# HP Proliant Essentials Vulnerability and Patch Management Pack

## Installation Instructions

**Legal notices**

Part number: 367561-006
Sixth edition: July 2007

000000- 000

## Overview

HP ProLiant Essentials Vulnerability and Patch Management (VPM) Pack extends the functionality of HP Systems Insight Manager (HP SIM) to provide vulnerability and patch management for target systems.

This document provides basic information about installing and using Vulnerability and Patch Management Pack. Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server (a shared configuration), or each component can be installed on a separate server (a distributed configuration).

For detailed infrastructure, installation, configuration, and usage information, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.

## Prerequisites

The following prerequisites must be met to properly install Vulnerability and Patch Management Pack.

### VPM server requirements

The VPM server, the server on which the Vulnerability and Patch Management Pack software is installed, must meet the following hardware and software requirements. Requirements listed for the VPM server are independent of requirements for HP Systems Insight Manager (HP SIM) and any other applications that coexist on the VPM server. For specific hardware and software requirements for the HP SIM server, see the *HP Systems Insight Manager Installation and User Guide*.

- The following operating systems are supported:
  - Microsoft® Windows® 2000 Server SP4
  - Windows Server™ 2003 SP1 or later
  - Windows XP Professional SP2
- Microsoft Internet Information Services (IIS) 5.0 or later must be installed and running

**IMPORTANT:** HP strongly recommends enabling HTTPS if HP SIM and Vulnerability and Patch Management Pack are installed on separate servers. To configure HTTPS service, see http://support.microsoft.com/?kbid=324069.

- TCP/IP, with DNS properly configured so that system names can be resolved to IP addresses
- The following applications are available either on the VPM server or on the network:
  - HP SIM 5.1 or later, installed and running on a Windows server with Windows Management Instrumentation (WMI) Mapper
  - Mozilla Firefox 2.0 or Microsoft Internet Explorer 6.0 or 7.0
  - Adobe® Acrobat® Reader 3.x or later (to view scan results)
- Any HP ProLiant server with:
  - At least 512 MB RAM
  - 1.5-GHz or higher processor
  - 1 GB available disk space for Vulnerability and Patch Management Pack (150 MB in the TEMP directory for installation)
  - Additional disk space for scan reports and patches
  - New Technology File System (NTFS)
  - DVD-ROM drive

## HP Systems Insight Manager

HP SIM 5.1 or later must be installed and running in the server environment to properly install and use Vulnerability and Patch Management Pack. HP SIM must be installed on a Windows server.

If you are not currently running HP SIM 5.1 or later, select one of the following migration paths depending on your server environment. For server environments currently using:

- **Systems Insight Manager 4.2**—Install HP SIM 5.1 or later.
- **Systems Insight Manager 4.1**—See the *HP Systems Insight Manager Installation and User Guide* to upgrade to HP SIM 5.1 or later.
- **Insight Manager 7**—See the *HP Systems Insight Manager Installation and User Guide* to upgrade to HP SIM 5.1 or later. Use the provided data migration tools to migrate key management data and configuration settings.
- **All other server environments**—See the *HP Systems Insight Manager Installation and User Guide* to install HP SIM 5.1 or later.

For additional information about HP SIM, see http://www.hp.com/go/hpsim.

## Installating Vulnerability and Patch Management Pack

### Preinstallation steps

A new version of Vulnerability and Patch Management Pack is automatically installed over a previous version. Any scheduled tasks, scan reports, and patch updates are retained.

1. Determine the Vulnerability and Patch Management Pack infrastructure for your server environment. Vulnerability and Patch Management Pack and HP SIM can be installed together on a single server (a shared configuration) or on separate servers (a distributed configuration).
2. Be sure to have the following items available before beginning the installation:
   - Location and credentials for HP SIM (user name, password, and domain)
   - Credentials for the VPM server if you are installing on a server other than the HP SIM server
   - Credentials for the Microsoft SQL Server database if an existing SQL Server database will be used
3. Be sure HP SIM 5.1 or later and IIS are installed, properly configured, and running.

### Installing from the Insight Control Management DVD

**IMPORTANT:** HP SIM restarts after the installation of Vulnerability and Patch Management Pack.

**NOTE:** The installation might take up to 20 minutes, depending on the speed of the server.

1. Insert the Insight Control Management DVD into the DVD-ROM drive of the intended VPM server. The ProLiant Essentials Software End User License Agreement appears. Read the agreement, and click **Agree**.
2. To open the configuration wizard and initiate the installation process, at the Welcome screen, click **Run Installer**, or to do a manual installation, click the **Products** tab.
3. The prerequisites for installing Vulnerability and Patch Management Pack are listed. Verify that all requirements are met before you perform the installation, and click **Next**.
4. Select a location for the installation files, and click **Next**.
5. At the Software Selection screen, select **HP ProLiant Essentials Vulnerability and Patch Management Pack**, and click **Next**.
6. Follow the onscreen instructions, entering your user specific information when prompted

### Installing from the VPM download website

1. After downloading Vulnerability and Patch Management Pack, double-click **setup.exe** to start the installation.
2. Follow the onscreen instructions, entering your user specific information when prompted. Enter the same credentials used when installing HP SIM.
3. When the installation is complete, log in to HP SIM from an account with administrator privileges to access Vulnerability and Patch Management Pack

### Installing the VPM Acquisition Utility (optional)

The VPM Acquisition Utility can be installed on a system with Internet access, enabling patch acquisitions and vulnerability updates without requiring the VPM server to be directly connected to the Internet.

**IMPORTANT:** In both a distributed and shared configuration, the VPM Acquisition Utility cannot be installed on the VPM server nor the HP SIM Central Management System (CMS).

For requirements for the system on which the VPM Acquisition Utility is installed, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*.

To install the VPM Acquisition Utility:

1. Insert the Insight Control Management DVD into the DVD-ROM drive of the system on which patch and vulnerability updates will be obtained. The ProLiant Essentials Software End User License Agreement appears. Read the agreement, and click **Agree**.

2. At the Welcome screen, click the **Products** tab, and then select **Vulnerability and Patch Management Pack** from Foundation Management Products.
3. At the top of the screen, under Vulnerability and Patch Management Pack, click **Install…**.
4. At the Welcome screen, click **Install**.
5. At the Software Selection screen, select VPM Acquisition Utility, and click **Next**.
6. Follow the onscreen instructions to complete the installation

## Post-installation configuration steps

After Vulnerability and Patch Management Pack is installed for the first time, perform the following steps to complete the configuration and install the latest vulnerability updates.

> NOTE: An administrator can add new users and set up existing users to access Vulnerability and Patch Management Pack. For instructions, see the *HP Systems Insight Manager Installation and User Guide.*

1. Log in to HP SIM from an account with administrator privileges.
2. Configure global Web Based Enterprise Management (WBEM) credentials to enable access to target systems
   a. Select **Options>Protocol Settings>Global Protocol Settings**.
   b. Configure settings for the \user account if Vulnerability and Patch Management Pack is located on the HP SIM server or for the DOMAIN\user account if Vulnerability and Patch Management Pack is on a separate server.
   c. Enter the Windows administrator account credentials in the Default 1 field, and enter the Red Hat administrator group credentials in the Default 2 field.
   d. Click **OK**.

> NOTE: If some target systems use individual administrator credentials, see the user guide for information about configuring System Protocol Settings.

3. Perform an automatic discovery to locate and identify target systems in the network that can be used with Vulnerability and Patch Management Pack. For information, see the *HP Systems Insight Manager Installation and User Guide.*
4. Modify the Vulnerability and Patch Management Pack settings:
   a. Select **Options>Vulnerability and Patch Management>Settings**.
   b. Select the source where patch and vulnerability updates will be obtained.
   c. Choose one of the following options:
      - If the VPM server has direct Internet access, select **Acquire updates from Internet** to use the VPM server to obtain updates.
      - If you use a proxy server, select the appropriate checkbox, and enter your configuration information.
      - If the proxy requires authentication, select the appropriate checkbox, and enter your user credentials. Only basic (not encrypted) authentication is supported.
   d. If the VPM server does not have Internet access, select **Acquire updates from local repository** to use the VPM Acquisition Utility on another system with Internet access to acquire updates. The update files can either be manually relocated to the VPM server or accessed from the network. Designate the directory or network path where the update files will be located in the Source path field. (Do not use a drive letter mapped to a network drive.) If necessary, enter user credentials to access the designated directory. The VPM server must have read access to the designated directory. Click **Apply**.
5. If Red Hat patch acquisitions will be run:
   a. Verify the Red Hat library, compat-libstdc++, is installed on all Red Hat target systems.
   b. Verify that each Red Hat target system to be patched has a valid subscription and license for the Red Hat Network, which are required for patch acquisitions. For information about subscribing to the Red Hat Network, see http://www.redhat.com.
   c. Log in to a Red Hat Enterprise Linux 2.1, 3, or 4 system as root.
   d. Execute the following command:

```
rhn_register
```

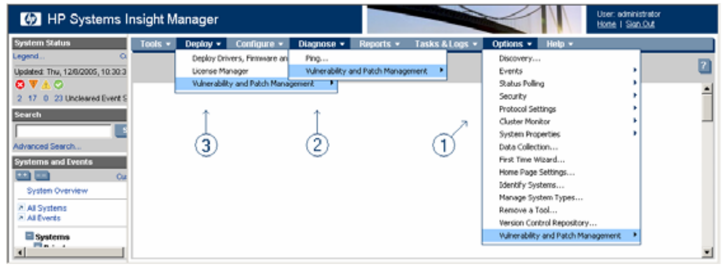
   e. Select **Existing**, and enter your user credentials.
   f. Enter a unique profile name for this machine (such as the IP address or host name).
   g. Exit the rhn_register application without applying any patches to the system.
   h. Copy the file created by the rhn_register tool from /etc/sysconfig/rhn/systemid to C:\Program Files\HP\VPM\radia\IntegrationServer\etc.
   i. Rename the systemid file to reflect the appropriate Red Hat distribution.
      - If the system that created the systemid file was running Red Hat Enterprise Linux 4 ES, rename the file “redhat 4es.sid.”
      - If the system that created the systemid file was running Red Hat Enterprise Linux 3 ES, rename the file “redhat 3es.sid.”
      - If the system that created the systemid file was running Red Hat Enterprise Linux 2.1 ES, rename the file “redhat 2.1es.sid.”
      - If the system that created the systemid file was running Red Hat Enterprise Linux 4 AS, rename the file “redhat-4as.sid.”
      - If the system that created the systemid file was running Red Hat Enterprise Linux 3 AS, rename the file “redhat-3as.sid.”
      - If the system that created the systemid file was running Red Hat Enterprise Linux 2.1 AS, rename the file “redhat-2.1as.sid.”
6. Acquire the latest Vulnerability and Patch Management Pack updates, either from the VPM server or using the VPM Acquisition Utility installed on another system. The first update process after the initial software installation might take a long time, depending on the number of patch sources selected and the quantity of updates available from each source.

> NOTE: HP updates and vulnerability scan definition files are always automatically downloaded.

   a. From the VPM server:
      - Select **Options>Vulnerability and Patch Management>Acquire Updates**.
      - Follow the onscreen instructions, selecting the appropriate update information for your server environment as prompted.
      - Click **Schedule**, and select a suitable time to acquire daily Vulnerability and Patch Management Pack updates. Updates might not be available daily, but scheduling the event daily ensures that critical updates are obtained promptly.
      - Select the **Run now** checkbox to run the initial patch acquisition, and click **Done**. Progress can be monitored at C:\Program Files\HP\VPM\Radia\IntegrationServer \logs\patch-acquire.log.
   b. By using the VPM Acquisition Utility:
      - Access the VPM Acquisition Utility from the selected system.
      - Follow the onscreen instructions, selecting the appropriate update information for your server environment as prompted.
      - Click **Run Now** to run the patch acquisition. Patch acquisition progress can be monitored at C:\Program Files\HP\VPM Acquisition Utility\logs\patch acquire.log.
      - When the acquisition process is complete, click **Done**.
      - On the VPM server, create a directory named “data” at C:\Program Files\HP\VPM\Radia\IntegrationServer. You can use a network share if the VPM server has read access to the share.
      - Copy downloaded files from the VPM Acquisition Utility server destination directory to the VPM server data directory.
      - From HP SIM, configure your import setting by selecting **Options>Vulnerability and Patch Management>Settings**.
      - Start the import process by selecting **Options>Vulnerability and Patch Management>Acquire Updates**.

## The Vulnerability and Patch Management Pack interface

From the HP SIM toolbar menu, select **Vulnerability and Patch Management Pack installation** to choose a menu.



| Menu | Action |
|---|---|
| 1 | Configure settings and acquire updates. |
| 2 | Perform or customize vulnerability scans, and view scan results, patch installation status, patches installed by VPM, patch reboot status, and the patch repository. |
| 3 | Deploy or remove patches and fixes, validate installed patches, and deploy the VPM Patch Agent. |

## Licensing systems

Vulnerability and Patch Management Pack requires one Insight Control Environment license for each target system being managed.

> IMPORTANT: Insight Control Environment includes a combined license key covering multiple ProLiant Essentials.

> IMPORTANT: After a license is applied to a specific system, the license cannot be removed or transferred to another system.

## Scanning for vulnerabilities

1. Select **Diagnose>Vulnerability and Patch Management>Scan>Scan for Vulnerabilities**.
2. Select the target systems to scan by selecting a group from the dropdown list or by selecting the checkbox next to individual systems.
3. Click **Apply**.
4. Verify that the correct target systems appear in the lists, click **Add Targets** or **Remove Targets** if it is necessary to reselect target systems, and then click **Next**.
5. If any selected systems are unlicensed or licensed with a time limited license, permanent licenses can be applied at this time. If licenses are available, select any unlicensed system in the list to license, and click **Apply License**.
6. Click **Next**.
7. Enter a name for the vulnerability scan, select a scan definition, and click **Run Now** to run the scan immediately.
8. View scan results after the task completes by clicking the system status icon or viewing the VPM Events list.

For additional information about vulnerability scanning and creating customized scans, see the user guide.

## Deploying patches and fixes

To deploy patches and configuration fixes after a vulnerability scan is complete:

1. Select **Deploy>Vulnerability and Patch Management>Patch-Fix Based on a Scan**.
2. Select the completed vulnerability scan, and click **Next**.
3. Select the vulnerabilities to patch or fix, and click **Next**.
4. Select the systems on which to apply patches or fixes, and click **Next**.
5. Designate when the patched systems should be rebooted, and click **Run Now** to deploy patches or fixes immediately.
6. View task results in the VPM Events list after the task completes.

For additional information about deploying patches, see the user guide.

# HP services and technical support

Vulnerability and Patch Management Pack is offered exclusively as a part of Insight Control Environment and Insight Control Environment for BladeSystem. Starting in July 2007, Insight Control Environment suites will include one year of 24 x 7 HP Software Technical Support and Update Service.

This service provides access to HP technical resources to help you resolve software implementation or operational issues. This service also provides access to software updates and reference manuals either in electronic format or on physical media as they are made available from HP.

With this service, Insight Control Environment and Insight Control Environment for BladeSystem customers will benefit from expedited problem resolution and proactive notification and delivery of Insight Control Management software updates.

To activate your HP Software Technical Support and Update Service for Insight Control and Insight Control Environment for BladeSystem, you must register your software purchase through the HP website at http://www.hp.com/go/ice.

**Failure to register your service will jeopardize service fulfillment.**

Your Service Agreement Identifier (SAID) will be delivered to you after registration. After you have received your SAID, you can go to the software update manager (SUM) web page to view your contract online and elect electronic delivery (in addition to standard media-based updates). For more information about this service, see http://www.hp.com/services/insight.

In addition to the new Software Technical Support and Update Service, HP also offers a number of additional software support services, many of which are provided to our customers at no additional charge.

- **Warranty**—HP will replace defective delivery media for a period of 90 days from the **date of purchase**. This warranty applies to all Insight Control Management, HP Systems Insight Manager, and ProLiant Essentials products.
- **Startup technical software support**—Phone support is available to help you with basic installation, set-up, and usage questions. This support is provided by the knowledgeable HP Insight Control Management and Systems Insight Manager specialists' team and is available for no additional charge up to 90 days from the **date of purchase** of your server. For support in the U.S., call 1-800-HP-INVENT (1-800-474-6836). (When prompted, say "Insight Manager, P2P, and SMP.") HP Worldwide support numbers for HP SIM, P2P, and SMP are available at http://www.hp.com/country/us/en/ wwcontact.html.
- **Join the discussion** (http://forums.itrc.hp.com)—The HP Support Forum is a community-based, user-supported tool for HP customers to participate in discussions about HP products. For discussions related to Insight Control and ProLiant Essentials software, click Management software and system tools.
- **Software and Drivers download pages** (http://www.hp.com/support)—These pages provide the latest software and drivers for your ProLiant products.
- **Management Security** (http://www.hp.com/servers/manage/security)—HP is proactive in its approach to the quality and security of all its management software. Be sure to check this website often for the latest downloadable security updates.
- **Obtain the latest SmartStart** (http://www.hp.com/servers/smartstart)—The SmartStart, Management, and Firmware CDs are now available for download by registering at the SmartStart website. If you wish to receive physical kits with each release, you can order single release kits from the SmartStart website. To receive proactive notification when SmartStart releases are available, subscribe to Subscriber's Choice at http://www.hp.com/go/subscriberschoice.