Settings from the HP SIM menu.

If you do not have WBEM systems in your network, you do not need to enter information here. If you have WBEM systems and you do not enter the user names and passwords for these systems, HP SIM will not discover them.

Note: See the HP Systems Insight Manager 5.2 User Guide at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html for more information about fine tuning protocol settings for a single system or a group of similar systems.

To enter WBEM settings using from the First Time Wizard WBEM page:

1. In the **User name**, **Password**, and **Confirm password** fields, enter a default user name and password as needed. To add additional default user name and password pairs, click **Add**. To delete user name and password pairs, click **Delete**. These defaults apply to all newly discovered systems.
    - HP recommends limiting WBEM user name and password pairs to 10 to reduce the overall discovery run time. To add more than 10 WBEM user name and password pairs, run the **mxnodesecurity -a -p wbem -c** username:password command for each additional set. You can also create an XML file that defines your system authorizations before running discovery.
    - If your network includes storage systems, enter the user name and password of each SMI CIMOM in this section. For example, if you have an HP host bus adapter (HBA) (Emulex OEM) for Windows, enter the user name cimadmin and password pwd580. See your storage system's SMI-S provider documentation for information about the SMI CIMOM user name and password.
    - The system identification process attempts each user name and password pair until a successful response is obtained. Future WBEM requests to a system will use the user name and password that succeeded the system identification process. For Windows-based systems, the user name must include the domain name, for example, domainname\username.
    - Enter the user 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.
2. In the **WMI Mapper Proxy** section, enter the mapper proxy **Hostname** and **Port Number**. If a WMI Mapper Proxy has already been discovered, it appears here. If you have selected not to manage Windows systems on the previous page, this section is not displayed.
3. To go to the next **First Time Wizard** step, click **Next**, or to return to the previous step, click **Previous** to return to the previous step. The users that are used for WBEM access do not need to be configured to sign-in.

Entering SNMP settings

HP Systems Insight Manager (HP SIM) uses SNMP to communicate with managed systems. Community strings establish the authentication that enables communication between HP SIM and a managed system. You can enter read community strings in the First Time Wizard, or from the HP SIM menu bar. To disable SNMP communication, enter community strings, or control other SNMP settings not available in the wizard, select **Options->Protocol Settings->Global Protocol Settings** from the HP SIM menu.

If you do not have SNMP systems in your network, it is not necessary to enter information here. If you have SNMP systems and you do not enter read community strings that match these systems, HP SIM does not discover them.

See the HP Systems Insight Manager 5.2 User Guide at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html for information about fine-tuning protocol settings for a single system or a group of similar systems.

To enter SNMP settings from the First Time Wizard SNMP page:

1. In the **Read community string** field, enter up to 10 read community strings. This value is case-sensitive. The identification process attempts communication with a 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. If you have SNMP systems and no read community string that match the systems are entered, the systems will not be discovered.
2. To go to the next **First Time Wizard** step, click **Next**, or to return to the previous step, click **Previous**.

Enabling automatic system discovery

HP Systems Insight Manager (HP SIM) uses automatic discovery to find and identify systems on the network. The System Automatic Discovery task is the default discovery task and is disabled by default. You can enable and configure the System Automatic Discovery task in the First Time Wizard, or by selecting **Options->Discovery** from the HP SIM menu.

If the System Automatic Discovery task is enabled, it runs immediately when the First Time Wizard is finished to initially populate the HP SIM database.

You can create additional automatic discovery tasks by selecting **Options->Discovery** from the HP SIM menu and entering the details, and you can also run manual discovery to discover single systems.

To enable automatic system discovery from the First Time Wizard Discovery page:

1. To configure HP SIM to run discovery immediately after you finish the First Time Wizard, select **Run discovery** once after wizard finishes.
2. To configure the System Automatic Discovery task to run on a regular schedule, select **Schedule** and enter the periodic run interval and time of day to run the task.
3. In the **Ping inclusion ranges**, system (hosts) names, templates, and/or hosts files field, specify the IP addresses to include for pinging. If you want to use this task to discover SMI-S storage systems, include the IP address of each SMI CIMOM. You can also enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. To use an existing hosts file, enter the hosts file name in the following format: **$HostsFileName** .
    - To discover SMI-S storage systems, you must add the IP address of each SMI CIMOM to the System Automatic Discovery task.
    - Alternatively, you can create a separate discovery task for your SMI CIMOMs. See the HP Systems Insight Manager 5.2 User Guide at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html for more information.

4. To go to the next **First Time Wizard** step, click **Next**, or to return to the previous step, click **Previous**.

Configuring managed systems

The Configure Managed Systems page in the First Time Wizard enables you to configure managed systems as they are discovered and to specify parameters for running the Configure or Repair Agents. All steps are optional and can be configured from the HP SIM Options menu at a later time. To skip this step, click **Next** to go to the next First Time Wizard step.

To configure managed systems from the First Time Wizard Configure Managed Systems page:

1. To use the First Time Wizard to configure managed systems when they are first discovered, select **Configure newly managed system**s when Discovery runs for the first time.
2. Enter the user name and password pair for an administrative user account on the managed systems.
3. Under Configure WBEM/WMI, select from the following:
    - **Create subscriptions for WBEM events.**
    - **Send a test WBEM or WMI indication to this instance of HP Systems Insight Manager to ensure that events appear in HP Systems Insight Manager events lists .**
    - **Deploy HP Systems Insight Manager WBEM certificate to the target systems to support client certificate authentication.**

      This option does not appear if there are no managed HP-UX systems.
4. Under Configure SNMP, select from the following:
    - **Set read community strings.**

      This string is pre-populated with settings from the SNMP page of the First Time Wizard.
    - **Set traps to refer to this instance of HP Systems Insight Manager.**
    - **Send a test SNMP trap to this instance of HP Systems Insight Manager to make sure events appear in the HP Systems Insight Manager events lists.**
5. Under Configure secure shell (SSH) access, select from the following:
    - **Host based authentication.**
    - **Each user has to be authenticated on the managed system.**
6. Select **Trust relationship** to set a trust relationship between managed systems and the Central Management Server (CMS).
7. To go to the next **First Time Wizard** step, click **Next**, or to return to the previous step, click **Previous**.

Configuring e-mail settings

To use the First Time Wizard to configure HP SIM to send e-mail notifications through automatic event handling:

1. Enter the **SMTP host name**. The SMTP host is the outgoing e-mail server that the CMS uses to send e-mail notifications.
2. In the **Sender's e-mail address** box, enter the e-mail address that the management server uses when sending e-mail notifications.
3. (Optional) Select **Send test email** and enter recipients e-mail address. Click **Send test email now**.
4. To authenticate your SMTP server, select **Server Requires Authentication**.
5. Enter the account user name and password in the corresponding boxes.

   Note If you did not enter a valid Simple Mail Transfer Protocol (SMTP) host, HP SIM notifies you that it cannot send e-mail notifications. If you do not want to enter e-mail settings now, click **OK**, or to enter a valid SMTP host, click **Cancel**.

   Note: If the **Server Requires Authentication** option is selected, and you enter incorrect account information, e-mail event notifications do not reach the intended recipients.

First Time Wizard summary

When you are finished entering information in the HP Systems Insight Manager (HP SIM) First Time Wizard, review your selections on the Summary Page, and then click **Finish** to save them.

If you enabled automatic discovery or initiated **Run discovery** after the wizard finishes, discovery runs when you exit the First Time Wizard. If you did not enable automatic discovery or the Run discovery once after wizard finishes, discovery does not take place until you select **Options->Discovery** from the HP SIM menu, and enable a discovery task or select a task and click **Run Now**.

Finishing the First Time Wizard

When you click **Finish** in the First Time Wizard, the **Finish** page appears with a message stating **Your changes are being applied**, please do not close the window. If you selected Run discovery once after wizard finishes on the Discovery page, you are notified that discovery is running and where to go in the HP Systems Insight Manager (HP SIM) to monitor the progress of discovery. Also included on this page is information on where to go to see discovered systems that you are managing and where to go to better manage these systems. To close the First Time Wizard, click **Close**.

Setting up Windows managed systems

Use the following checklist as a guideline to assist you with setting up managed systems from a Windows Central Management Server (CMS):

1. Ensure that HP Systems Insight Manager (HP SIM) is installed on the CMS.
2. Ensure the First Time Wizard has been completed on the CMS.

   Important: Discovery must be run before setting up managed systems. Configuring automatic discovery is part of the First Time Wizard.
3. Configure the managed system software. See Configuring the managed system software using the Configure or Repair Agents feature from the CMS for more information.

Configuring the managed system software using the Configure or Repair Agents feature from the CMS

The HP SIM Configure or Repair Agents tool is a quick and easy way to configure Linux, HP-UX and Windows managed systems to communicate with HP SIM from a Windows 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 SIM community strings in the system security file. In addition, you must enter administrator level user credentials for the target system.

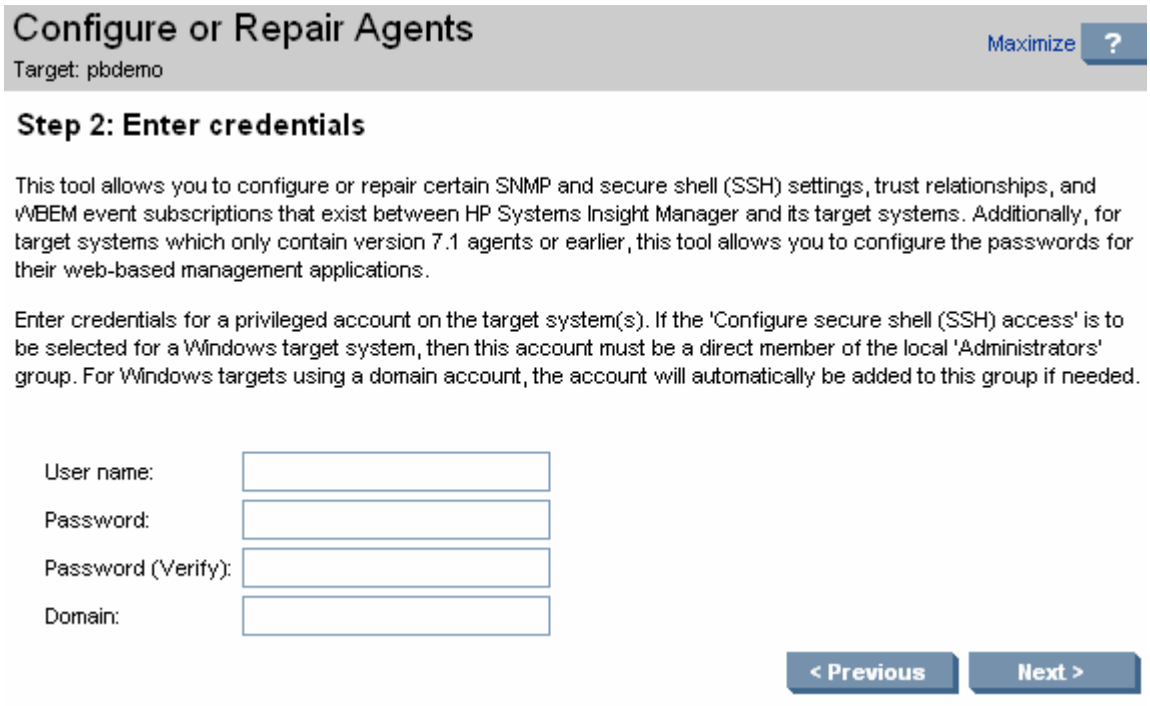
To configure agents remotely:

1. Select **Configure->Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.

   Note: The Step 1: Verify Target Systems page appears if the targets are selected before selecting a tool.

2. Select target systems.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

   Note: If you plan to Configure secure shell (SSH) access on a Windows target system, the account specified must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group if applicable.



4. From the Step 2: Enter credentials page:
   a. In the **User name** field, enter the system administrator name.
   b. In the **Password** field, enter the system administrator's password for the user name previously entered.

c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the Password field.

d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain administrator credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

5. Click **Next**. The **Step 3: Install Providers and Agents (Optional)** page appears.

6. You can install Insight Management Agents or providers, either Web-Based Enterprise Management or Simple Network Management Protocol, on managed systems so HP SIM can collect inventory and status information from these systems and receive event notifications from the systems. Installation is supported only on ProLiant or Itanium-based servers with Windows operating system.

   From the Step 3: Install Providers and Agents (Optional) page:

   a. Select **Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** to install WBEM or WMI providers on Windows managed systems.

   b. Select **Install SNMP Agent (HP Insight Management Agents) for Windows** to install the SNMP agent on Windows managed systems. This Insight Management Agent allows network monitoring and control.

   c. Select **Install Open SSH to install OpenSSH on Windows managed systems**.

   d. Select **Install the Version Control Agent (VCA)** to install the HP Version Control Agent; (VCA) on Windows managed systems. The VCA enables you to view the HP software installed on a system and install updates for the software are available in the repository.

   HP SIM determines the type of agent/provider to install based on the system type, subtype, and operating system description of the system.

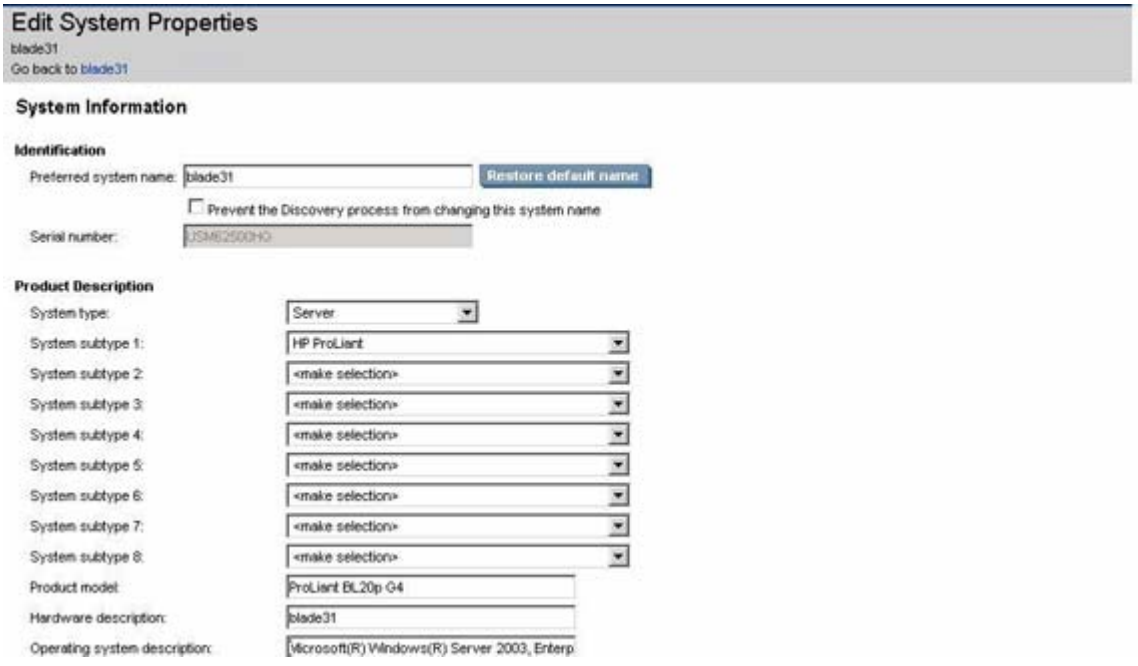
   Table 6.1 Version Support Matrix for components used for install.

Supported systems	HP WBEM Provider	HP ProLiant Agent	Open SSH	Version Control Agent
Unknown	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (64 bit)	7.90 (64 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating systems (2000)	Not supported	7.60 (32 bit)	3.71	2.1.8
Itanium-based systems with Windows operating system (2003)	Not supported	5.1.10	3.71	2.1.7.770

System Management Homepage version 2.1.7 is also installed, if necessary, with these agents.

Note: If you wish to install a 64 bit agent or provider, make sure the target system is identified as a 64 bit system in HP SIM.

If your system is not correctly identified, go to System Page ->Edit System Properties. Select the correct system type, subtype and enter the operating system description manually.



Example: Installing Insight Management Agents on a ProLiant Windows 64 bit system:

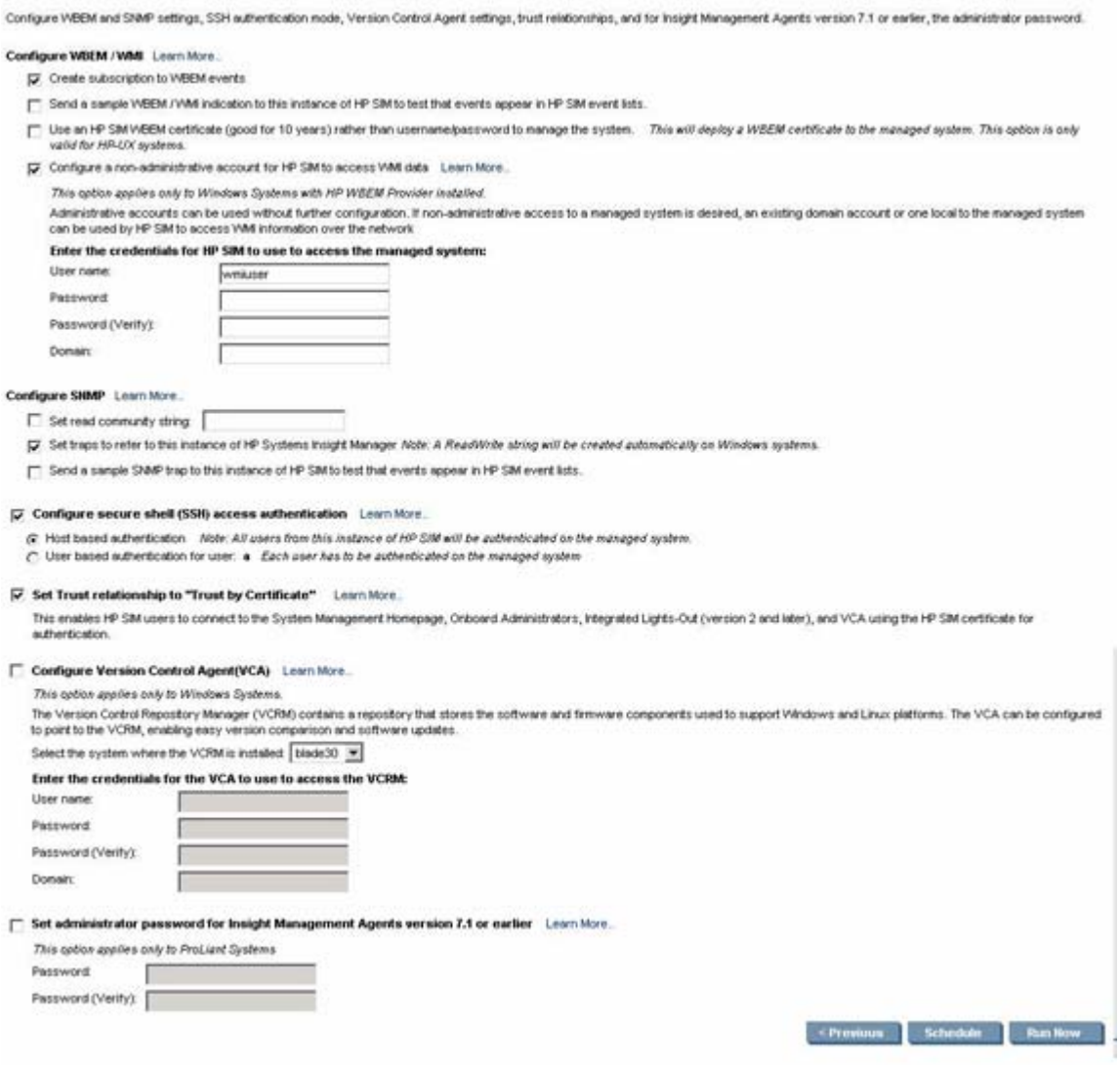
5. Select system Type: server.
6. Select system subtype 1: ProLiant

7. Enter operating system description as Microsoft Windows Server 2003, x64 Enterprise Edition Service Pack 1 or the correct operating system description of your system.

If you want to configure the agents after installing, select the force reboot option. This allows the newly installed component to be completely initialized before configuring it.

Note: Installation with reboot typically takes about 8 minutes to complete.

7. Click **Next**. The **Step 4: Configure or Repair Agents** page appears.



8. The **Step 4: Configure or Repair Agents** page enables you to select options to configure the target system.

The following options are available:

- **Configure WBEM / WMI.** This section enables you to configure the target Linux, Windows or HP-UX system to send WBEM indications or events to HP Systems Insight Manager.

  For this section, the following must be considered:

- Create subscription to WBEM events, so that WBEM events will be sent to the CMS.
- Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system.

  Note: The indication will appear as an Informational Event in the Event List of HP SIM.

  Note: This is supported only on HP-UX and Windows managed systems with WBEM provider installed.
- Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system. This option deploys a WBEM certificate to the managed system and is only valid for HP-UX systems.
- Configure a non-administrative account for HP SIM to access WMI data. This option is applicable to Windows systems with HP WBEM providers. The configuration of the managed system will be updated to allow the specified user to access WMI information over the network. This user will be used by HP SIM to read inventory and configuration information from the system, and will be configured as the WBEM user in the System Protocol Settings. This configuration step is not necessary if HP SIM is configured with a user with administration rights. This user is not created by HP SIM; it should already exist as either a domain user or one local to the managed system.

  The user will be added to the "DCOM Users" group on the managed system and will be given read-only access to WMI information, plus read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system and need not have logon rights. A special purpose domain account is recommended, and should be created by the domain administrator.

  To enter the credentials for HP SIM to use to access the managed systems:

  1. In the **User name** field, enter a user name.
  2. In the **Password** field, enter the password for the user's name previously entered.
  3. In the **Password (Verify)** field, reenter the password exactly as it was entered in the Password field.
  4. In the **Domain** field, enter the Windows domain if the target belongs to a domain.

     If configuring a non-administrative user is successful, then these credentials are saved as the System Protocol settings for WBEM access in HP SIM.

- **Configure SNMP.** This section enables you to configure SNMP settings.

  For this section, the following must be considered:

a. Select **Set read community string** to specify a community string. By default, HP SIM's first community string, that is not public, appears in the field. If no community string exists in HP SIM, you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you need not set this option. HP-UX enables 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 systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

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 30 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 SIM over the network. Linux and HP-UX systems do not require a Read Write community string; hence the Read Write community is added on Windows systems only.

b. Select **Set traps** to refer to this instance of HP Systems Insight Manager in the target systems' SNMP Trap Destination List. This setting enables the target systems to send SNMP traps to this instance of HP SIM.

c. Select **Send a sample SNMP trap to this instance of the HP SIM** to test that events appear in HP SIM event lists to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

Note: A test trap can only be sent from a Windows managed system with HP Insight Management Agent installed. If you attempt to run this task on a Linux or HP-UX managed system, a message displays indicating the operation is not supported.

Note: The trap will appear as a Generic Trap from the system. This event will appear as an Informational Event in the Event List of HP SIM.

- **Configure secure shell (SSH) access.** Select this option to configure SSH access on managed systems.

  If this option is selected, you must select one of the following options:

  - **Host based authentication for SSH.**

    Note: For this option to work, the user name and password provided in step 2 must be an administrative level account. For Linux or HP-UX targets, it must be the "root" account and password.

  - **Each user has to be authenticated on the managed system**

Note: If you do not want all users that have login access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

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 as done in step three or by selecting the tool under **Deploy->Deploy Drivers->Firmware and Agents->Install Open SSH**.

- **Set Trust relationship to "Trust by Certificate".** Select this option to configure 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 SIM system certificate to the target system's trusted certificate directory. This option enables HP SIM users to connect to the System Management Homepage using the certificate for authentication.

  You can configure Single Sign-On (SSO) to management processors for Onboard Administrators and for Integrated Lights-Out 2 (iLO2). To configure SSO, select Set Trust Relationship. After SSO is configured, you are not continually prompted to supply the login credentials for the management processor.

  Note: For systems with Management HTTP Server 4.x and earlier, Configure or Repair Agents adds the Administrator password in the Management HTTP Server store and modifies the SNMP settings but cannot change trust relationship information because Management HTTP Server 4.x and earlier did not deploy trust relationships.

- **Configure Version Control Agent (VCA).** Select this option to configure the VCA to point to the HP Version Control Repository Manager (VCRM), where the repository of software and firmware is located, enabling version comparison and software updates. This option is available only for Windows systems. This section can be accessed in the Configuration section of all CMS systems including Windows, Linux and HP-UX.

  To configure VCA:

  1. In the **Select the system where the VCRM is installed** field, select the server where the VCRM is installed from the dropdown list.
  2. In the **User Name** field, enter the user name to access the VCRM. This user cannot be the default "Administrator" user. It has to be a user with administrative privileges.
  3. In the **Password** field, enter the password to access the VCRM.
  4. In the **Confirm Password** field, reenter the password for the VCRM just as you entered it in the **Password** field.

2. **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: Do not set 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 need not set this option.

If this option is selected, you must complete the following steps:

a. In the **Password** field, enter the new administrator password.
b. In the **Confirm Password** field, reenter the new administrator password exactly as you entered it previously.

2. Click **Run Now**. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The log results indicate whether the repair attempt was successful.

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. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed and for some to fail.
- **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.
- **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:

  a. 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.
  b. Select which report to display.
  c. Click **OK** to display the report, or click **Cancel** to return to the **View Task Results** page.

10. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents tool can be configured to run automatically on a schedule, or you can run it manually. Only one instance of Configure or Repair Agents tool can run at a time.

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 on a managed node for HP SIM to discover SAN storage. This includes storage devices such as Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters.)

See 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 provides the SMI-S provider and installation instructions for its storage system. The webpage referenced in the previous section provides information on obtaining 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 SSL is enabled for each SMI-S provider.

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 CIMOMs exist on the same host, you must configure them to use different ports to communicate 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 by performing the following steps:

1. Enter the user name and password for each provider's SMI CIMOM in the Default WBEM settings section on the Setting Global Protocols page.
2. Add each SMI CIMOM IP address to the System Automatic Discovery task or to the Creating a New Discovery task. See the HP SIM User Guide at http://docs.hp.com/en/index.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 HP SIM User Guide at http://docs.hp.com/en/index.html.

Summary

After you complete the HP SIM installation, the core capabilities of the software enables you to automatically discover systems, monitor system health, deploy system software and firmware updates, and set up paging or e-mail notifications for proactive notification of potential problems.

As your needs grow, you can easily integrate value added plug-ins into the base CMS to deliver management across the server and storage lifecycle. These plug-ins include applications for rapid deployment, vulnerability and patch management, virtual machine management partition management, performance management, and others. You can also customize your management platform with off-the-shelf or internally developed scripts and applications.

Finally, you can further extend the capabilities of HP SIM with plug-ins for HP clients, storage, power, and printer products, enabling management of your entire HP infrastructure.

Glossary

central management server (CMS)	A system in the management domain that executes the HP SIM software. All central operations within HP SIM are initiated from this system.
HP VCRM (Version Control Repository Manager)	An HP agent that enables a customer to manage HP provided software stored in a user-defined repository.
HTTPS (Hyper Text Transfer Protocol)	The underlying protocol used by the World Wide Web. HTTPS is HTTP over SSL, a protocol that supports sending data securely over the Web. HTTPS is used to access WBEM data and ProLiant agent information. Digital certificates are used instead of user names and passwords to establish trust between the agent and the central management server (CMS). The certificate of the CMS should be loaded into each agent to be managed by that CMS.
SNMP (Simple Network Management Protocol)	SNMP is 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.
SSH (Secure Shell)	SSH is a program that enables you to log into 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. The private key is kept secure on the CMS, while the public key is installed on each managed system.
SSL (Secure Sockets Layer)	Secure Sockets Layer is a protocol for enabling secure communications over an HTTP session. It uses public/private key algorithms to authenticate and encrypt data communication across the network.
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 either integrate SMI-S providers with their systems, or provide them as separate software packages.
system collection	System collections provide a way to search the HP SIM database for 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.
WBEM (Web-Based Enterprise Management)	WBEM is 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.
WMI (Windows Management Instrumentation)	An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled.

Additional resources

For additional information, refer to the resources detailed below.

Resource description	Web address
HP SIM web site	http://h18004.www1.hp.com/products/servers/management/hpsim/
To download the latest version of HP SIM	http://h18004.www1.hp.com/products/servers/management/hpsim/download.html
Migrating from Insight Manager™ 7 to HP SIM	http://h18004.www1.hp.com/products/servers/management/hpsim/infolibrary.html
Moving HP SIM to a New System	http://h18004.www1.hp.com/products/servers/management/hpsim/infolibrary.html
HP SIM QuickSpecs	http://h18013.www1.hp.com/products/servers/management/hpsim/quickspecs.html
HP SIM white papers and technical documentation	http://h18004.www1.hp.com/products/servers/management/hpsim/infolibrary.html
HP Storage Essentials information	www.hp.com/go/storageessentials/

© Copyright 2004-2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation

441289-002, 02/2008