

# HP ProLiant Essentials Vulnerability and Patch Management Pack Release Notes



Supported platforms .....	2
What's new in version 2.1 .....	2
What's new in version 2.0.3 .....	2
What's new in version 2.0.2 .....	2
What's new in version 2.0.1 .....	2
What's new in version 2.00 .....	2
Changes in version 2.1 .....	3
Changes in version 2.0.3 .....	3
Changes in version 2.0.2 .....	4
Changes in version 2.0.1 .....	4
Changes in version 2.00 .....	4
Installation notes .....	5
Other environment setup requirements .....	5
Important notes .....	7
Limitations and known issues in version 2.1 .....	8
For more information .....	11

## Supported platforms

For information about supported platforms and system prerequisites, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix* located on the HP Management CD or HP Insight Control Management DVD.

### What's new in version 2.1

- Vulnerability and Patch Management Pack (VPM) version 2.1 resolves some existing issues with the installer and the tool.
- VPM version 2.1 supports RedHat Linux AS 2.1, 3, and 4 as target operating systems.
- VPM version 2.1 supports Firefox versions 2.0 or later.
- VPM version 2.1 requires HP SIM version 5.1 or later.
- A new End User License Agreement (EULA) is available.

### What's new in version 2.0.3

- VPM version 2.0.3 resolves some existing issues with the installer and the tool.
- VPM version 2.0.3 supports HP SIM 5.1.
- VPM version 2.0.3 supports Microsoft Internet Explorer (IE) 7.

**NOTE:** VPM is not available on the HP Management CD version 7.60 or later. VPM is included on the Insight Control Management DVD.

### What's new in version 2.0.2

- VPM version 2.0.2 resolves some existing issues with the installer, the uninstaller, and the tool.

**NOTE:** This version encompasses the content of VPM SP1 and SP2 for version 2.0.1.

### What's new in version 2.0.1

- VPM version 2.0.1 resolves some existing issues with the installer and uninstaller.
- The English version of VPM version 2.0.1 can now be installed on a Japanese operating system. Scanning and patching Japanese targets is also supported. Information about Japanese support can be found at <http://www.hp.com/jp/servers/vpm>.

**NOTE:** Kanji characters cannot be used in passwords, directories, or scan names.

### What's new in version 2.00

- VPM version 2.00 is a required upgrade for current users. The installer for VPM version 2.00 completes a new installation or upgrades previous versions. All users are required to run a full patch acquisition to update the patch database and download the latest VPM patch agent. Microsoft® recently introduced Microsoft Update Catalog, a centralized repository for all Microsoft patches. Patches for new products introduced by Microsoft are only available through this new repository. Because of this change, VPM has adopted this new repository as a source for the patches being provided by Microsoft.

- HP SIM 5.0 SP2 or later is supported. To download the latest patch or HP SIM installation, see <http://www.hp.com/go/hpsim>.
- New patch installation status reports are available. Gain new insight with status reports created by patch, system, or search filter (advisory, system, or patch status).
- Microsoft SQL Server database is supported. To use a SQL Server database, the database must be installed before installing or upgrading VPM. Users upgrading from a previous version of VPM have the option to switch database types.

## Changes in version 2.1

- Added target operating system support for RedHat Linux AS 2.1, 3, and 4.
- Added support for Firefox 2.0.
- Requires HP SIM version 5.1 or later.
- Created a menu item to access the VPM web page at [www.hp.com](http://www.hp.com).
- Acquisition utility uninstaller removes only its own files and folders.
- Acquisition utility is correctly uninstalled from system.
- VPM uninstaller removes only its own files and folders.
- Resolved the occasional occurrence of system crash in View Patch Repository after acquisition from the Internet. All values from the database are now validated and any exception is handled properly.
- The message to set the proxy information is highlighted (bold) in order to better warn the user to verify if the proxy information is set.
- The VPM logs contain the VPM version number: (vpmsetup.log (install), vpmlog.log (webapp), vpsimsetup.log (uninstall)).
- The RADIA logs placed in c:\VPMSetupLogs are moved to the correct log folder in order to better interact with ICM.
- VPM no longer allows an attempt to deploy an agent for systems without an IP address.
- The message to access mapped drive letters is more user friendly.
- Only one advisory entry is shown on vulnid.
- Scan report are now correctly opened from the CMS system.
- VPM is correctly upgraded to the proper location.
- Scan now works on HP SIM private collections.
- Japanese strings now correctly appear on Scan pages.
- The use of a proxy server can now be disabled correctly.
- VPM executable package now displays the correct version information.
- A new property "timeout" was added to the VPM settings.xml file so that you can control the value for the acquisition HTTP timeout.

## Changes in version 2.0.3

- Added support for HP SIM 5.1.
- Added support for IE 7.
- VPM now stores its proxy configuration inside HP SIM. This new method avoids redundant proxy settings being stored in multiple places. No changes were made to the VPM user interface, so this change is transparent to the user.

- A message dialog was removed from the installer, which indicated the database configuration was changed when, in fact, it was not. This message was related to the changes on the Microsoft data feed infrastructure and is not valid anymore.
- Fixed an issue where the passwords supplied during Vulnerability and Patch Management Pack installation could not end with blank characters.
- Fixed an issue where scheduled tasks (which run in the future) were being executed even with expired system licenses.
- Fixed an issue where some log files presented open password strings.
- Fixed an issue where some HTML code was showing on the screen.
- Fixed an issue where a large set of patches was applied at once, causing Vulnerability and Patch Management Pack to malfunction.

## Changes in version 2.0.2

- The installer blocks upgrades from version 1.x. If an upgrade from version 1.x is required, upgrade to version 2.0.1 first (which can be downloaded from VPM website at <http://www.hp.com/go/vpm> and then to version 2.0.2 (or later).
- Included HP Vulnerability and Patch Management Pack Critical Update (SoftPaq SP33092), which fixes the issue in which the VPM license page cannot license a target running the Red Hat Linux 4.0 operating system, was incorporated as part of this release.
- Included HP Vulnerability and Patch Management Pack Critical Update (SoftPaq SP33202), which fixes the issue in which “view patch installation status by patch,” “view path installation status by search filter,” and “view patch installation status by system” do not return results when connected to a remote database, was incorporated as part of this release.
- VPM Patch Agent installs correctly when HP SIM and VPM are installed on a server running a Spanish or German Microsoft Windows® system.
- It is not possible to perform a scan on a system that does not contain a valid IP address.
- A scan with a single quote in its name does not appear as Aborted in View Scan Results.
- The STAT scan engine does not report an exception when installed on the F: drive.

## Changes in version 2.0.1

- The Radia Management Agent (RMA) has been updated to eliminate potential to hang on some target systems or the HP SIM Central Management Server (CMS) when they are rebooted. If you disabled the RMA service on a target system as a workaround, you can redeploy the VPM Patch Agent or reset the server to start automatically after you have installed Vulnerability and Patch Management Pack 2.0.1. The next patching session for the target system automatically updates the RMA service.
- The installer allows passwords with spaces.
- The uninstaller stops all services using SNMP to remove the EDMSNMPX.DLL file.
- The missing license.nvd file is included in the VPM Acquisition Utility.

## Changes in version 2.00

- Support is available for the new Microsoft patch repository, Microsoft Update Catalog. The patch acquisition process using VPM remains unchanged.
- Microsoft Windows NT® 4.0 patch acquisitions are no longer supported.

- The link for obtaining STAT® Scanner updates has changed. If your firewall is configured for access to HP, change your firewall settings to allow access to the <https://ftp.hp.com/pub/essentials/vpm> directory to ensure that VPM can successfully continue to obtain updates.  
**NOTE:** This URL will not work as shown here, but when configured properly, it will provide VPM access to the required files. To ensure the firewall is correctly configured for VPM, see <https://ftp.hp.com/pub/essentials/vpm/versions.xml>.
- Some advisories are listed as MS-KBxxxxx. This new naming convention is for security rollups, bundled patches that are not considered service packs. Vulnerability and Patch Management Pack now supports distribution and management of these security rollups.

## Installation notes

- For information about the installation and setup of VPM, see the HP ProLiant Essentials Vulnerability and Patch Management Pack Installation Instructions and the HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide.
- Microsoft Internet Information Server (IIS) 5.0 or later must be installed and running on the VPM server, the server on which VPM is installed. For information about configuring a secure HTTPS connection between Vulnerability and Patch Management Pack and HP SIM, see the HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide and <http://support.microsoft.com/?kbid=324069>.  
**NOTE:** HP recommends an HTTPS connection when VPM and HP SIM are installed on separate servers.
- HP SIM 5.1 or later and WMI Mapper must be installed and running before installing VPM. HP SIM is available at <http://www.hp.com/go/hpsim>.
- VPM must be installed using an account password that does not contain curly braces (“{” or “}”). To change the installation account password before installing VPM, see the HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide.
- If a version of Microsoft Data Access Components (MDAC) earlier than 2.5 SP1 is loaded on the VPM server, MDAC 2.5 SP1 is automatically installed and the system is rebooted. Vulnerability and Patch Management Pack installation must be restarted.
- HP SIM is restarted at the completion of Vulnerability and Patch Management Pack installation or uninstallation.
- SNMP service must be started on the HP SIM system to facilitate the HP SIM discovery and identification of target systems.

## Other environment setup requirements

- To install VPM, your Internet security settings must (temporarily) be set to Low.
- When installing VPM in a distributed environment where servers are not members of a Windows Domain (that is, servers are part of a Workgroup), the VPM installer requires the install account to have the “Replace a process level token” and “Create a token object” permissions enabled in the Windows Policy. If these permissions are not enabled, the VPM installation might fail.
- These permissions can be added through **Control Panel -> Administrative Tools -> Local Security Settings -> Local Policies -> User Rights Assignment**. In this window, double-click on the “Replace a process level token” item, click the **Add User or Group** button and add your user name or Administrator group. If these permissions are changed for the current logged account, log out and log in again with this account before restarting the VPM install process.

- If the target systems, the systems to be managed by HP SIM and VPM, are not defined in a DNS server, complete the following steps before installing HP SIM to allow HP SIM to correctly discover and identify these systems.
- Update the hosts file (located at C:\%system%\drivers\etc on the HP SIM server) with the IP address, short name, and full name of these systems.
- Configure the primary DNS suffix.
- Include the VPM server if Vulnerability and Patch Management Pack is installed on a separate server from HP SIM.
- Microsoft Internet Explorer 6.0 or later must be used to access HP SIM. Adobe® Reader 3.x or later must be installed on the system used to view vulnerability scan results. To view the scan result .pdf files, validate the following browser settings:
- Internet Access Security is set to **Medium**.
- Under Advanced Options, the **Do not save encrypted pages to disk** checkbox is **not** selected.
- If the VPM server is inside a firewall and patches will be acquired from the VPM server, the firewall must allow FTP and HTTP to successfully perform the patch acquisitions.
- If the VPM server does not have Internet access or the firewall blocks either FTP or HTTP communication, the VPM Acquisition Utility can be used on a separate system to acquire patches. The system on which the VPM Acquisition Utility is installed must have Internet access, and the firewall must allow FTP or HTTP communications.
- Upgrade the VPM Acquisition Utility when Vulnerability and Patch Management Pack is upgraded.
- If Microsoft Windows XP systems not joined to a Windows domain are target systems in a vulnerability scan or patch-fix operation, Simple File Sharing must be disabled on those systems for these scanning/patching functions to be successful. For more information, see <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q304040>.
- Windows XP systems with Service Pack 2 installed which are used as target systems in a patch-fix operation must place the RADEXECD and NVDKIT programs on the firewall exception list. These programs open sockets that must be accessible to deploy patches.
- When scanning a target system that is a domain controller, be sure that the credentials for accessing that system include the domain name and user name since there are no local accounts on a domain controller.
- A subscription to the Red Hat Network and additional setup procedures are required to acquire patches from the Red Hat Network. To successfully deploy patches to Red Hat Linux target systems, a systemid file must be created for each version of Red Hat patches and a required library must be installed on the target systems. For information, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.
- VPM allows credentials with administrator-level privileges to access remote systems. In some environments, it might be possible to spoof a remote system causing a “man-in-the-middle-attack.” In a Windows environment, stealing the credentials used to access a remote system is highly unlikely because Windows authentication uses a one-way hashing function to encrypt the credentials. In a Linux environment, SSH provides a similar mechanism over an encrypted communications channel. For additional information about configuring HP SIM SSL and SSH features for use with the HP Insight Management Agents, see the HP SIM documentation at <http://www.hp.com/go/hpsim>.
- Red Hat Enterprise Linux 3 automatically configures a firewall when installed. To patch these systems, the firewall must be disabled by executing setup to launch the user interface on the target system and disabling the firewall from the user interface.

## Important notes

- For information about setting up credentials to access the target systems, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Installation Instructions*. Scanning and patching target systems require administrator-level access.
- The VPM Patch Agent is automatically deployed when a target system is first licensed. If the system is not accessible or the credentials are not set up correctly, the VPM Patch Agent might not be installed. You can verify the installation by viewing the VPM events listed in the HP SIM event log. If necessary, manually install the VPM Patch Agent after correcting the credentials by selecting **Deploy>Vulnerability and Patch Management>VPM Patch Agent**.
- To use VPM immediately, you might want to select only one operating system the first time patches are acquired to minimize acquisition time. The acquisition of the first operating system and scan definitions can take approximately two hours. A patch acquisition of every operating system can take 4 to 6 hours to complete the first time the acquisition is run. The start of the patch acquisition event is displayed in the HP SIM event log.
- If you use a proxy in your environment, be sure to set up the proxy settings before using Vulnerability and Patch Management Pack to acquire updates. Set up the proxy settings by selecting **Options>Vulnerability and Patch Management>Settings**.
- Patches that have been superseded are not acquired. If you apply a patch that has been superseded, the superseding patch is applied instead.
- When applying patches to a RedHat target system, the following steps must be verified first:
  1. It must be possible to logon to the target system using SSH (such as, using the Putty application).
  2. Both target and CMS systems must recognize each other on the Intranet (that is, the ping command must reach each other).
  3. HP SIM global settings must contain the right set of target system credentials.
  4. The hosts file must be correctly configured on both ends:
    - a. On the target system (RH), the file is located at `"/etc/hosts"`
    - b. On the CMS system (Windows), the file is located at `"%windir%\system32\drivers\etc\hosts"`
  5. The SNMP package must be installed on the target system.

**IMPORTANT:** The Import Patches function does not work when remote paths are mapped to local drive letters. For example, if a network path [\\server\path](#) is locally mapped as "X:", using this drive letter for patch acquisition will cause Vulnerability and Patch Management Pack to display an error message stating that there is no valid repository available even if the patches are actually there. The full network file path (<[\\server\path](#)>) must be used to point to the folder located on the system containing the repository.

## Limitations and known issues in version 2.1

- The Radia Management Agent (RMA) does not correctly uninstall from Windows target systems. If the RMA is removed using the **Add or Remove Programs** option in the Control Panel, it may be removed successfully from the list, but its services continue to run, even if the target system is rebooted.
- A message similar to the following is written to the Windows Event Log and can appear as a message box occasionally when the STAT Scanner components are installed, updated, or uninstalled:

**Application popup w3wp.exe - Application Error: The instruction at 0x7c82f350 referenced memory at 0x02bf0824. The memory could not be written.**

This error can occur during a patch acquisition operation (in which STAT Scanner is updated with the latest vulnerability database). It could also show up during VPM install, update, or uninstall operations (in which STAT Scanner is installed, updated, or uninstalled).

This error can be ignored because STAT Scanner component w3wp.exe sometimes ends abnormally when a new version is put into place. In case this error shows as a message box, click the **OK** button for the operations to proceed correctly.

- VPM allows upgrades to a third server. For example, if HP SIM was installed on server A, and an older version of VPM was installed on a server B, the upgrade allows for VPM installation on a server C. The VPM database is updated for the new installation on server C, and all the patch data from the older installation on server B is lost.
- If the VPM database is located in the current domain, it is possible to use the Connect using Windows Authentication installer option with valid Windows user credentials to validate the database. Otherwise, if the VPM database is located in another domain, do not use this option. Instead, use valid SQL user credentials to validate the database.
- Patch acquisitions can generate events containing HTTP 300 errors for some older Microsoft patches. For example:  
Error downloading patch data for Bulletin MS02-050 at URL  
<http://www.microsoft.com/ntserver/terminalserver/downloads/critical/q329115/default.asp> error code 300  
HP is working to correct the metadata for these older patches. However, this maintenance is ongoing.
- If an HP SIM discovery or identification task is in progress when target systems are licensed for Vulnerability and Patch Management Pack, target systems that have an IP address as their name at the time of licensing that are later identified with a system name might become unlicensed and have to be licensed again. Avoid this situation by allowing discovery and identification tasks to complete before licensing the target systems. Another alternative is to complete the following steps to properly set up the name in HP SIM for the target systems:
  - a. Display the All Systems list.
  - b. Double-click the node name to display its system page.
  - c. Click the **Links** tab.
  - d. Select **Edit System Properties**.
  - e. Enter the desired system name in the preferred system name field.
  - f. Click **OK**.



- When a SQL Server database is used, VPM database credentials are not updated by the Change VPM Credentials utility. There is currently not a supported method for changing the credentials manually. An engineering advisory will be issued at a later time with instructions to change the database credentials.
- When licensing a VMware system with a serial number longer than 30 characters, a limitation in the HP SIM License Manager causes the VPM license to function incorrectly on this system, as well as any other HP SIM node licensed by serial number. The VMware target host is continually considered unlicensed, and must be relicensed each time the system is selected for a licensed operation. This issue will be resolved in a future release of HP SIM.
- Some systems might be incorrectly identified and appear capable of being licensed in both the VPM column and licensing pages. Before applying a license to a system, be sure the system is supported by referring to the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*.
- Some Microsoft patches, such as MS04-025, do not appear in the Control Panel after being installed. To verify installation, run the vulnerability scan again.
- Microsoft Windows File Protection maintains backup copies of critical system files in a hidden directory named "dllcache" so that these critical files can be replaced if they are removed for any reason. Uninstalling an application can remove some of these critical files. In rare situations, you might be prompted to insert the installation media into a system when a patch is being installed and a backup file is missing or corrupted. This condition can also occur when installing software other than patches.
- The installation fails if curly braces ("{" or "}") are used in the account password used to install VPM. The account password must be changed to remove those characters before installation. The password can be changed back to the original password after Vulnerability and Patch Management Pack installation is complete. For details, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*.
- A generic Radia internal error appears in the HP SIM event log if the patch repository is viewed before a patch acquisition is performed.
- Resolutions for some fixable vulnerabilities cause the local security policy to log more events. If the logs are configured not to overwrite old events, the event log can become full and cause abnormal system behavior. Read and understand the effects of all fixes before applying them.
- Acquiring patches from the Red Hat Network requires the network connection to remain connected for the duration of the acquisition operation. If the network goes down, the patch acquisition must be restarted.
- If a group of systems is selected to receive configuration fixes and some systems in that group do not require all the fixes, the fix events are still displayed for those systems. However, Vulnerability and Patch Management Pack does not actually apply the fixes to those systems that do not require them.
- When applying fixes and patches based on a scan, VPM could possibly try to apply a fix that is not available for Linux systems (only patches are available for Linux systems). This might show an error event on the HP SIM event log and also on the Windows event log. This issue will be addressed in a future release of VPM; however, it does not affect the correct execution of VPM.
- If a patch causes a reboot when patching the system on which HP SIM is running, the **Diagnose>Vulnerability and Patch Management>View patch installation status>View Patches Installed by VPM** list might continue to indicate Reboot Required. Select **Deploy>Vulnerability and Patch Management>Validate Install Patches** to update the installed patches list.
- If multiple systems are scanned as a group and many vulnerabilities exist, the Scan Detail report for the group might be too large to be generated. View the Scan Detail report for individual systems in the group.

- If a system has a Microsoft service pack installed that is not the final release, patches applied to that system might return the status "Not Applicable." Only official releases of service packs should be installed on a system being scanned and patched by Vulnerability and Patch Management Pack.
- Applying more than 100 patches in a single operation can cause a timeout to occur. HP recommends installing less than 100 patches at a time.
- The Back button in the web browser does not function properly. Use navigation buttons within the HP SIM and VPM pages.
- If a secure connection is configured between VPM and HP SIM by installing an IIS certificate, scanning no longer works if the certificate is later removed. To continue without renewing the certificate, uninstall and reinstall VPM.

## For more information

- <http://www.hp.com/go/vpm>
- *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*
- *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*
- *HP ProLiant Essentials Vulnerability and Patch Management Pack Installation Instructions*

© 2006, 2007 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.

Itanium is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

July 2007

