How to manage non-HP x86 Windows servers with HP SIM

Screenshots

Introduction

HP Systems Insight Manager (HP SIM) is able to manage non-HP servers using industry standard interfaces of Simple Network Management Protocol (SNMP), Web-Based Enterprise Management (WBEM), and secure Hypertext Transport Protocol (HTTPS). Integrating the management of non-HP servers into HP SIM is very similar to setting up an HP server. Although HP SIM, also known as the Central Management Server (CMS), has some built in monitoring support for non-HP servers, HP recommends that the third party MIBs be installed into HP SIM 5.x to aid in monitoring the server.

This document details how to set up two non-HP servers to be managed by HP SIM: Dell and IBM. Since configuration and setup are specific to the host operating system, this paper first discusses the HP SIM features available for non-HP servers, and then discusses specific configuration requirements necessary to enable the features. To avoid repetition, examples are shown from different servers instead of showing examples of every feature from every server.

HP SIM inventory for non-HP x86 Windows servers

HP SIM can discover and identify non-HP servers using SNMP. HP SIM also requires WMI services be enabled and configured for HP SIM to retrieve asset inventory details. The SNMP MIB must be compiled within HP SIM to properly receive and display SNMP traps.

Discovery and identification

HP SIM can discover non-HP x86 servers using SNMP. HP SIM can identify non-HP server's names via DNS. IP address, product name and OS name are identified by discovery using SNMP. For VMWare and Microsoft VM clients and hosts, install and enable the HP Virtual Machine Manager (VMM) SNMP agent. HP SIM associates the hosts with their clients. Blade servers are identified as servers. However, clusters are not identified since no SNMP or WBEM/WMI standard exists. HP SIM can identify proprietary management pages, such as Dell OpenManage, as shown in Figure 1.

Note: HP SIM cannot display a graphical picture of blade enclosures for non-HP servers or associate the servers with Rack or Enclosure information.

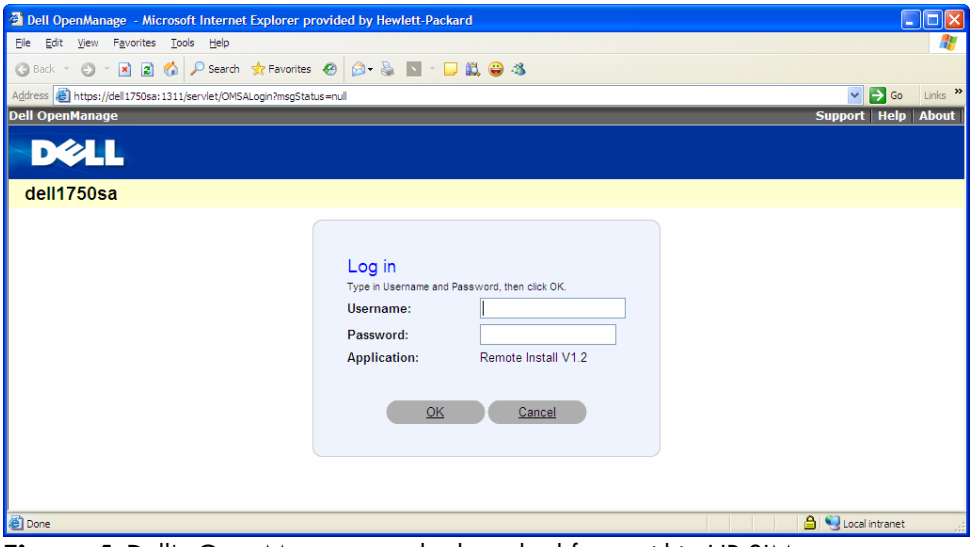

Figure 1 Dell's OpenManage can be launched from within HP SIM

Events

Once the SNMP MIBs are compiled in HP SIM, events will be properly received and important data fields (varbinds) will be displayed for each event.

System properties and reports

After configuring SNMP and WMI on your server, you can collect inventory information and view HP SIM property pages. Figure 2 shows a WBEM **Properties** page, and Figure 3 shows an inventory report for a Dell server.

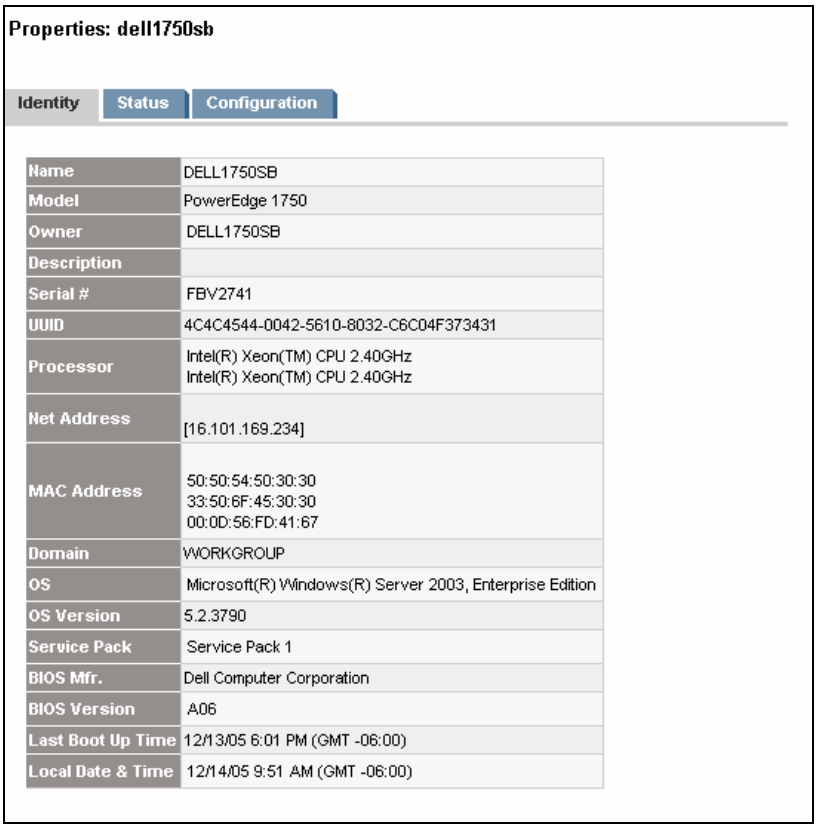

Figure 2 Dell WBEM Property Page

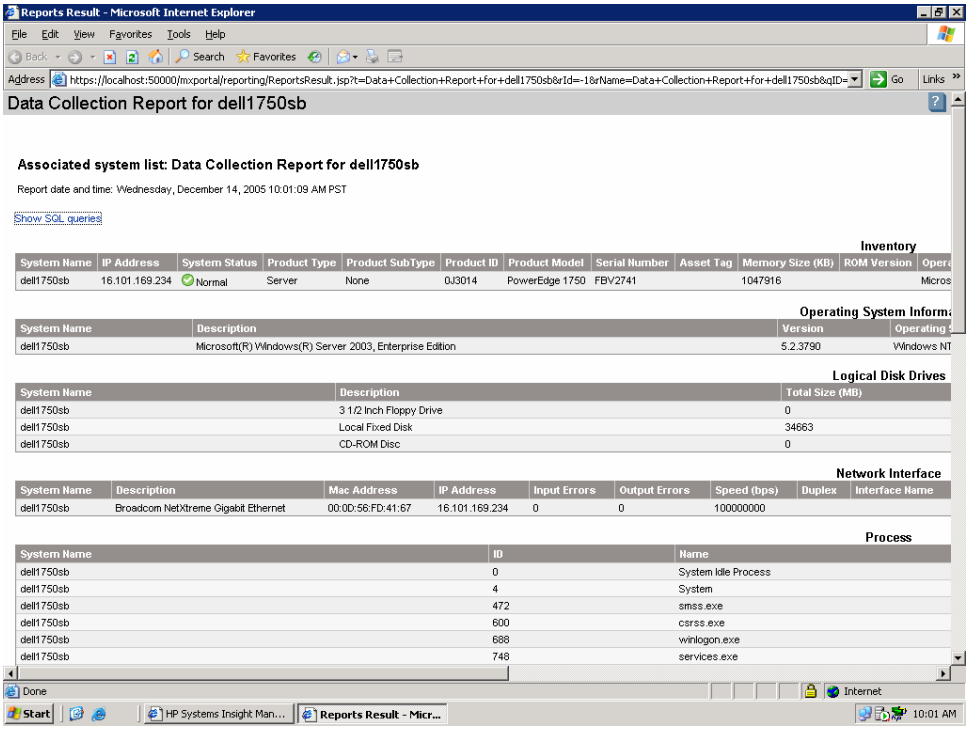

Figure 3 Dell Data Collection Report.

Executing remote tasks

Once SSH is properly configured you will be able to run tasks and scheduled jobs on one or multiple managed server.

Security

HP SIM provides highly secure management of remote systems once SSH is correctly configured and HP SIM to server trust relationships have been established. This includes all role-based security features that are available for HP systems.

ProLiant Essentials for managing non-HP x86 servers

Vulnerability and Patch Management (VPM)

HP SIM has an added feature that other network manageability software products do not offer, which is the HP ProLiant Essentials Vulnerability and Patch Management (VPM) pack. This plug-in enables the user to gain the upper hand against hackers, worms, and blended threats that exploits software security vulnerabilities. The integration of VPM helps identify and resolve security vulnerabilities quickly. VPM also has the ability to download the necessary patches found during the scanning process. VPM enables users proactive protection for your business, enabling you better control in keeping your network systems updated. Figure 4 shows an example of a VPM report from an IBM server.

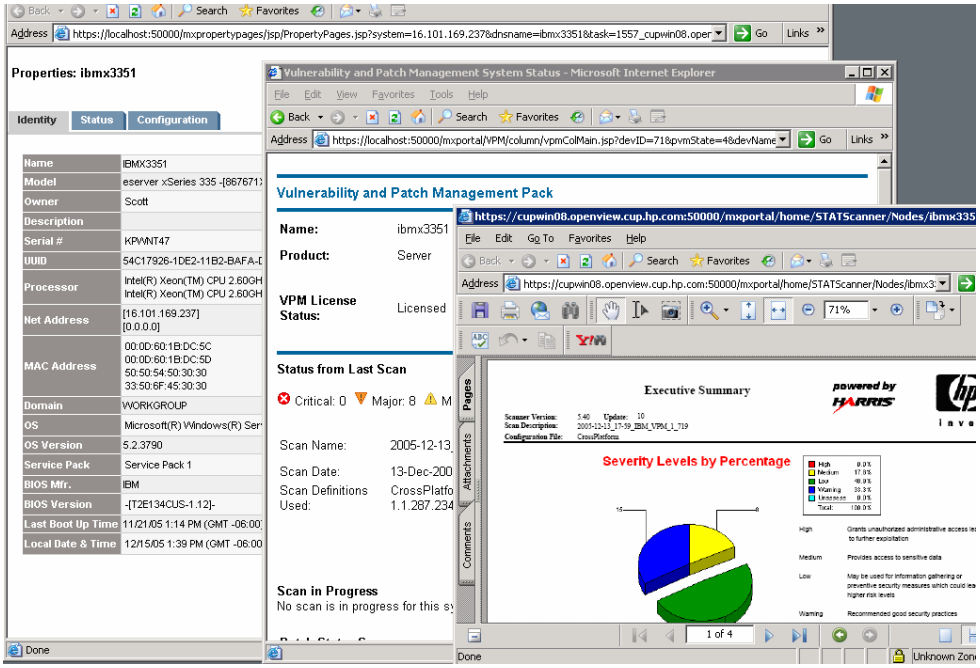

Figure 4 IBM WBEM Property Page and VPM Report.

Installing and configuring VPM on non-HP servers:

1. Install VPM on the same server as HP SIM.
2. Select the Managed Node.
3. Deploy the VPM Agent, as shown in Figure 5 by selecting **Deploy>Vulnerability and Patch Management>VPM Patch Agent.**

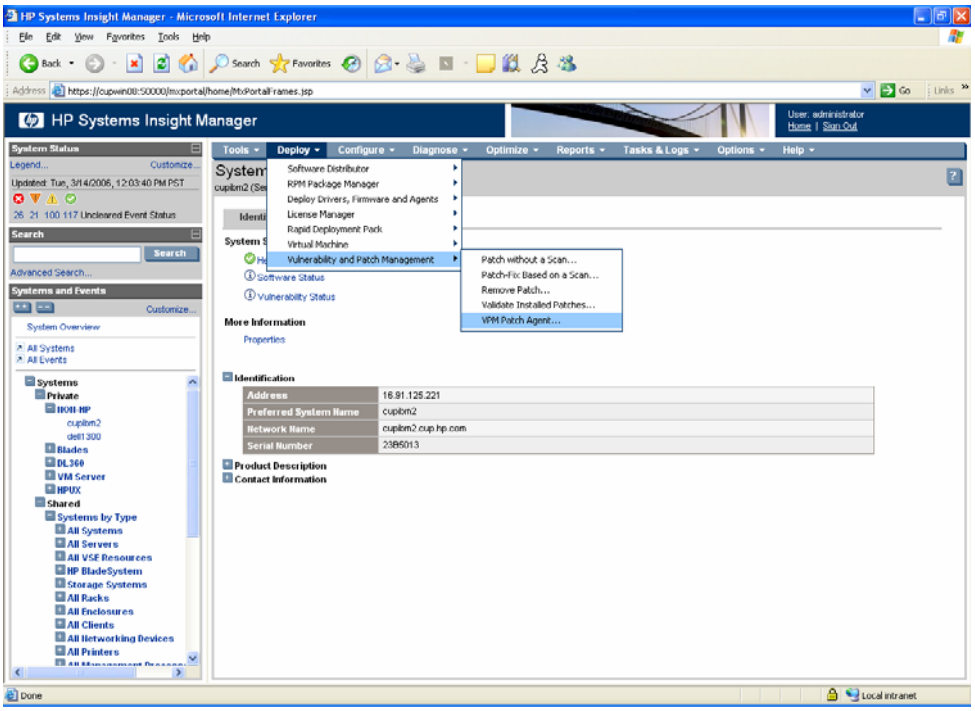

Figure 5 Navigation to deploy the VPM Agent

4. Deploy License Key for VPM by selecting the VPM Server Keys by selecting **Deploy>License Manager>Deploy Keys**. See Figure 6.

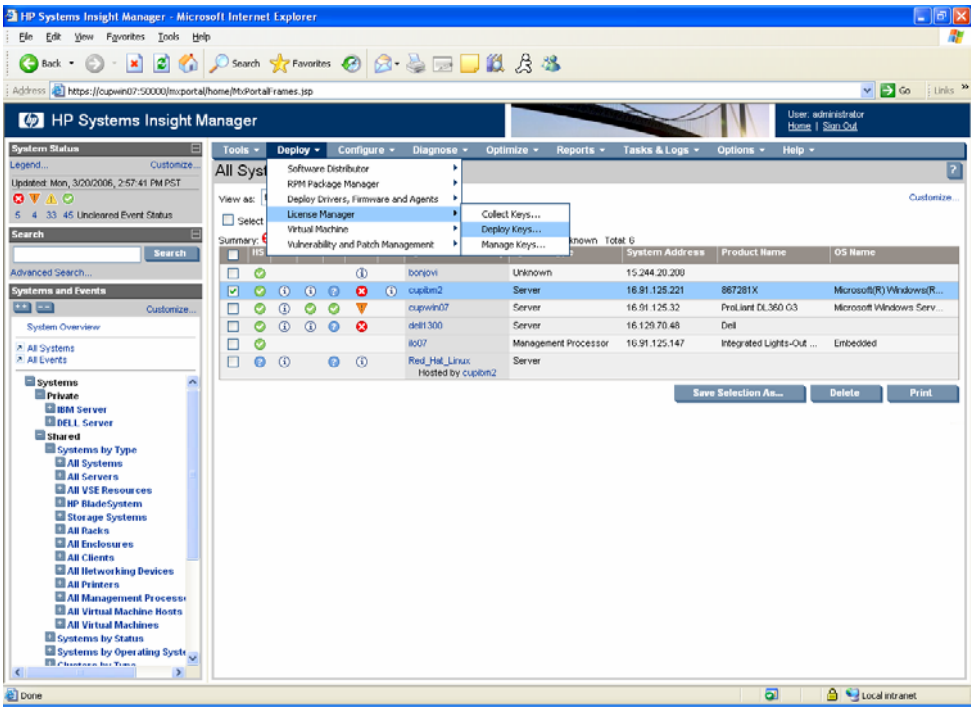

Figure 6 Navigation to deploy the licensing keys to the managed node

5. Re-Identify the Managed system. This produces an icon in the **VPM** column.

6. Select **Tools>System Information>System Page** then select **Vulnerability Status.** This can also be done by selecting the icon in the **VPM** column.

7. Select **Scan for Vulnerability** and complete the wizard.

Virtual Machine Manager (VMM)

The Virtual Machine Management Pack provides central management and control of VMware and Microsoft virtual machines and provides physical host to virtual machine association. Virtual Machine Management Pack is installed with HP SIM and includes five free licenses to try. The VMM service extends its manageability to non-HP x86 servers. The information below briefly describes how to setup VMM on HP SIM.

Note: Each virtual host must have a license. Additional licenses can be purchased from http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/vms/index.html

Note: Each virtual machine host can only be registered to one HP SIM instance.

Setting up VMM in HP SIM:

1. Select the managed system.
2. Deploy the VMM Agent, by selecting **Deploy>Deploy Drivers, Firmware and Agent>Install VMM Agent>Windows**, as shown in Figure 7.

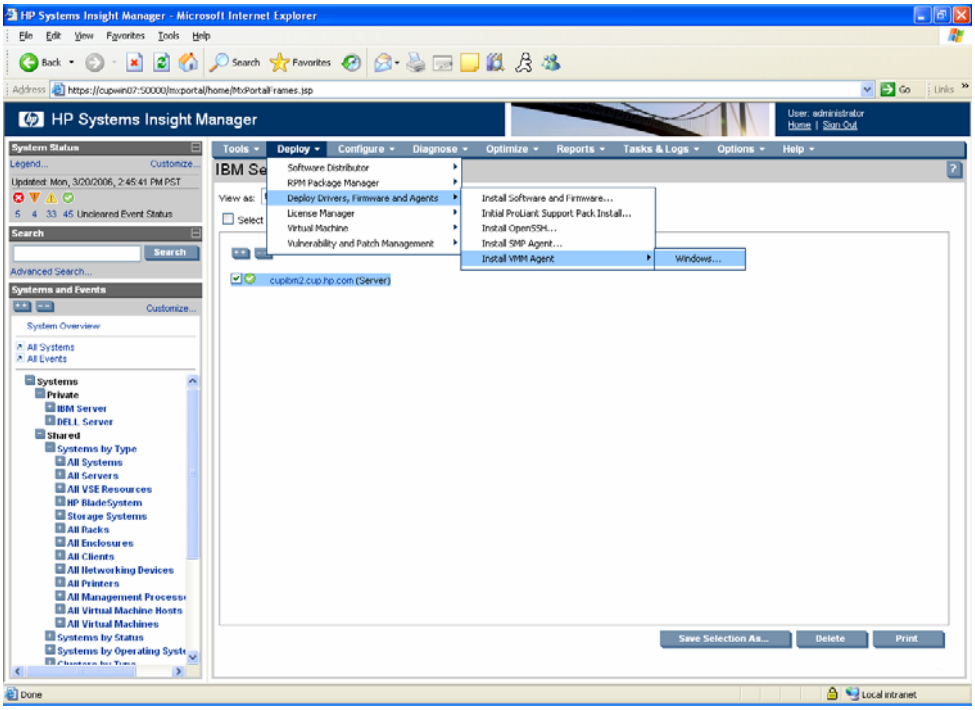

Figure 7 Select Managed Node and deploy the VMM Agent

3. Deploy License Key for VMM by selecting the VMM Server Keys. Select **Deploy>License Manager>Deploy Keys**.

4. Reidentify the managed system. A green checkmark icon appears, see Figure 8.

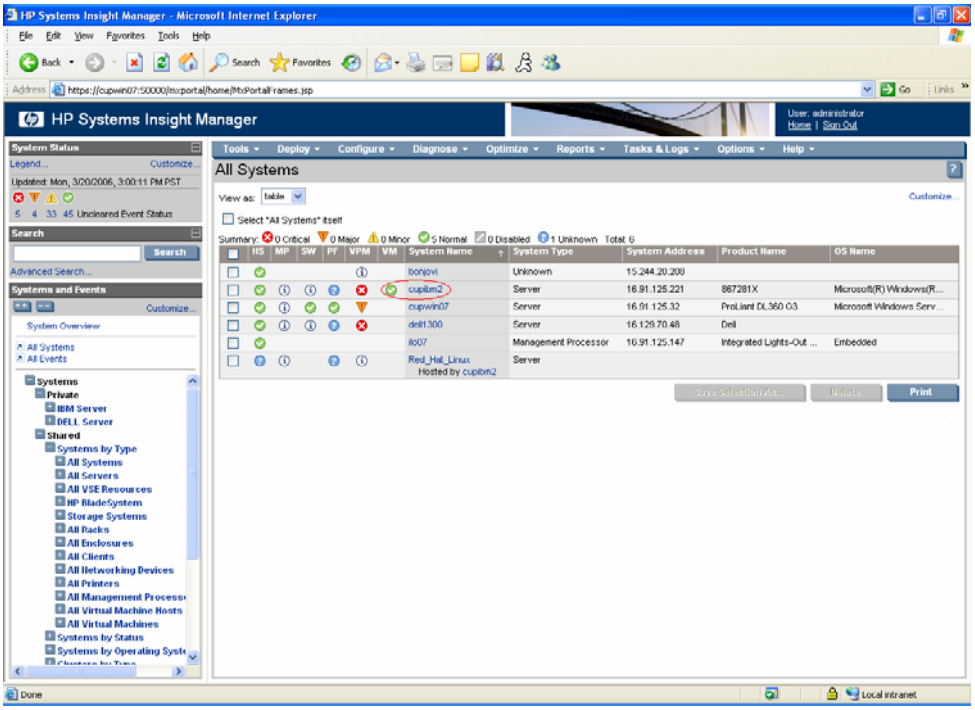

Figure 8 Green checkmark icon in the VMM column

5. Select **Tools>System Information>System Page** then select **Virtual Machines.** This can also be done by click the icon in the **VMM** column. See Figure 9.

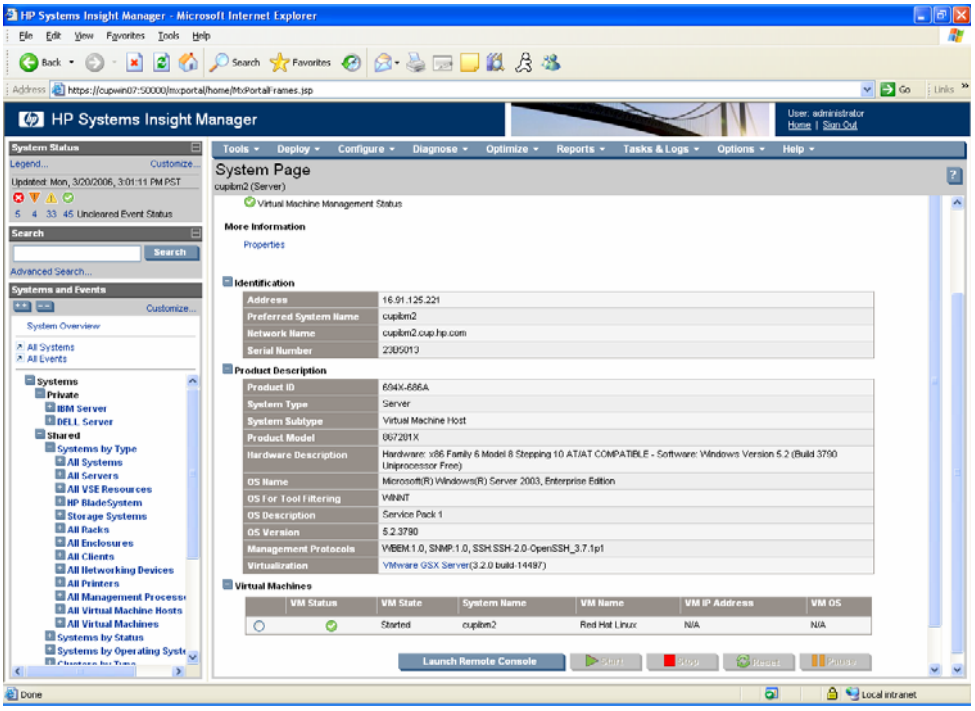

Figure 9 System Page for IBM with virtual machine being displayed

Server Migration Pack (SMP)

The Server Migration Pack (SMP) works together with Virtual Machine Manager to extend HP Systems Insight Manager capabilities to manage virtual machines. SMP automates the manual task of migrating servers between physical or virtual platforms. The Server Migration Pack allows P2V, V2P and V2V migration. The information below briefly describes how to migrate a physical non-hp x86 servers to a virtual host on a HP ProLiant server.

Note: A registered virtual host must be running. See Virtual Machine Manager (VMM).

Steps to migrate physical-to-virtual server for non-HP x86 Servers:

1. Select the managed system.

2. Deploy the SMP Agent and step through the wizard by selecting **Deploy>Deploy Drivers, Firmware and Agent>Install SMP Agent**. This is shown in Figure 10.

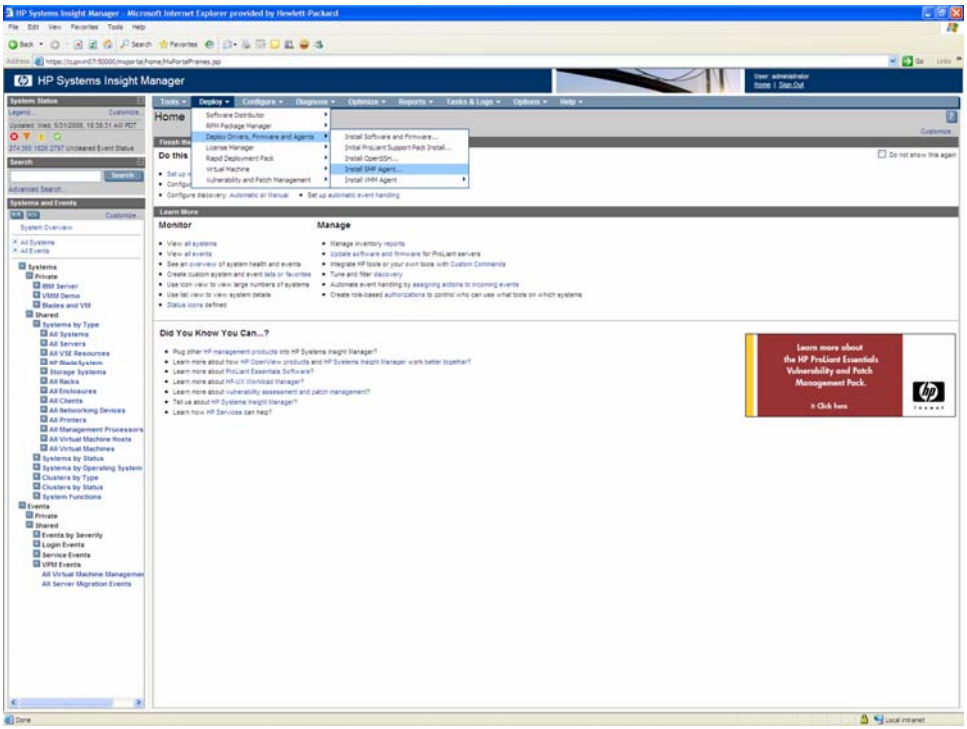

Figure 10 Select Managed Node and deploy the SMP Agent

3. Deploy License Key for SMP by selecting the Server Migration Pack Keys, as shown in Figure 6. Select **Deploy>License Manager>Deploy Keys**.

4. Select **P2V** for physical-to-virtual migration and step through the wizard, as shown in Figure 11. Select **Deploy>Virtual Machine>P2V**.

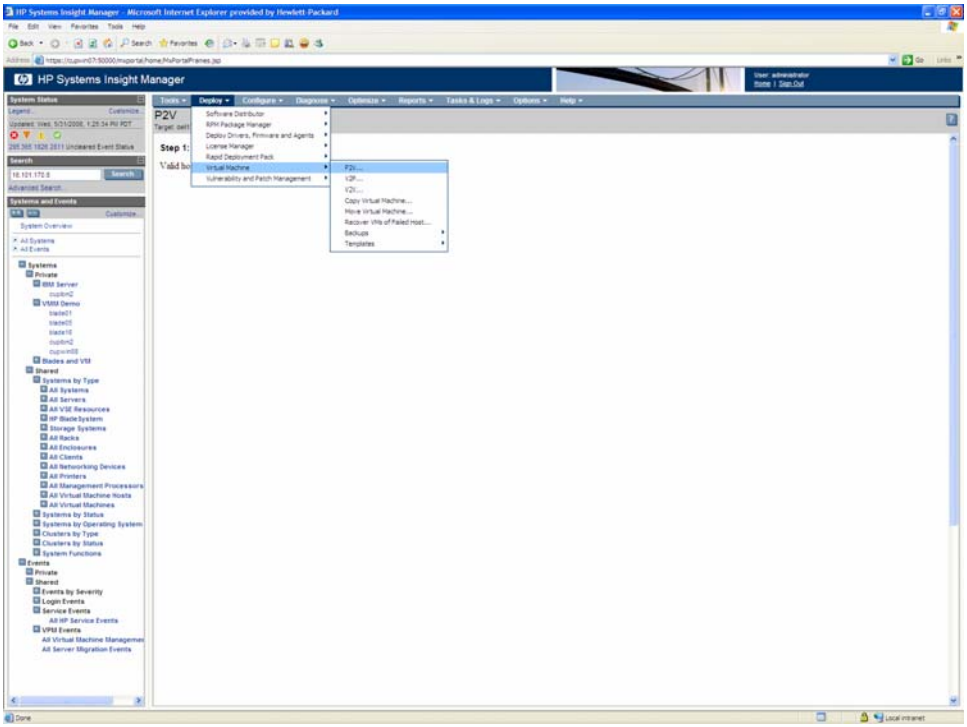

Figure 11 Deploy > Virtual Machine > P2V to launch the P2V Wizard

5. Perform the Post-Migration task to clean up the network configuration after the migration is complete.

Note: For the Post-Migration task, different types of migration and how to use SMP can be found at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00498328/c00498328.pdf

Step-by-step configuration details

This section details the configuration steps required on the non-HP server being managed, and the steps required for configuring HP SIM to manage the non-HP server.

Configuring and setting up SNMP

These steps show how to install SNMP on Windows. SNMP is required to allow HP SIM to collect basic information about the server.

1. In Internet Explorer, select **Control Panel>Add/Remove Programs** to bring up the application.

2. Select "**Add/Remove Windows Component**.

3. Select **Management and Monitoring Tools**.

4. Click **Details**. Select **Simple Network Management Protocol**. This is shown in Figure 12 and Figure 13.

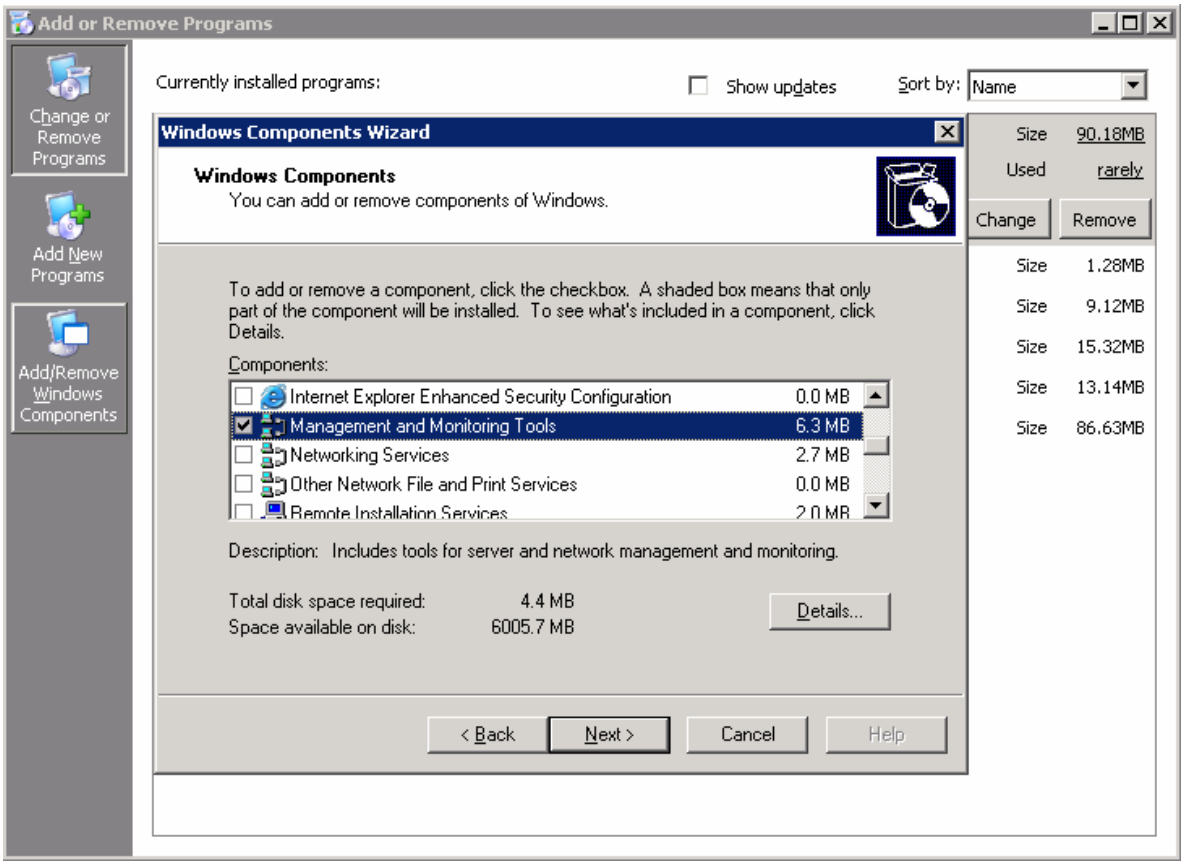

Figure 12 - Add/Remove Programs > Add/Remove Windows Components.

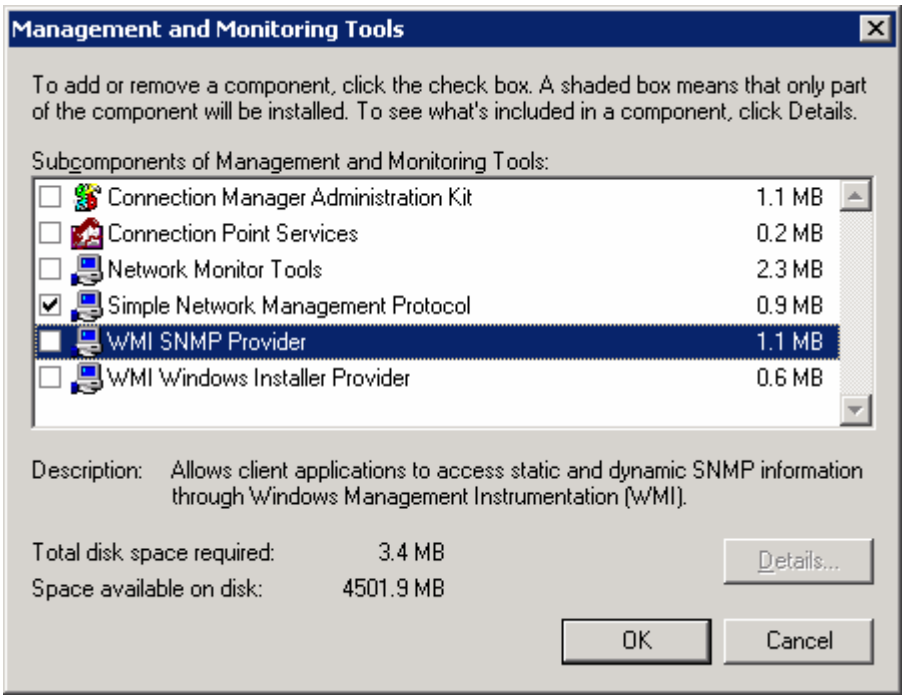

Figure 13 - Select Simple Network Management Protocol.

After the SNMP components are installed, the parameters for SNMP must be set. This can be done by right-clicking the mouse on the SNMP services from the **Service Management Console**. The two tabs that will be focused on are **Traps** and **Security**. The community names and trap destinations can be set in the **Traps** tab. Community names are case-sensitive and the host name or IP address of the HP SIM server must be listed The **Security** tab enables you to set **Accepted community names** for read and write. Select **Accept SNMP packets from these hosts** and add the host name or IP address of the HP SIM server. This is shown in Figure 14.

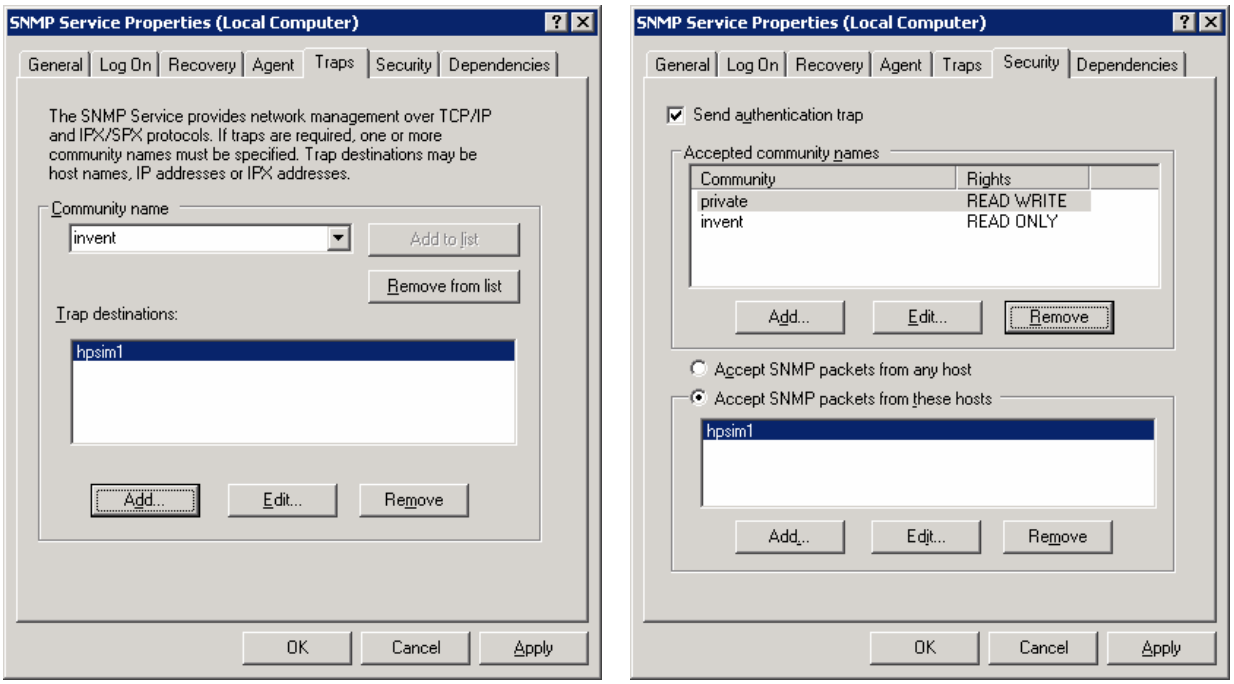

Figure 14 - SNMP "Traps and Security" tabs.

Loading MIBs

The Management Information Base (MIB) can be found on the website for the server manufacturer. On the Dell or IBM website, MIBs can be found by running a web search on **Dell MIBS for Poweredge** or **IBM MIBS**. After the MIBs are downloaded and expanded (if necessary), they must be copied to the HP SIM directory, compiled, and registered with HP SIM.

Copying MIBs

Copy the MIB file to the HP SIM MIB directory located at:

```
<install drive>:\Program Files\HP\Systems Insight Manager\mibs
```

Note: HP SIM generates an error if the MIB filename contains only numerical characters. The MIB should be renamed with alphanumerical characters for example `10892.mib` to dell10892.mib.
Note: The Dell MIB comes compiled and registered with HP SIM.

Compiling MIBs

Compiling the MIBs will create a .cfg file that will be used to register into HP SIM. In order to compile the MIBs, the following command line can be entered from a command prompt (this example is for a Dell server).

1. Navigate to the MIB director in HP SIM:

   cd <install drive>:\Program Files\HP\Systems Insight Manager\mibs

2. Enter:

   mcompile <mibname>

The MIB should compile and return the following message Mib Compiliation completed successfully, as shown in Figure 15.

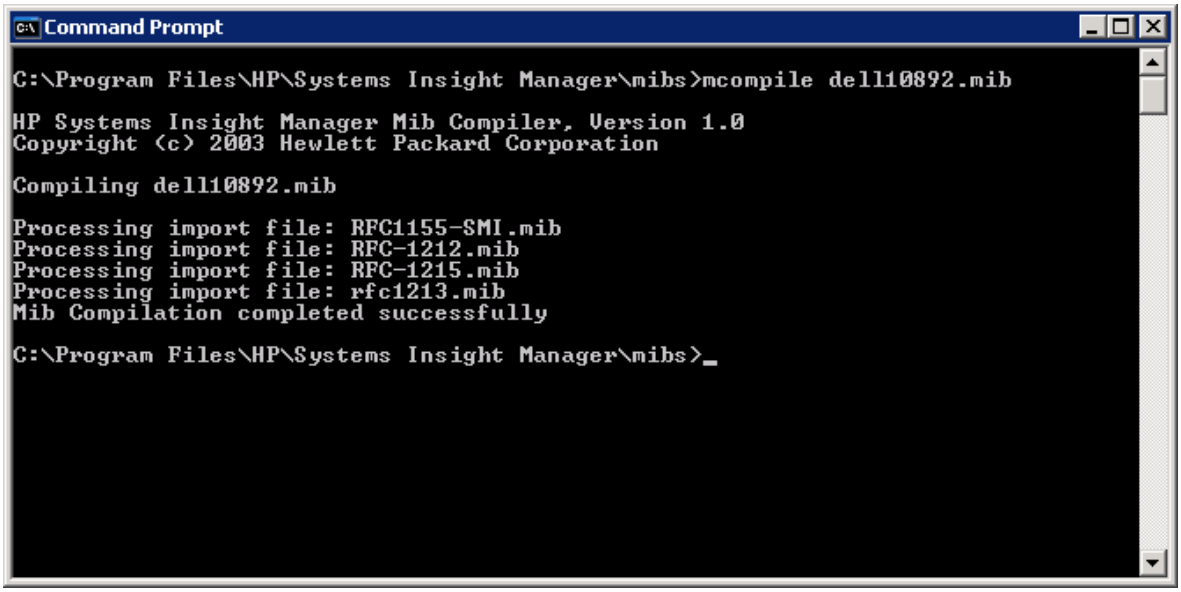

Figure 15 Compiling the MIBs for DELL

Registering MIBs

After the MIB is compiled, it must be registered with HP SIM so that SNMP can identify and send notification messages from the managed systems. The following command is used to register the MIB with HP SIM. This is shown in Figure 16 for a Dell server.

1. Navigate to the MIB directory in HP SIM:

   cd <install drive>:\Program Files\HP\Systems Insight Manager\mibs

2. Type the command:

   mxmib –a <mibname.cfg>

The MIB registers and displays the following message, COMMAND COMPLETED SUCCESSFULLY.

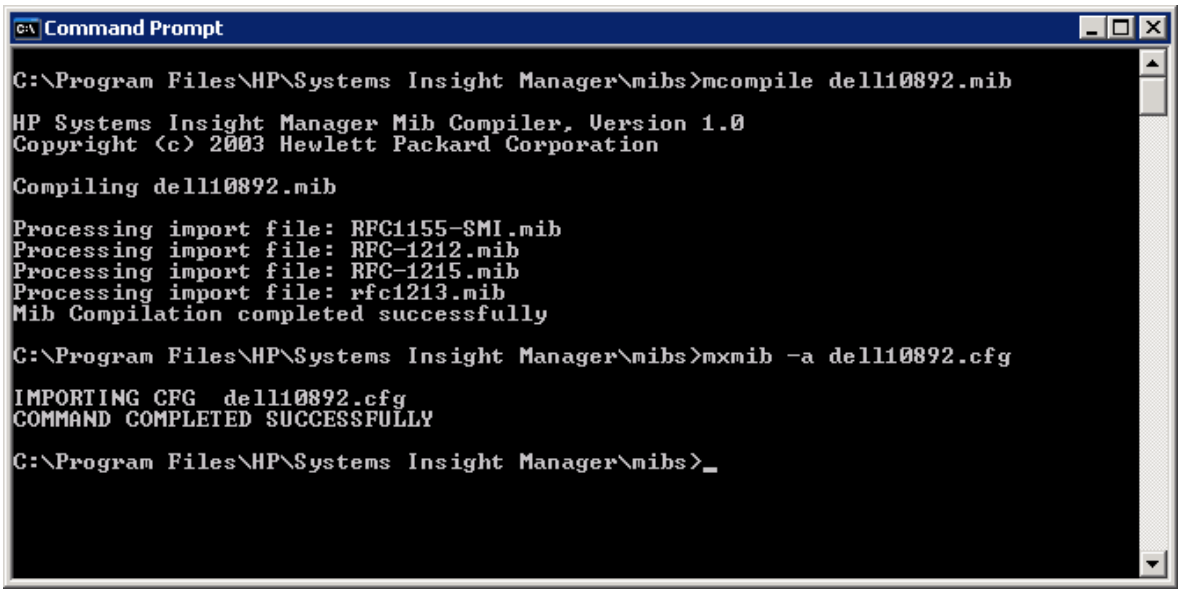

Figure 16 - Registering the MIB for DELL

Configuring and setting up HP SIM

Manually discovering non-HP servers

Use Manual Discovery to add the nodes to HP SIM. The settings for WBEM and SNMP should be configured using the "**more settings**" options. This is shown in Figure 17 and Figure 18.

1. In HP SIM, select **Options**>**Discovery**, and click 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. Select **More Settings** to enter the following additional information:

WBEM settings:

a. User name

b. Password

SNMP settings:

a. Read-only community string

b. Write community string

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.

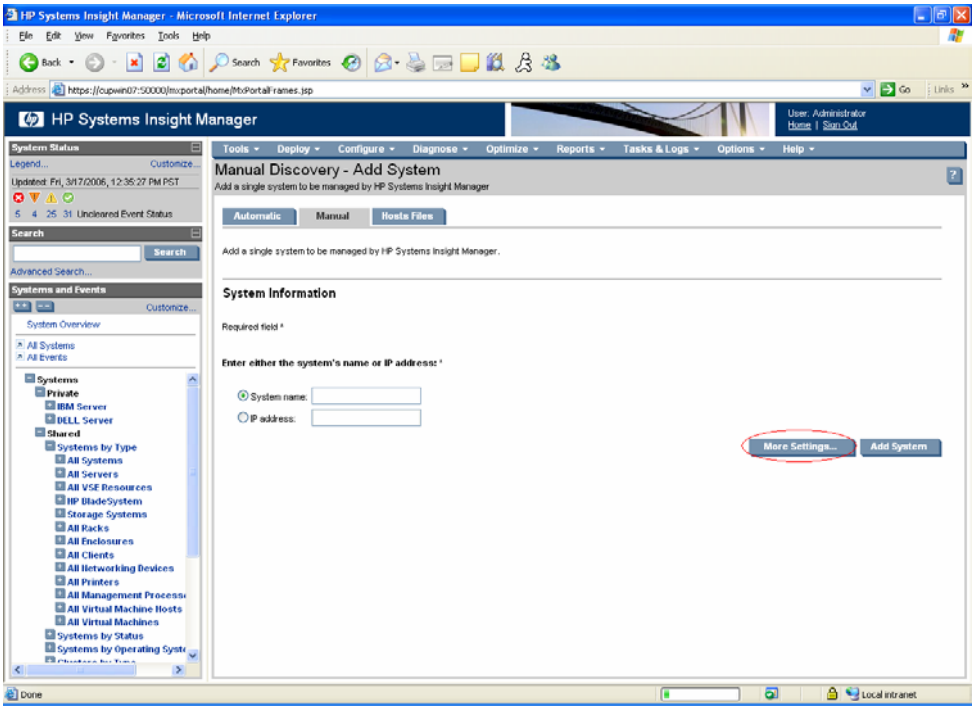

Figure 17 Select "More Settings" to enter WBEM and SNMP information

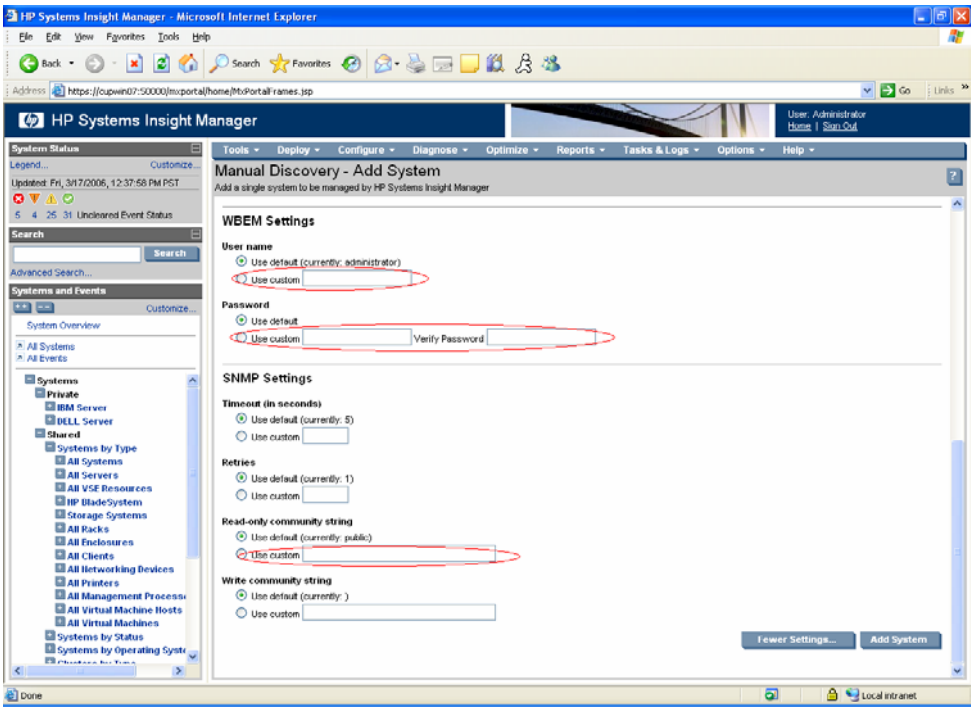

Figure 18 - Select customized settings

Running commands from HP SIM

To execute secure commands on that system, OpenSSH needs to be installed on the managed server. A version of OpenSSH for Windows that has been tested with HP SIM can be found at:

http://h18023.www1.hp.com/support/files/server/us/download/22546.html

After OpenSSH is installed, a copy of the SSH-generated public key can be copied from the CMS to the managed server using the **Configure and Repair Agent** GUI, or **mxagentconfig** from the command line.

Configure and Repair Agent

From HP SIM menu:

1. Select to **Configure>Configure and Repair Agents.**
2. Enter the sign in credential for the administrator of the managed system.
3. Uncheck **Configure SNMP**. This function only works with HP servers.
4. Uncheck the **Trust Certificate**, **Set administrator password for Insight Management Agents version 7.1 or earlier** and **Create Subscription for WBEM events**. See Figure 19.

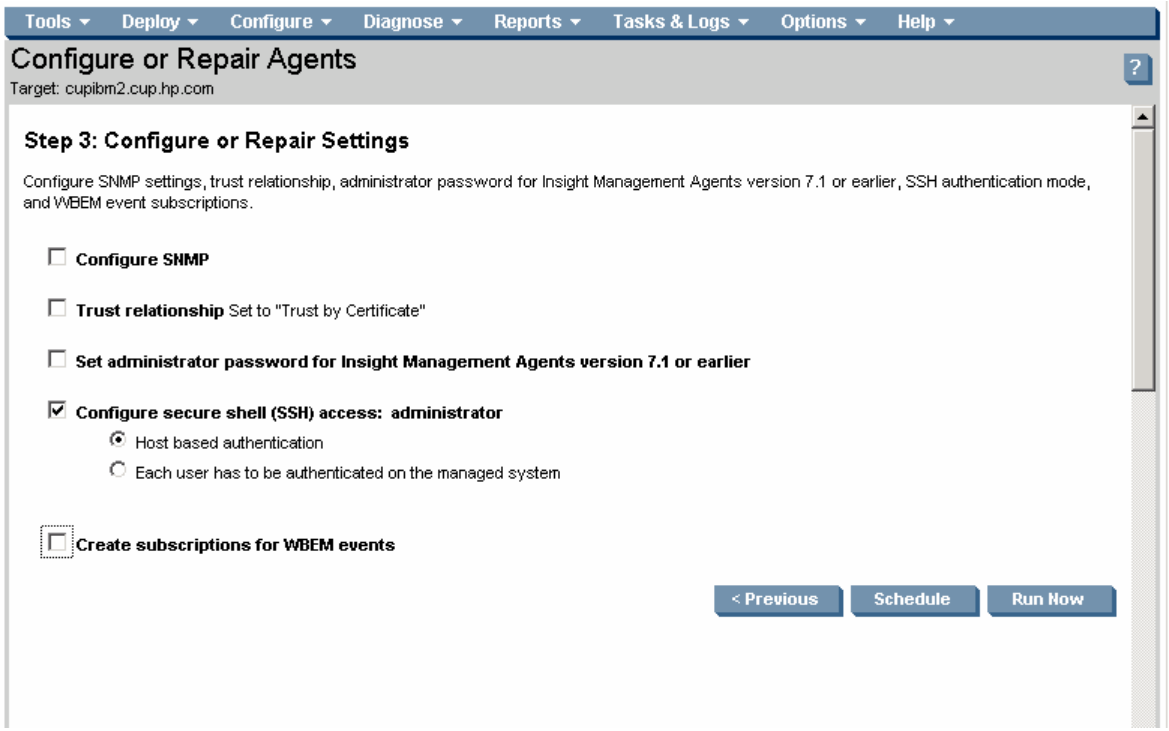

Figure 19 - Configure and Repair settings for SSH access.

5. Select **Configure secure shell (SSH) access**, and then select **Host Based Authentication.**

6. Click **Run Now**.

mxagentconfig

Use one of the following commands from a command prompt:

mxagentconfig -a -n <hostname> -u administrator -f <file_with_administrator_password>

or

mxagentconfig -a -n <hostname> -u administrator -p <administrator_password>

This is shown in Figure 20.

Note: Using the -p option exposes the password through **ps** output. Therefore, HP recommends using the **-f** option (with a file only readable by administrator, and containing only the managed system administrator password) when using **mxagentconfig -a**.

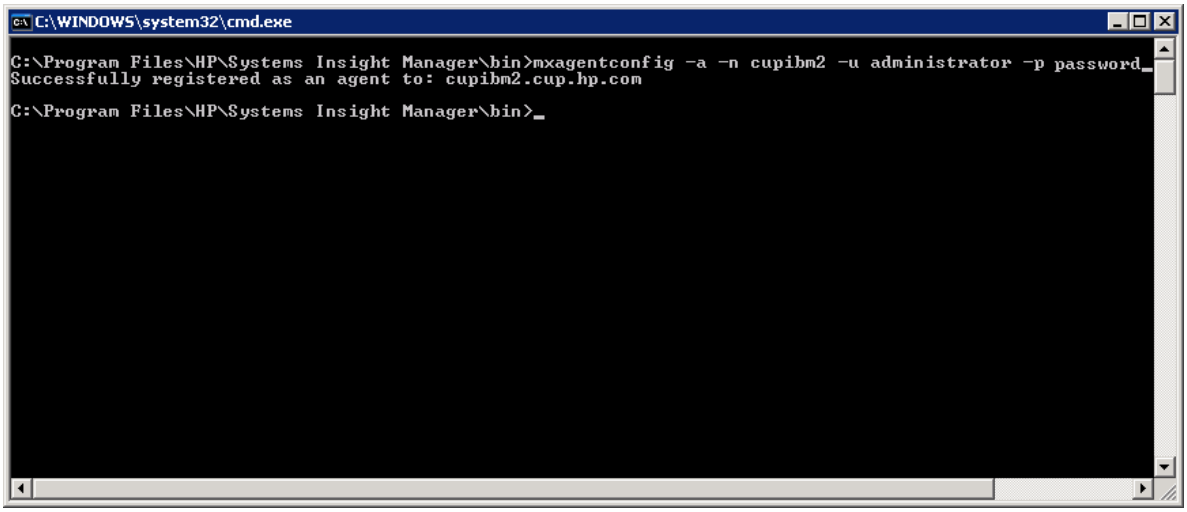

Figure 20 - Successful registration of IBM managed node to HP SIM.

Run a tool from the command prompt to verify the successful configuration of SSH. See Figure 21.

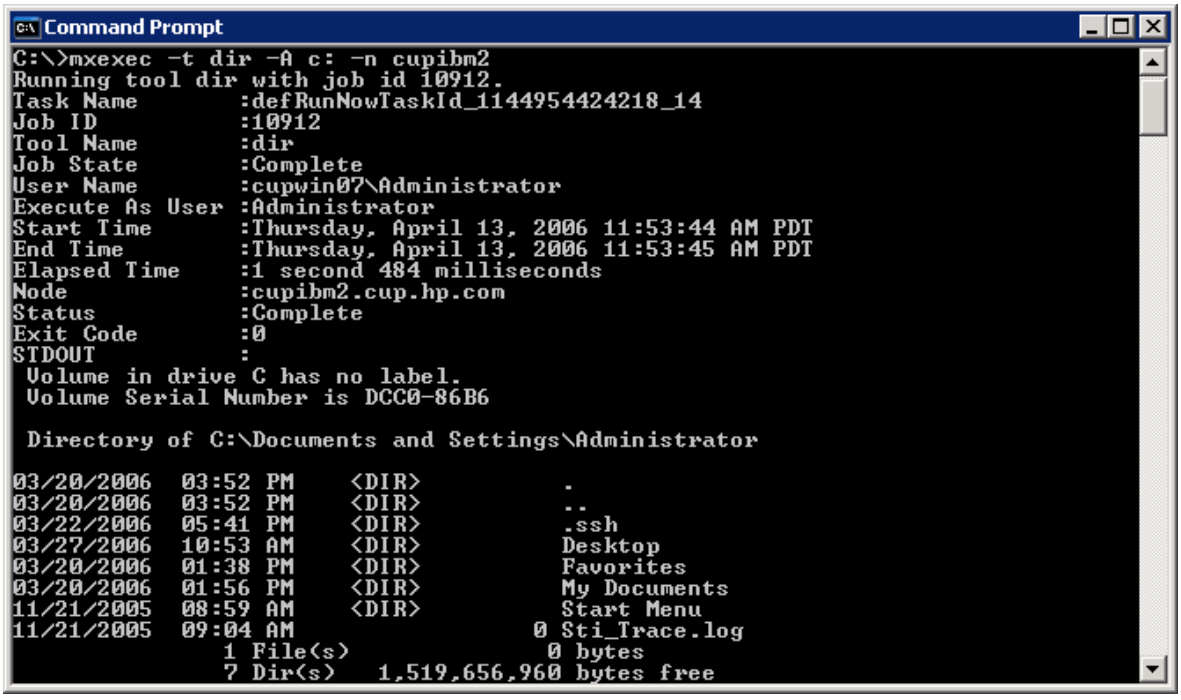

Figure 21 - SSH verified by executing the command "mxexec –t dir –A c: -n cupibm2".

Setting global protocol settings

Configuring the protocol defines how HP SIM will communicate with managed systems, including any passwords needed.

To configure the protocol settings:

1. In HP SIM, select **Options**>**Protocol Settings**>**Global Protocol Settings**. The **Global Protocol Settings** page appears. Figure 22 shows the navigation path.

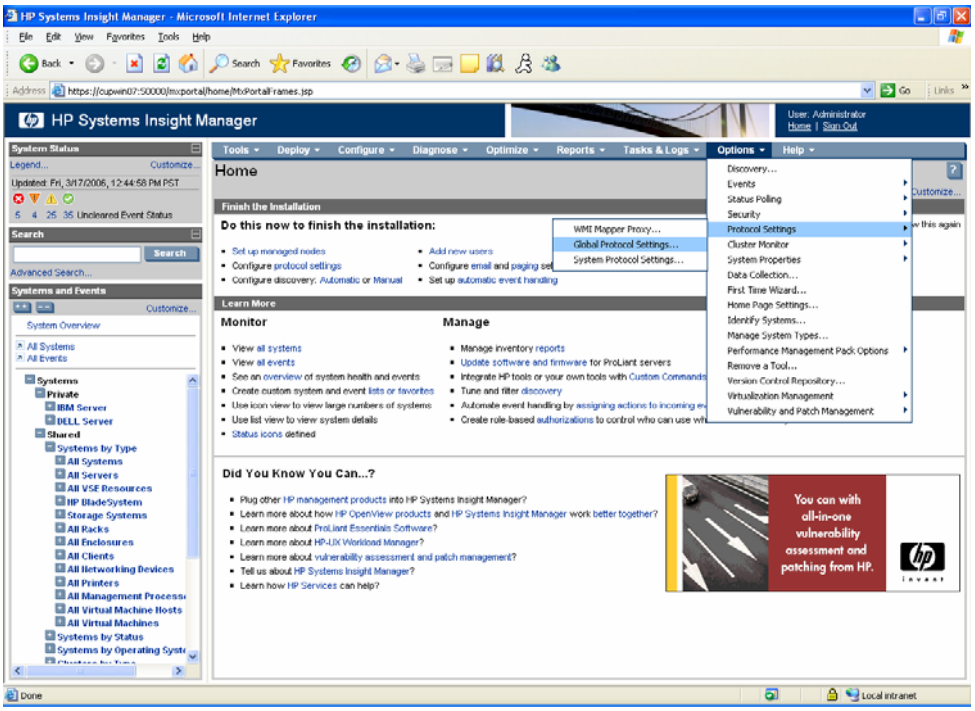

Figure 22 - Navigate to Options > Protocol > Global Protocol Settings.

2. In the **Default WBEM settings** section, select **Enable WBEM** to allow *Web-Based Enterprise Management* (WBEM) requests to be sent. **Enable WBEM** is enabled by default. Enter as many default user names and passwords as needed. For Windows-based systems, the user name should include the domain name, for example, *domainname\username*. Be sure that WMI services are set to start automatically.

   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.

3. 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, which is the default, for proper management and discovery of systems.

4. In the **Default SNMP settings** section, select **Enable SNMP**, which is the system default, and set the **Default time out** and **Default retries**. If some systems are managed over a WAN or satellite link, use a larger timeout (for example, ten seconds) with at least two retries. For a LAN, a shorter time out can be used. These settings can also be configured on a single-system basis.

5. Enter the **Default write community string**. This value is case-sensitive. Only a few tools need this option set. Community strings are case-sensitive.

6. 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.

7. Click **OK** to accept the settings. Steps 2 through 6 are illustrated in Figure 23.

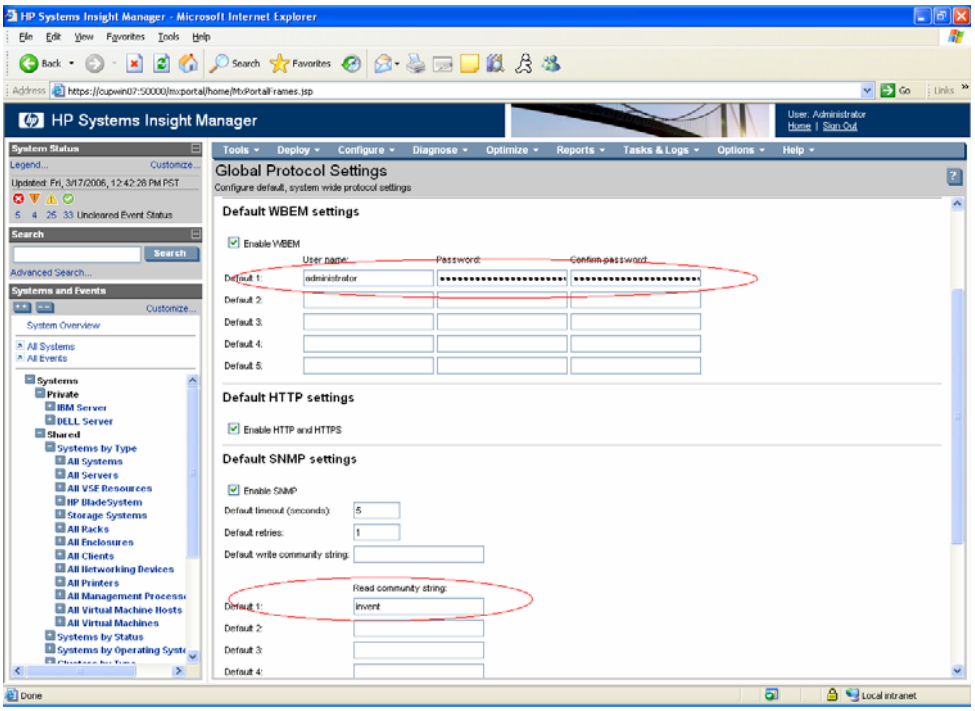

Figure 23 - Populate WBEM username: password and SNMP read community string.

HP SIM is now ready to run auto discovery.

Appendix 1: Protocol Overview

HTTPS

HTTPS is simply HTTP over SSL, a protocol that supports sending data securely over the web. HTTPS is used to access WBEM data from the managed system as explained below.

SNMP

SNMP is a common protocol used for managing many different types of systems on complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant systems run software packages called agents, which store data about the systems they are running on 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 only supports SNMP v1 MIBs and does not support SNMP v2 MIBs.

HP SIM keeps a database of read and write community names for managed systems running SNMP. Community names are case dependent and must exactly match those configured on the management systems. The SNMP community names and passwords can be set from HP SIM's CLI or GUI. HP SIM itself does not use SNMP SetRequests, and therefore, does not require an SNMP write community string. However, on the managed system itself, SNMP read-write or read-create strings are used for intra-agent communication, for example, Insight Agents to Version Control Agent, so a read-write or read-create string must be present. HP SIM does not need to know this as it does not use it.

Without a read-write or read-create string on the managed server, the **Server Role** field cannot be entered and saved, thresholds can not be saved, and Version Control software updates can not be done. By default, the supported operating system platforms have SNMP SetRequests disabled.

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 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

Web-Based Enterprise Management (WBEM) is an industry standard that simplifies system management over a network. 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 or applications 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 HP SIM's CLI or GUI. HP SIM uses Hyper-Text Transport Protocol Secure (HTTPS) to access WBEM data to provide 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 DCOM and NT security.

For more information

For more information on HP SIM visit the HP website at the following URL:
http://www.hp.com/go/hpsim

Call to action

Please send comments about this paper to: TechCom@HP.com.

422793-001 May 2006