

# HP Client Automation Enterprise

## Release Notes

**Software version:** 7.90 / July 2010

This document provides an overview of the changes made to the HP Client Automation (HPCA) Enterprise components for the 7.90 release. It contains a bulleted list of new features and functionality for each component, information about the current software and hardware support, and tables that show the fixed defects and known issues in this release.



HPCA version 7.90 includes only the Core and Satellite installation model and does not include the Classic configuration. Moving from the Classic to the Core and Satellite model can be a very complex task. HP strongly recommends that customers employ the HP Professional Services organization to assist with this migration. HPCA version 7.80 includes both the Classic and the Core and Satellite models. Customers wishing to continue with their Classic model are encouraged to upgrade to version 7.80.

# Contents

- HP Client Automation Enterprise ..... 1**
  - Release Notes .....1
- In This Version.....4**
- Documentation Updates.....5**
  - HPCA Documentation Note .....5
- Documentation Errata .....6**
- Software and Hardware Requirements .....7**
  - Supported Platforms.....7
  - Hardware Support .....7
  - Database Servers .....7
    - Oracle Requirements .....7
    - MS SQL Server Requirements .....8
  - Backward Compatibility .....8
    - End of Life .....8
- Installation Notes .....9**
- Migration Notes.....9**
  - Component-Specific Migration Notes.....9
- New Features and Enhancements ..... 10**
  - Core and Satellite Servers .....10
  - Application Manager and Self-Service Manager Agent .....10
  - Configuration Server .....11
  - Out of Band Management .....11
  - OS Management.....11
  - Patch Management .....11
  - Usage Management .....12

Fixed Defects .....	13
Known Issues .....	22
Support .....	40
Legal Notices .....	41

---

## In This Version

Many new features and enhancements have been introduced in this release. See the section, [New Features and Enhancements](#) on page 10 for details.

For additional information about the features now included with Core servers, refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide*.

Depending on your active license, different features will be available in the Core and Satellite Consoles. Refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide* for more information.

Please note the following:

- Software and hardware requirements have changed for many products. See [Software and Hardware Requirements](#) on page 7 for details of current support.
- The HPCA Portal user interface functionality has been replaced by the HPCA Console. However, the underlying Portal service continues to play an important role in managing the device and group repositories, as well as providing the job-engine support for certain classes of jobs such as HPCA agent deployment.
- The MySQL database instance that is embedded in the HPCA Core is an operational database that holds information about jobs and user role assignments. The availability of this database is not critical to the functioning of HPCA. It is, however, required to support GUI access to the Console and job information. This database is not intended to have any user- or engineer-accessible elements, nor does it provide any extensibility. It is intentionally a locked down, fixed-purpose, embedded database. To this end, it is configured to be accessible only via a special service account, to processes that are local to the HPCA Core—direct network access is not possible.
- The Business Service Automation (BSA) Essentials Network (Live Network) is the online portal that provides access to the BSA Essentials Security and Compliance subscription services, tools and capabilities to enhance collaboration for the BSA community, and value-added content for BSA products. For Client Automation, this includes application management profiles, settings profiles, migration best practices, and various tools and utilities. To register for an account go to <http://www.hp.com/go/bsaenetwork>, click **Help and Support** and then click **Need an account?**
- Security and Compliance Manager is a product introduced in 7.50. It includes Vulnerability Management, Security Tools Management, and Compliance Management. See your HP Sales representative for more information, or visit <http://www.hp.com/go/bsaenetwork> and click **Subscription Services**.

---

# Documentation Updates

The first page of this document contains the following identifying information:

- Version number, which indicates the software version.
- Publish date, which changes each time this document is updated.

Always check the HP Software Product Manuals web site to verify that you are using the most recent version of this release note and check for updated product manuals and help files. This web site requires that you have an HP Passport ID and password. If you do not have one, you may register for one at:

**<http://h20229.www2.hp.com/passport-registration.html>**

Or click the **New users - please register** link on the HP Passport login page.

Once you have your HP Passport ID and password, go to:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

- 1 In the Product list, scroll to and click the product name, e.g., Client Automation.
- 2 In the Product version list, scroll to click the version number.
- 3 In the Operating System list, scroll to click the operating system.
- 4 In the Optional: Enter keyword(s) or phrases box, you may enter a search term, but this is not required.
- 5 Select a search option: Natural language, All words, Any words, or Exact match/Error message.
- 6 Select a sort option: by Relevance, Date, or Title.
- 7 A list of documents meeting the search criteria you entered is returned.
- 8 You can then filter the documents by language. Click the down arrow next to **Show Manuals for: English**. Select another language from the drop-down list.
- 9 To view the document in PDF format, click the PDF file name for that document.

**NOTE:** To view files in PDF format (\*.pdf), the Adobe® Acrobat® Reader must be installed on your system. To download Adobe Acrobat Reader, go to: **<http://www.adobe.com>**.

## HPCA Documentation Note



Take care when copying and pasting text-based examples of code from a manual, because these examples often contain hidden text-formatting characters. These hidden characters will be copied and pasted with the lines of code, and they can affect the execution of the command that is being run and produce unexpected results.

---

## Documentation Errata

The following statement appears in the “Preparing and Capturing OS Images” chapter in both the *HPCA OS Manager System Administrator Guide* and the *HPCA Core and Satellite Enterprise Edition User Guide*:

- ▶ If you are using an existing OS WIM image (this includes the OS .WIM files on the Microsoft Windows OS installation media) or have created an OS WIM image using the Microsoft Windows Automated Installation Kit (AIK), you do not need to prepare or capture the image, and you can skip to the next chapter.

This statement requires clarification. If you intend to deploy the OS image using Windows Setup, this statement is correct. If you intend to deploy the OS image using ImageX, however, you must capture it by using HPCA OS Image Capture tool provided on the ImageCapture media.

Refer to “Preparing and Capturing Desktop OS Images” in either guide for more information.

---

# Software and Hardware Requirements

Only those operating systems explicitly listed in the HPCA Support Matrix are supported within a specific product release. Any operating system released after the original shipping date for HP software release is not supported, unless otherwise noted. Customers must upgrade HP software in order to receive support for new operating systems.

HP Software will support new releases of operating system service packs, however, only new versions of HP software will be fully tested against the most recent service packs. As a result, HP reserves the right to require customers to upgrade their HP software in order to resolve compatibility issues identified between an older release of HP software and a specific operating system service pack.

In addition, HP Software support for operating systems no longer supported by the original operating system vendors (custom support agreements notwithstanding) will terminate at the same time as the vendor's support for that operating system.

HP announces product version obsolescence on a regular basis. The information about currently announced obsolescence programs can be obtained from HP support.

## Supported Platforms

For a list of supported hardware platforms, operating systems, and databases, see the HPCA Support Matrix available at the following URL: [http://h20230.www2.hp.com/sc/support\\_matrices.jsp](http://h20230.www2.hp.com/sc/support_matrices.jsp).

## Hardware Support

For hardware support information refer to the HPCA Support Matrix referenced in the [Supported Platforms](#) section of this document.

## Database Servers

For database servers that are supported by HPCA products, refer to the HPCA Support Matrix referenced in the [Supported Platforms](#) section of this document. Refer to the product documentation for limitations and additional information.

## Oracle Requirements

### Required Oracle User Roles

- CONNECT
- RESOURCE

### Required Oracle User System Privileges

- CREATE ANY VIEW
- SELECT ANY TABLE
- UNLIMITED TABLESPACE
- UPDATE ANY TABLE

## MS SQL Server Requirements

- MS SQL Server must be configured to use static ports. For information on how to use static ports, refer to your SQL Server documentation.

## Backward Compatibility

### End of Life

Version 4.2, 4.2i and 5.0 are entering an end-of-life (EOL) program. Details of the EOL will be available on the HP Software support portal at <http://support.openview.hp.com/prod-sppt-lifecycle/index.jsp>. We recommend that customers upgrade to version 7.90 (or 7.5x for version 4.2i customers).

For information about the backward compatibility of some components of the HPCA 7.90 release with previously released versions of the product, refer to the HPCA Support Matrix referenced in the [Supported Platforms](#) section of this document.



---

## Installation Notes

You can find installation instructions for each product in its respective getting started or installation and configuration guide. These guides, in Adobe Acrobat (.pdf) format, are on the product DVD in the \Documentation directory. You can also find these guides on the HP Software Product Manuals web site. See [Documentation Updates](#) on page 5 for the URL and instructions on how to find them.

For Core and Satellite Server installations, refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide*.

---

## Migration Notes

Review the following information about migrating to the current version of HPCA.

If your current **HPCA Enterprise** version is 7.20, 7.50, or 7.80, migrate to version 7.90 of the Core and Satellite servers.

Refer to the *HP Client Automation Enterprise Migration Guide*. Previous versions of HPCA Enterprise must be migrated to version 7.20 before they can be migrated to version 7.90 Core and Satellite.

### Component-Specific Migration Notes


- **Batch Publisher:** The 7.90 installation program will upgrade all software with the exception of the configuration files. This will allow customers to retain the previous customized publishing configurations to use with the updated software and runtime interpreter. For installation instructions, refer to the *HP Client Automation Enterprise Batch Publisher Installation and Configuration Guide*.
- **Configuration Server:** If customers have customized their RADISH Rexx script by replacing it with the RADISHSS Rexx script, they may use the out-of-the-box solution with 7.90 to do the single service optimization. Use the default RADISH script supplied in the 7.90 installation and configure the domains to be optimized as described in the *Policy Server User Guide*.

---

# New Features and Enhancements

The following sections describe the new features and enhancements that have been introduced in the 7.90 release of HPCA Enterprise edition.

## Core and Satellite Servers

- Smart Card authentication is now available for increased security. It is a form of strong security authentication for single sign-on within large companies and organizations. Smart cards can be used for identification, authentication, and data storage. Enterprise editions of Client Automation support two-way authentication using this method of authentication.
- A new extensible framework is now available, which allows you to create, modify, and deploy settings profiles for various software products. A settings profile consists of customized configuration settings for devices, which include settings related to applications, operating systems, and hardware. New settings profile support for select software is now available through HP Live Network. Reporting on the settings deployed across your environment is also available as indicated in the additional items listed below.
- HP Live Network is a subscription service that enables you to obtain the most current content for HPCA. The type of content available from HP Live Network varies depending on your HPCA license. Settings profile templates and report packs can now be updated from the HP Live Network site.
- Several new reports are available including those for settings profiles and HP Live Network acquisition details. The latter provides unified reporting for HP Live Network acquisitions.
- The new library options areas for Software, Patch, and OS Management on the Operations tab allow customers to conveniently and easily import and export services from QA to production machines, from QA to QA machines, and from Core Server to Core Server as needed. It also allows the administrator to change certain values which are stored in the CSDB through the console rather than opening the System Explorer utility.
- A new software service is pre-installed for collecting HP Power Assistant (HPPA) reporting data; its service ID is `HPPA_REPORTING`. If you want to utilize the PA reports, this service needs to be regularly deployed on a weekly basis. To deploy this service, create a DTM, timer, or recurring notify job to regularly deploy it.  
 Use HPPA version 1.1.1.5 or later for the best user experience.
- Import, Export, and Delete functionality has been moved to the Operations tab for consistency and better usability.
- The `hpcabackup` and `hpcarestore` migration scripts now support migration of customer customizations to the CSDB class definitions and default values. Modifications made to a class definition (by editing a class in the CSDB Editor) or default values (by editing a class `_BASE_INSTANCE_` in the CSDB Editor) will be preserved during migration.

## Application Manager and Self-Service Manager Agent

- Agent LOCKDOWN facility has been incorporated into this release. The goal of the lockdown mode is to ensure the integrity, confidentiality, and availability of the content and methods that are stored and used by the agent to prevent non-privileged users from tampering with critical system-level content or breaching confidentiality by viewing content they should not have access to. Refer to the *Application Manager and Application Self-service Manager for Windows Installation and Configuration Guide* for details.

## Configuration Server

- Out of the box support for the radish single service policy resolution optimization is now available. While resolving the desired state of a single service instead of walking the tree of services, HPCA can be optimized to just resolve that service. (The customer will however lose some customization capability for those domains.) . The domains to be optimized can be added into the database as instances of the `POLICY.POLPRMS` class. Refer to the *Policy Server User Guide* for details.
- Out-of-the box support for a core-to-core data synchronization is now available without having to specifically change the configuration of the Distributed Configuration Server (DCS).
- A new `SETTINGS` Domain has been introduced into the CSDB to facilitate settings profile management.

## Out of Band Management

- You can now access the remote console of the vPro device in both text and graphical mode using Keyboard Video Mouse Redirection (KVM) technology.

## OS Management

- A new OS capture wizard has been created, which greatly simplifies the capture process for Windows desktop (Vista and later) and server (2008 and later) operating systems. It reduces the required input to one screen, and eliminates the need to pre-populate the image with the (`Sysprep`) files required to prepare the image. Once the image has been uploaded to the server, the publishing process now allows the administrator to select the proper `unattend` answer file for this particular image. A set of `unattend.xml` answer files are provided to cover all platforms and most deployment scenarios.
- The user dialogs and progress indicators shown during a WinPE-based deployment have been completely overhauled, resulting in an intuitive UI that informs the user of the imaging progress and clearly shows how the process ended with graphical green checkmarks or red Xs as required.
- Thin client deployment has been enhanced to preserve the existing hostname when the OS is being refreshed on a previously managed device.
- Imagex-based deployments now automatically extend the OS partition to recover any unused disk space. In addition, driver injection is now supported using Imagex.
- OS Manager requires certain Microsoft `WAIK` files to reside in its upload directory to support the capture and publishing processes. OS Manager now checks for these files during startup, and if needed, copies these files from the `WAIK` standard install directory automatically.

## Patch Management

- There is increased support for handling policies with regard to patch management in the Virtual Desktop Infrastructure (VDI) for VMware View and Citrix Xen systems.
- Patch Metadata Distribution Model is now the default for better performance. This is a lightweight model for acquiring and delivering patch updates to your Agent devices.
- The Enterprise HPCA Console now contains options for importing and exporting bulletins between test and production machines. This functionality extends its support to the Patch Metadata Distribution Model by exporting and importing binaries from the Patch Gateway server.
- The most recently published HP Live Network Patch Manager announcements are now available. This information is provided by an RSS feed from the HP Live Network subscription site.

- Patch Gateway is now available on the Satellite Server. On the Satellite Console, you can use the Patch Management link to configure Satellite servers to either retrieve the requested binaries from the Internet through the Patch Gateway or to forward the request to the configured upstream server.
- SuSE 10 SP3 is now supported.

## Usage Management

- The renaming of devices in your network is now handled in a way to improve device reporting.
- New Inventory Reports, Operational Reports, and Executive Summaries have been added under Usage Management Reports.
- New Materialized View scripts have been included to enhance reporting performance.
- Utility scripts have been included for ease of database maintenance.

# Fixed Defects

The following defects have been fixed in this release.

## Core and Satellite: **\*\*RESOLVED\*\*** sync jobs do not work with non-default satellite install location

PROBLEM:	Notify and DTM Satellite synchronization jobs do not work with Satellites that are installed into a non-default location.
CAUSE:	Satellite synchronization script does not work correctly when not installed into default location.
WORKAROUND:	Install Satellite into default location.

## Core and Satellite: **\*\*RESOLVED\*\*** CA agent is always installed in default location regardless of directory specified during Satellite install

PROBLEM:	Satellite install ignores the user-specified target directory when installing HPCA agent components.
CAUSE:	The HPCA agent is installed without specifying the desired location; therefore, the default destination is used.
WORKAROUND:	After installing the Satellite, go to Control Panel, uninstall the HPCA agent, and re-install it to your preferred location.

## Core and Satellite: **\*\*RESOLVED\*\*** The bottom part of the Historical Compliance Assessment pane might be truncated on some displays

PROBLEM:	In an environment where there are many SCAP Benchmarks, the legend lists all of the entries in a single column which cannot fit within the widgets drawing space (i.e., default setup where it is one of three widgets and is placed at the bottom of the dashboard). This results in the lower half of the widget being truncated from the view.
CAUSE:	In an environment where there are many SCAP Benchmarks, the legend lists all of the entries in a single column which cannot fit within the widgets drawing space i.e., default setup where it is one of three widgets and is placed at the bottom of the Compliance Executive dashboard.
WORKAROUND:	Maximize the pane so the entire contents are visible. You maximize the widget by clicking on the maximize icon in the upper right corner of the widget. You can also hide the legend by clicking on the legend icon in the toolbar at the bottom of the widget.

## Core and Satellite: **\*\*RESOLVED\*\*** Downloads from Satellite Data Cache is Slow

PROBLEM:	Download speed from satellites is slow when data is cached on satellite. Client will take longer to install services when installing from satellite.
CAUSE:	
WORKAROUND:	None. Contact HP for hotfix.

## Core and Satellite: **\*\*RESOLVED\*\*** Mac Agent install bits are not available in the Core and Satellite installation media

PROBLEM:	Mac Agent install bits are not available in the Core and Satellite installation media.
CAUSE:	The bits are not present in the media.
WORKAROUND:	If you want to manage Mac devices, install the Agent from the HPCA Classic installation media.

Core and Satellite: **\*\*RESOLVED\*\*** Satellite registration heartbeat should flip values to SSL when SSL is enabled on the satellite

PROBLEM:	Enabling satellite communication for SSL will not change the COP instances to use SSL, they will use the non-ssl communication. Agent communication to satellite will not use SSL.
WORKAROUND:	None, contact HP for hotfix.

Administrator/Admin Packager: **\*\*RESOLVED\*\*** Admin Tool Packager crashes on Chinese and Japanese language Windows Vista and Windows 2008 platforms

PROBLEM:	If the user inputs the I18N characters in the input fields of the Packager for Chinese or Japanese Windows Vista or 2008 operating systems, the Packager crashes.
CAUSE:	Due to issue with the third-party tool dependency.
WORKAROUND:	When using the Packager on Chinese and Japanese operating systems for Vista and 2008, use the English inputs for the user defined input fields.

Administrator/Admin Publisher: **\*\*RESOLVED\*\*** Publisher promotes HKCU keys

PROBLEM:	Publisher promotes HKCU keys with machine context.
CAUSE:	The Publisher publishes .reg files with machine context by default and allows for no override of the ZCONTEXT flag.
WORKAROUND:	Keys in the HKCU hive must be published in a separate .reg file from HKLM keys. They must also be in a separate package. After promoting the HKCU keys, use the CSDB Editor to change the ZCONTEXT flag on the resultant EDR file from 'M' to 'U'.

Administrator/Admin Publisher: **\*\*RESOLVED\*\*** Native Publisher is not working on Linux

PROBLEM:	Native Publisher is not working on Linux.
CAUSE:	Native Publisher is broken on the 7.8 version of the product.
WORKAROUND:	Use the Batch Publisher for publishing. However, advanced features of the Native Publisher are not available in the Batch Publisher.

Administrator/Admin Publisher: **\*\*RESOLVED\*\*** Permission denied error when launching the Publisher

PROBLEM:	When you try to start the Publisher when Agents and Admin tools co-exist on the same machine, you will get the "Permission denied" error.
CAUSE:	The nvdtk binary does not have execute permission by default.
WORKAROUND:	Add execute permission to the nvdtk binary and start Publisher.

Administrator/Admin Publisher: **\*\*RESOLVED\*\*** Admin and Agent Co-existence error when both are installed with default installation path on Mac x86

PROBLEM:	This error occurs only when (1) Agents and Admin co-exist on the same machine, and (2) the order of install is Admin first and Agents second. Only if installed in this sequence, you will get the Package Information screen with the error box "ZOSVALUE" when you try to login to the Publisher.
CAUSE	The default path for Admin installation is /opt/HP/CM/Agent, but when the Publisher is launched, it searches for a file in the install directory for the Agent, namely, applications/HP/CM/Agent and hence throws the error.
WORKAROUND:	When you want Agents and Admin to co-exist on the same machine, make sure to install the Agents first and the Admin next.

Administrator/Admin CSDB Editor: **\*\*RESOLVED\*\*** CSDB Editor Runtime Error 339

PROBLEM:	This error occurs when the CS Database Editor is launched by a restricted user.
CAUSE:	The CS Database Editor is launched by a restricted user.
WORKAROUND:	Launch the CSDB Editor with Administrator rights.

Administrator/Admin CSDB Editor: **\*\*RESOLVED\*\*** CSDB editor fails to promote an edited file using 'edit component' when some specific tools like write are used for editing

PROBLEM:	Promote of the edited file using Edit component option fails when you use a tool like write.exe, notepad++, etc.
CAUSE:	Only standard editing tools like Notepad and WordPad are supported for the above operations.
WORKAROUND:	Use the Notepad or WordPad for the purpose of editing files.

Application Manager Agent: **\*\*RESOLVED\*\*** 7.8 PRDMAINT instances have a connection to 7.5 hot-fix instances instead of 7.8 hot-fix instances

PROBLEM:	The 7.8 PRDMAINT instances have a connection to 7.5 hot-fix instances instead of 7.8 hot-fix instances. This results in the failure to deploy Agent hot-fixes for 7.8. However, Agent patch deployment is not affected by this issue.
CAUSE:	The connection to Agent hot-fixes for 7.8 is broken.
WORKAROUND:	<p>With the CSDB editor, you can manually edit the 'Requires' connections for the PRDMAINT 7.8 RAM, RIM, and RSM instances to point to the 7.8 maintenance packages instead of 7.5.</p> <p>For example for the RAM_WIN32_NT_7_8 PRDMAINT instance do the following:</p> <p>Change the 'REQUIRES' connection from PRDMAINT.PACKAGE.RAM_WIN32_NT_7_5_HOTFIX to PRDMAINT.PACKAGE.RAM_WIN32_NT_7_8_HOTFIX and change PRDMAINT.PACKAGE.RAM_WIN32_NT_7_5_CUSTOM to PRDMAINT.PACKAGE.RAM_WIN32_NT_7_8_CUSTOM</p> <p>Note: This needs to be done for all OS flavors to which fixes will be applied. If you do not want to manually edit all these instances (since there are quite a number of them), the alternative is to acquire the export decks from HP with the fixes that will correct this problem.</p>

Application Self-service Manager: **\*\*RESOLVED\*\*** Linux Agent upgrade from DVD ROM produces bad interpreter error

PROBLEM:	Linux Agent upgrade from the DVD ROM produces the "bash: ./upgrade: /bin/ksh: bad interpreter: No such file or directory " error.
CAUSE	The shell script for ./upgrade is in DOS format.
WORKAROUND:	Run dos2unix on the upgrade script before executing it.

Application Self-service Manager: **\*\*RESOLVED\*\*** Connect can be deferred forever for certain domains (AUDIT, PATCH, OS)

PROBLEM:	If the domain name is less than 8 characters in length, then the Connect deferral does not restrict the deferrals to the values specified in 'Maximum number of deferrals' in the PRIMARY.CLIENT.CDFCFG.<<DomainName>> attribute in CSDB. As a result, it allows the user to have an endless connect deferral.
CAUSE	CDFDEFER.EDM expects an attribute size of at least 8 bytes.
WORKAROUND:	Predefined domains such as SOFTWARE and PATCHMGR will work as expected. However, a predefined domain, such as OS domain, will have this issue. There is no workaround for existing domains whose name contains less than 8 characters such as OS, AUDIT and USAGE. To eliminate this problem for user defined domains, create domain names with at least 8 characters.

Application Self-service Manager: **RESOLVED\*\*** Installation Agent in text mode fails on Mac OS

PROBLEM:	Installation of Agents fails on Mac OS in the text mode.
CAUSE:	Not known.
WORKAROUND:	Use the setup script to install the Agent on Mac in text mode, or alternatively, use the graphical install mode to install the Agent.

Application Self-service Manager: **\*\*RESOLVED\*\*** Publisher Login fails when both Agent and admin tools are installed on the same machine/path in Mac OS

PROBLEM:	On Mac OS, when Agent is installed on the same machine as admin tools, the Publisher login fails.
CAUSE:	The execute permission is missing for NVDTK.
WORKAROUND:	Grant the execute permission to the NVDTK file located in install folder.

HPCA Console: **\*\*RESOLVED\*\*** Pressing enter in a wizard on Firefox prompts for cancel

PROBLEM:	While using Firefox and pressing enter in certain wizards, instead of 'Next' being pressed, it is pressing 'Cancel' and providing an 'Are you sure?' prompt.
CAUSE:	
WORKAROUND:	Click Next instead of pressing enter, or use internet explorer.



### HPCA Console: **\*\*RESOLVED\*\*** Console refresh doesn't work right for Jobs and Policy UI

PROBLEM:	Client Automation Enterprise Console Jobs interface may not retrieve all the current or past jobs successfully. In this case an error notification pop up may appear.
CAUSE:	Server side may not respond in a timely manner when retrieving the list of all the jobs.
WORKAROUND:	Simple workaround is to click on the refresh button in the Jobs data grid.

### HPCA Console: **\*\*RESOLVED\*\*** HPCA Operations dashboard Executive view may fail to display

PROBLEM:	The Operations widgets in the Executive view of the HPCA Operations dashboard may fail to display if you are running in a Simplified Chinese (SCH) locale.
CAUSE:	Localized characters are not being correctly interpreted for display.
WORKAROUND:	Use an English locale in the browser.

### Messaging Server: **\*\*RESOLVED\*\*** RMS Log shows error: Invalid command name "remove"

PROBLEM:	Normally there is a meta data (qf) file for each message data file (df) that a Messaging Server processes. When attempting to remove a qf file from the queue that does not have a corresponding df file, the error message: Invalid command name "remove" is written to the log file and the file is not removed.
CAUSE:	This can happen in unusual situations where the df file gets removed but the qf file remains around. Typically, the qf file is held open when the df file is being processed. The error received will not stop the queue from operating.
WORKAROUND:	Stop the Messaging Server and remove any active or qf files that do not have a corresponding df file in the queue. Then restart the service for the Messaging Server.

### OOBM on Core: **\*\*RESOLVED\*\*** Messages appear in mixed locales when Server and Client locales are different

PROBLEM:	OOBM messages appear in both locales when Server and Client locales are different; however, all features will work as expected.
CAUSE:	Since both locales are present in the configuration, some of the OOBM pages will display messages in both locales.
WORKAROUND:	Ensure that both Server and Client systems are configured to have the same locale.

### OS Management for Windows: Windows 7 **\*\*RESOLVED\*\*** Windows Setup Merge failed to WinXP/Vista with OS+Data partition

PROBLEM:	<p>Deployment of Windows 7 using the Windows Setup method and the DISKMAP.TYPE "Merge" is only supported when deploying to hard disks with no partitions other than an OS Partition or a System partition and an OS partition. It is not supported for hard disks that contain additional data partitions. In these cases, the ImageX deployment method must be used, or the described workaround must be applied.</p> <p>The only exception to this rule is when the original OS was deployed using HPCA OS Manager, and the bare metal partitioning was done using DISKMAP.TYPE "Add."</p>
WORKAROUND:	<p>Disable the creation of the System partition – install Windows 7 into a single partition. Set the SYSPSPACE attribute in the OS.DISKMAP class to 0. For further information please refer to "Allocating Disk Space for Partitions" in the <i>HPCA OS Manager System Administrator User Guide</i>.</p> <p>For customers relying on Windows Setup deployment, HPCA will provide a hot fix promptly after the product release.</p>

OS Management for Windows: **\*\*RESOLVED\*\*** ImageX capture failed on Win2K3-64bit

PROBLEM:	The OSM Image Preparation Wizard fails while executing on Windows 2003 64-bit and Windows XP 64-bit.
CAUSE:	An OSM Image Preparation Wizard module named <code>tcclfsredirect.dll</code> fails to load because of missing Microsoft Visual C++ 2005 runtime redistributable files.
WORKAROUND:	<p>Download this package from Microsoft at the following URL:</p> <p><a href="http://www.microsoft.com/downloads/details.aspx?familyid=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&amp;displaylang=en</a></p> <p>NOTE: Although the OS are capturing is 64-bit, you must download and install the x86 32-bit version of these modules, because the HPCA modules are 32-bit executables.</p>

OS Management for Windows: **\*\*RESOLVED\*\*** Windows 2003 R2 SP2 target devices cannot go to desired state after Windows Setup deployment

PROBLEM:	<p>The HPCA Agent is not installed at the end of the OS installation.</p> <p>NOTE: This was observed on Windows 2003 R2 SP2 target devices but may also occur with other pre-Vista versions of Windows.</p>
CAUSE:	The GuiRunOnce command injection that starts the HPCA Agent installation uses an incorrect format.
WORKAROUND:	<p>Option 1: Use the ImageX deployment type through the Image Preparation Wizard. Do not use the Windows Native Install Packager.</p> <p>Option 2: If you want to use native installation as the deployment method, then you must edit the unattended installation file (then called WINNT.SIF) after you run the Windows Native Publisher but before you reboot to upload the image.</p> <p>Follow these steps:</p> <ol style="list-style-type: none"> <li>Navigate to the drive that you selected during the WNI Publisher.</li> <li>Edit <code>&lt;drive&gt;:\\$WIN_NT\$.~BT\WINNT.SIF</code></li> <li>Search for <code>radsetup</code></li> <li>On the line containing <code>radsetup</code>, replace the first double quote (") with the string <code>command0="C:</code></li> </ol> <p>For example, change:</p> <pre>"\Program Files\Hewlett-Packard\HPCA\Agent\RADsetup\RAMINSTALL.CMD"</pre> <p>To:</p> <pre>command0="C:\Program Files\Hewlett-Packard\HPCA\Agent\RADsetup\RAMINSTALL.CMD"</pre>

OS Management for Windows: **\*\*RESOLVED\*\*** Cannot use WinPE as the default SOS when OS Deployment Wizard is used

PROBLEM:	Even when the default SOS was changed to WinPE SOS for PXE and/or LSB deployment method, the machine boots to Linux SOS when OS Deployment Wizard is used to initiate OS deployment.
CAUSE:	ROM object created by OS Deployment Wizard overwrites the PXE/LSB settings with the default value, which is Linux SOS.
WORKAROUND:	There is no workaround for the issue. The machines will always boot to Linux SOS first, then re-boot to WinPE SOS if needed.

OS Management for Windows: **\*\*RESOLVED\*\*** OS Capture fails to override existing ImageX or WinSetup image

PROBLEM:	Operating system capture does not overwrite the existing ImageX or WinSetup image stored in upload folder.
CAUSE	Not known
WORKAROUND:	Manually delete or rename the existing OS image file in the upload folder.

OS Management for Windows: **\*\*RESOLVED\*\*** ImageX/Windows Setup Agent injection will fail if media\client\win32 directory contains rogue MSI files

PROBLEM:	Agent injection fails when trying to find the agent installation path.
CAUSE:	Unnecessary files exist in the media\client\win32 directory
WORKAROUND:	<ol style="list-style-type: none"><li>1. Provide the *clean* agent media to publish when you publish an OS.</li><li>2. Do not change the file name of the MSI file that contains the HPCA agent</li><li>3. Do not provide multiple versions of the HPCA agent MSI file in the same media directory.</li></ol>

OS Management for Windows: **\*\*RESOLVED\*\*** Multiple console windows pop up when running SOS WinPE

PROBLEM:	When using SOS WinPE to deploy an operating system, the user will see multiple console windows popping up and partially disappearing again. They do partially cover the HPCA SOS WinPE splash screen.
CAUSE:	This is a known issue with the Windows 7 kernel. Because Windows PE 3.0 (contained in the Windows Automated Installation Kit (AIK) 2.0, which was released for Windows 7) runs the same kernel, it is also affected. We can do nothing about this behavior.
WORKAROUND:	None

OS Management for Windows: **\*\*RESOLVED\*\*** "conhost.exe - Application Error" messages box can pop up when running SOS WinPE

PROBLEM:	<p>When using SOS WinPE to deploy an operating system, if the user hits ALT+TAB to see the console window hidden by the HPCA SOS Windows splash screen, a message box indicating an application error within <code>conhost.exe</code> can pop up.</p> <p>This is most likely to happen if ALT+TAB is hit early in the initialization phase of SOS WinPE.</p> <p>Pressing "OK" on the message window allows the process to continue. The deployment process is not affected.</p>
CAUSE:	This is a known issue with the new Windows 7 system service <code>conhost</code> that gets started to handle console window output.
WORKAROUND:	Do not press ALT+TAB during the deployment.

OS Management for Windows: **\*\*RESOLVED\*\*** ProductKey field error in unattend.xml samples for Windows7/Windows2008R2

PROBLEM:	The unattended Windows 7 or Windows 2008 R2 setup may stop with the following message: "The unattended answer file contains an invalid product key."
CAUSE:	Sample files contain an invalid product key.
WORKAROUND:	<p>Remove the Product Key from this section of unattend.xml:</p> <pre>&lt;settings pass="windowsPE"&gt; &lt;component name="Microsoft-Windows-Setup"&gt; &lt;UserData&gt; &lt;ProductKey&gt; &lt;Key&gt;</pre> <p>Example:</p> <pre>&lt;UserData&gt;   &lt;AcceptEula&gt;true&lt;/AcceptEula&gt;   &lt;ProductKey&gt;     &lt;Key&gt;&lt;/Key&gt;   &lt;WillShowUI&gt;OnError&lt;/WillShowUI&gt; &lt;/ProductKey&gt; &lt;/UserData&gt;</pre> <p>Add the Product Key to the following section:</p> <pre>&lt;settings pass="specialize"&gt; &lt;component name="Microsoft-Windows-Shell-Setup"&gt;</pre> <p>Example:</p> <pre>&lt;ProductKey&gt;AAAAA-BBBBBB-CCCCC-DDDDD-EEEE&lt;/ProductKey&gt;</pre> <p>(replace AAAAA-BBBBBB-CCCCC-DDDDD-EEEE with your Product Key)</p> <p>Full details on placing Product Keys in unattended answer files can be found in the Windows Automated Installation Kit documentation on unattended Windows installations.</p>

OS Management for Windows: **\*\*RESOLVED\*\*** Only "Desktop" mode is supported for T5745 Climbers Linux

PROBLEM:	Although there are 3 Visual Experience modes available for the Climbers eLinux image (Desktop, Kiosk, and No UI), HPCA only supports image capture when the unit is operating in Desktop mode.
CAUSE:	Kiosk and No UI modes do not allow access to the task bar.
WORKAROUND:	Log in as Administrator. When prompted for the Visual Experience mode, choose Desktop.

Patch Management Device Compliance Report: **\*\*RESOLVED\*\*** When -mib none option is used then the Applicable Products in the report show up zero.

PROBLEM:	When the -mib option is set to NONE, after the second patch connect, the Applicable Products in the "Device Status" reports show up as zero.
CAUSE:	The issue is with the Patch Agent. The patches folder in the NVDLIB gets deleted when -mib none is set. As a result, the product count is not calculated. So the DESTATUS sent object will have the product count of 0.
WORKAROUND:	<p>Set -mib option to "Yes".</p> <p>The fix for patchagt.tkd will be posted to the HP Patch Manager Update web site. Patch Agent Updates are obtained during an acquisition and the fix is automatically published and distributed.</p>

Patch Management: **\*\*RESOLVED\*\*** Bulletins pre-packaged with the media will not deploy any patches

PROBLEM:	Bulletins pre-packaged with the product will not deploy any patches.
CAUSE:	The bulletins pre-packaged on the media do not contain any patch binaries. Hence, they cannot be used to install the patch. This is intended so they can be used for Patch Discovery.
WORKAROUND:	To obtain and deploy the patches for the pre-packed bulletins, run an acquisition with the FORCE and REPLACE options turned to YES. Acquiring them without FORCE and REPLACE turned to YES does not work.

Patch Management: **\*\*RESOLVED\*\*** HPCA Patch Manager Service on the Core Server fails to start under certain conditions

PROBLEM:	<p>The HPCA Patch Manager Server Service fails to start when the following operations occur simultaneously:</p> <ol style="list-style-type: none"><li>1. The Patch Gateway (with INTERNET set to Y) receives an agent request for a Patch binary download but is unable to connect to the internet due to one of the following reasons:<ol style="list-style-type: none"><li>1.1 Network issue</li><li>1.2 Web Proxy issue</li><li>1.3 Vendor site maintenance</li></ol></li><li>2. During the above situation, the service for the HPCA Patch Manager Server is restarted due to one of the following reasons:<ol style="list-style-type: none"><li>2.1 A user updates any of the Configuration settings for Patch Management from the Core Console.</li><li>2.2 A user manually restarts the service from the Windows Service Management Console.</li></ol></li></ol>
CAUSE:	The Patch gateway is actually a component of the HPCA Patch Manager Server. Whenever the Patch Manager Service is restarted, the Patch Gateway is initialized. During Patch Gateway initialization, it cleans up all the unsatisfied requests from the <code>patchgw.mk</code> , which is the Patch Gateway Database. The code that handles the clean-up triggers an error when there are multiple failed requests.
WORKAROUND:	Delete the <code>patchgw.mk</code> file under <code>[HPCA CORE Install Directory]\Patch Manager\etc\patch</code> and restart the HPCA Patch Manager Server Service.

Patch Management: **\*\*RESOLVED\*\*** I/O Error during Patch Manager Gateway cache contents export

PROBLEM:	An I/O error can occur during the Patch Manager Gateway cache contents export into the compressed file.
CAUSE:	There is a size limitation of 2GB for the type of file compression that is performed; if the size of the compressed file created during the export exceeds this limit, it will cause the I/O error to occur.
WORKAROUND:	Make sure that the bulletins selected for export do not exceed the 2GB limit. In such cases where they do, perform multiple exports by selecting a subset of the bulletins at a time.

Patch Management: **\*\*RESOLVED\*\*** SuSE10 Patches with dependent package requirements are incorrectly reported as "Patch Installed".

PROBLEM:	On SuSE 10 systems, patches for some entitled bulletins will fail to install if dependent packages are missing from the system. The agent connect (radconnect) exits with error 709. However, in the HPCA Console Reporting tab the "Compliance by Patches" page still reports the status as "Patch Installed".
CAUSE:	The HPCA object containing the Patch Install Error status is not being updated when the patch installation fails on SuSE10 systems.
WORKAROUND:	Make sure all dependent packages required for the patch are already installed and present on the SuSE10 system before installing the patch from Patch Manager. If the required dependent packages are not present, install them before installing the patches for the entitled bulletins. The patch installation will be successful if all dependent packages are present.

Security and Vulnerability: **\*\*RESOLVED\*\*** Security Tools Management scanner fails to retrieve firewall rules with Chinese names

PROBLEM:	If firewall rule is modified to have a Chinese name, the Security Tools Management (STM) scanner does not retrieve the rule. No error messages are written to the <code>sectools-director.log</code> file.
CAUSE:	The STM scanner is not able to correctly write multi-byte character to the results file.
WORKAROUND:	Do not use Chinese characters when modifying a firewall rule name. This may be fixed in a future version of the STM scanner available through HP Live Network updates.

## Known Issues

The following are known issues in this release.

[Core: Quick Search does not apply filter when using Firefox](#)

PROBLEM:	When using the home page Quick Search feature on Firefox, the value you enter does not get applied properly making quick search unusable.
CAUSE:	Defect in code.
WORKAROUND:	Apply a filter manually using the navigation tree instead.

[Core and Satellite: Service list does not refresh automatically](#)

PROBLEM:	The service list on the left-hand side of the Management tab will not be refreshed after a Live Network acquisition. This can be a problem (at least initially) if the acquisition defined services are in a domain that previously had no services.
CAUSE:	A service domain is not displayed in the left navigation pane if there are no services defined in this domain. After the database priming or after the Live Network acquisition, the new services will be defined, but the domain list will not refresh automatically. The UI does not provide a way to request the refresh.
WORKAROUND:	Logout and login to the console.

### Core and Satellite: Virtual Management Reporting View is not localized

PROBLEM:	The Virtualization Management report view always appears in English regardless of locale.
CAUSE:	The localized message file is missing.
WORKAROUND:	None.

### Core and Satellite: Messages in vms-server.log displayed with incorrect characters in non-English locale

PROBLEM:	Messages in the vms-server.log file are displayed with an incorrect character set when non-English language browser settings are used. As a result, certain logged database values will be unreadable in non-English locales.
CAUSE:	Not known.
WORKAROUND:	There is no workaround for this problem.

### Core and Satellite: When exporting large services, the console may timeout during the operation

PROBLEM:	Exporting large resources from the database may cause the console to time out throwing an error message even though the export is successful.
CAUSE:	The time it takes to export large amounts of data may exceed the console time-out value.
WORKAROUND:	The export succeeds, but you may have to re-login to the console to complete the export.

### Core and Satellite: Live Network Connector has long changeable argument list

PROBLEM:	The Live Network Connector has a long list of options passed to it in order to drive the actual acquisition. The command is dynamically assembled based upon the settings selected in the HP Client Automation UI. When new content is released over live network, the settings passed to the Live Network Connector may even change. If you would like to execute the Live Network Connector manually, it is very important to use the most up to date command line options
CAUSE:	The options for Live Network Connector may change over time.
WORKAROUND:	<p>If you would like to execute the Live Network Connector manually, it is very important to use the most up to date command line options. In order to obtain the latest command line options used by HP Client Automation, you may do the following:</p> <ol style="list-style-type: none"><li>1) Go to the HPCA Live Network configuration and set the options up correctly as you would if you were to have HPCA executed the Live Network Connector.</li><li>2) Save the options.</li><li>3) Go to the HPCA Live Network Operations area and perform an update now choosing Live Network as the source. Verify any other settings that apply to your environment.</li><li>4) Open the log file at &lt;install-dir&gt;\VulnerabilityServer\logs\connector-exec-cmd.log</li><li>5) Copy the most recent command executed.</li><li>6) Take the command to the system where you want to execute the Live Network Connector</li><li>7) Modify the command to have the appropriate path, appropriate user name, appropriate password, and appropriate import directory. Note that passwords in the command will be displayed as asterisks **** and will not work if directly invoked.</li></ol> <p>It should be noted that if you execute this command using the same Live Network installation on the same system that HPCA is running on that you may cause HPCA and Live Network to become out of sync. If you do this, refer to the Live Network Connector user guides for clearing the Live Network Connector cache.</p>

### Core and Satellite: Migration script stops RCS service while VMS is using the RCS

PROBLEM:	After doing a migration, the vms-server.log file may have multiple error messages that look like "Failed to run Content Priming Management".
CAUSE:	The migration script stops the configuration server while the vulnerability server is attempting to publish the sample security services to the configuration server.
WORKAROUND:	At this time, there are not believed to be any persistent problems related to these errors, because the errors displayed are believed to be resolved automatically by the vulnerability server when it is restarted at the end of the migration script processing. However, any customer who has a Live Network subscription should perform a full update from Live Network after migration is completed.

### Core and Satellite: After migration, the HPCA Agent version column is blank

PROBLEM:	Following migration to 7.90 but prior to upgrading all deployed agents, an agent version may appear as blank in the Reporting tab. For example, the HPCA Agent Version column in the Managed Devices report may be empty for a particular device.
CAUSE:	Agents prior to 7.80 did not always properly report the agent version.
WORKAROUND:	Upgrade to the latest 7.90 agent.

### Core and Satellite: Manually removed satellite still shows as installed.

PROBLEM:	After manually removing a satellite server, it still appears as installed in the console interface.
CAUSE:	
WORKAROUND:	Delete the device in the UI to complete the manual removal of the satellite information and also cleanup any created SAP objects accordingly.

### Core and Satellite: sync Documentation error in Getting Started and Concept Guide

PROBLEM:	The Core and Satellite Getting Started and Concepts Guide incorrectly states that the HP ProtectTools management (TPM) service is available in HPCA Enterprise Edition. It is only available in HPCA Standard Edition.
CAUSE:	Documentation error.
WORKAROUND:	None.

### Core and Satellite: Documentation error in Enterprise User Guide

PROBLEM:	The Core and Satellite Enterprise Edition User Guide incorrectly indicates that you can create Dynamic Discover Groups in HPCA Enterprise Edition. This feature is only available in HPCA Standard Edition.
CAUSE:	Documentation error.
WORKAROUND:	None.



[Core and Satellite: Satellite sync area only syncs proxy cache and does not run a DCS.](#)

PROBLEM:	When using the SYNC options located in the satellite management portion of the UI, the SYNC only syncs the proxy cache and does not run a DCS sync for Configuration Data.
CAUSE:	DCS sync not run for Configuration Data.
WORKAROUND:	Use the satellite UI or a DTM JOB which will perform both syncs. Does not apply to CAS users.

[Core and Satellite: CSDB port upstream is non-configurable, DCS sync from satellite fails.](#)

PROBLEM:	When installing a satellite server, you cannot configure the upstream Configuration Server port. The product defaults to 3464, however if you need to use a different upstream port, you cannot edit that in the UI.
CAUSE:	
WORKAROUND:	You will need to edit HPCA/dcs/dmabatch.rc to manually change the port to match the upstream port.

[Core and Satellite: RMP/RMS: IP Address reported in RMP when VMware installed on client is incorrect.](#)

PROBLEM:	RMP/RMS: The IP Address reported in RMP when VMware is installed on a client is incorrect. When a Satellite server has multiple NICs on separate networks, the IP address picked is the first one reported. This IP will be reflected in the satellite management UI and may cause an issue using the Configuration and Operations tab within the satellite details window.
CAUSE:	The Messaging Server is not detecting the active IP address, just the first one it queries.
WORKAROUND:	Access the satellite UI directly.

[Core and Satellite: Filter function is not working for some columns in Job management](#)

PROBLEM:	The filtering functionality in the Jobs data grid might appear broken because the underlying data, rather than the UI representation, is used to filter the items in the data grid.
CAUSE:	The underlying data in the data grid might be slightly different than the UI representation in the renderer.
WORKAROUND:	Hover over the target item in the data grid and use the underlying data, as displayed in the Tooltip, for the filtering functionality.

[Core and Satellite: Patch bulletins acquired with 'Enable Download of Patch Meta-Data Only' set does not show applicable product info in reporting page](#)

PROBLEM:	If new products are added into the products.xml, and if acquisition is performed with 'Enable Download of Patch Meta-Data only' enabled, and if patches for those products are deployed, then in the 'Device Status' Report, the link to the applicable products will return no records.  This issue is not applicable to CAE Classic or CA Standard / Starter versions as this feature (download of patch metadata) is not available in those versions.
CAUSE:	When 'Enable Download of Patch Meta-Data only' is enabled under 'Distribution Settings', syncing of the products.xml file and the PRODUCTS class in the Configuration Server does not take place. It does not take place because the explicit product detection is not required in this method of patching. As a result, these new products are not available in the database and are not displayed in the link to applicable products.
WORKAROUND:	If new products are added in the products.xml file, and if at-least one bulletin is acquired with 'Enable Download of Patch Meta-Data only' enabled, the products.xml file will be synced with the PRODUCTS class and the reports will correctly display the list of applicable products.

### Core and Satellite: An LDAPS connection to Directory Service fails when just filename is put in "CA Certificates File"

PROBLEM:	The Portal fails to connect to a Directory Service when using LDAPS.
CAUSE:	The CA Certificates File field requires the fully qualified path to the CA Certificates file.
WORKAROUND:	When configuring an LDAPS connection for a Directory Service, specify the fully qualified path and filename in the "CA Certificates File" field on the Core Console's Configuration > Infrastructure Management > SSL page.

### Core: Backup of the Portal LDAP Directory is not supported on the Core server

PROBLEM:	When running the Portal as a Windows NT Service (e.g., from a Core server or CAS installation), the ENABLE_BACKUP configuration parameter for the Portal is set to 0 and must be kept at 0.
CAUSE:	We do not support the current CAE Portal backup and replication (secondary slapd and slurpd processes) in a Windows NT Service configuration.
WORKAROUND:	<p>There is no workaround for the current release. The ENABLE_BACKUP configuration parameter for the Portal must be kept at 0 (disabled).</p> <p>The current process-based slapd/slurpd mechanisms are being deprecated. These processes are being superseded with Windows NT Service management and will leverage Open LDAP's multi-master replication mechanism in upcoming releases.</p>

### Core and Satellite: Jobs for deploying services are not hibernating, ending with errors, for some reboot settings

PROBLEM:	Job does not hibernate when agent is not rebooted immediately. When deploying multiple applications with reboot settings set to "reboot after install, prompt user," if the agent is not rebooted within 4 minutes then the job ends with errors and subsequent notifies are not run.
CAUSE:	Not known
WORKAROUND:	Use "reboot after install, do not prompt user" as the reboot setting.

### Core and Satellite: Portal installed on Core: Does not install correctly into an I18N path when the locale is set to English

PROBLEM:	RMP: setup-slapd.tcl unable to run correctly when the locale is set to EN and the installation path is in Chinese.
CAUSE:	When installing the Core in an i18n path that is different from the local OS code page (i.e. OS is in EN and Path is Chinese), this is a valid setup but highly unlikely.
WORKAROUND:	Use an Installation path of same code page as the installed OS.

### Core and Satellite: Satellite Sync: Reporting table is not updated when a service is deleted and the sync is run

PROBLEM:	Satellite Sync: Reporting table is not updated when a service is deleted and the sync is run. Appevent report for satellite sync may not contain correct data as a service is unentitled from a satellite.
CAUSE:	Apache satellite doesn't contain all logic that agent contains to manage appevent lifecycle.
WORKAROUND:	Manually update appevent table to remove un-entitled services for given satellite.

### Core and Satellite: CLIENT.SAP and POLICY.USER instances are created in Core RCS 10 minutes later than the satellite is manually installed

PROBLEM:	CLIENT.SAP and POLICY.USER instances are created in Core RCS 10 minutes later than the satellite is manually installed IMPACT: Satellite UI may not function correctly for given server.
CAUSE:	Messaging Server timing issue on restart may cause heartbeat to not post in time after restart.
WORKAROUND:	Restart hpca-ms service on satellite and instances will be created.

### Administrator/Admin Publisher: Packages have connections to FILE and PATH instances that do not exist

PROBLEM:	Packages that were published with only registry keys (no files) may have connections to FILE and PATH instances that do not exist.
CAUSE:	The Publisher fills in connections to FILE and PATH by default even when there are no FILE or PATH instances to create.
WORKAROUND:	This is a cosmetic issue only and will not affect the deployment of the package.

### Administrator/Admin Publisher: Linux Deployment of an application fails on SUSE 11 when publishing an application

PROBLEM:	In the Publisher, when deploying a SUSE 11 application, if you select Novell as the OS in Package Information, the deployment of the application fails.
CAUSE	Selection of Novell as the OS does not map to SUSE 11.
WORKAROUND:	When publishing SUSE 11 applications, specify Linux as the OS for the application to deploy successfully.

### Administrator/Admin CSDB editor login fails when the HPCA Agent and the HPCA Administrator are installed on same machine and SSL is enabled for the HPCA Agent or the RCS

PROBLEM:	Unable to access the HPCA CSDB editor when HPCA Agent and HPCA Administrator (Admin Tools) are installed on the same machine and SSL is enabled for the HPCA Agent or the RCS.
CAUSE	The HPCA Administrator does not support SSL.
WORKAROUND:	Install the HPCA Administrator on a computer where SSL is not enabled for the HPCA Agent or the RCS.

### Administrator/Admin CSDB Editor: CSDB Editor displays an error when editing a registry instance

PROBLEM:	When trying to edit the registry instance in CSDB Editor for the first time after installation, an error is returned
CAUSE:	Not known.
WORKAROUND:	Log out of CSDB editor, login again, and try the same operation, it will succeed now.

### Administrator/Admin CSDB Editor: CSDB editor fails to save changes made to components associated with SYSPREP instances

PROBLEM:	Editing the component associated with the SYSPREP instances under the OS domain in the HPCA CSDB Editor fails with the following error: An error occurred attempting to copy <filename> during the edit process. This edit cannot be published. Save the Radxplore.log file from this session for diagnostics.
CAUSE:	The length of the SYSPREP instance name exceeds the maximum allowed characters.
WORKAROUND:	To successfully use the "edit component" and save the changes to a SYSPREP instance, make sure the length of the SYSPREP instance name is less than 12 characters.

### Application Manager Agent: Not all STARTUP ONCE timers get executed on system reboot

PROBLEM:	Not all of the startup timers that are configured to execute once when the system is rebooted are actually processed upon reboot.
CAUSE	This issue can occur when multiple startup timers are configured on an agent machine to execute once when the system is rebooted. However, timers that are not processed initially are eventually processed in subsequent reboots. This is not desirable. All startup timers that are configured to execute once should be processed upon reboot.
WORKAROUND:	None.

### Application Manager Agent: Trusted Platform Module (TPM) enablement service not supported on HPCA Enterprise

PROBLEM:	The Trusted Platform Module (TPM) enablement service is not supported on HPCA Enterprise.
CAUSE	The Trusted Platform Module (TPM) enablement service is restricted to HPCA Standard only. It requires configuration that is only available in this edition of the product. It is therefore not supported on HPCA Enterprise.
WORKAROUND:	Use scripts provided directly by the HP Personal Systems Group (PSG).

### Application Self-service Manager: Halt in upgrading agent from 5.11 to 7.5 on Win2008/Vista Chinese OS

PROBLEM:	Upgrading an agent from version 5.11 to 7.5 running on Windows 2008 in a Chinese OS pops a dialog box that states: "Listed below are busy files..." followed by the application that's using the file.
CAUSE:	The 5.11 agent uses a different language transform than the 7.5 agent resulting in this error.
WORKAROUND:	The workaround is to click the "Ignore" button or run a silent upgrade.

### Application Self-service Manager: Upgrade of Agent that includes Self-service Manager may detect temp file in use and require user interaction on Vista

PROBLEM:	Agent upgrade displays dialog indicating a .tmp file is in use. Problem only occurs if agent being upgraded includes the Self-service Manager and the upgrade is being performed on Vista. Dialog will appear even during a silent install.
CAUSE	Not known
WORKAROUND:	During the upgrade, dispose of the dialog (by clicking <b>Ignore</b> or <b>OK</b> , depending on the dialog) to continue with the agent install.

### Application Self-service Manager: CM\_Agent\_79\_UPGRADE\_MACX86 failed to upgrade to 7.90

PROBLEM:	When a user upgrades the HPCA agent from 7.50 to 7.90 on MAC OSX, the upgrade fails with the following error message: "/Applications/HP/CM/Agent/ClientUpgrade/upgrade[32]: ./Users/abc/.nvdr: cannot open [No such file or directory]".
CAUSE	The post install script of HPCA 7.50 install bits fails to create the ".nvdr" file in the user's home directory.
WORKAROUND:	Before you upgrade the HPCA agent from 7.50 to 7.90, apply the hotfix "MACX86A750102" to the agent computer by following the instructions given in the readme provided with the hotfix.  To obtain the hotfix, contact HP Software Support. You can go to the <a href="http://www.hp.com/go/hpssoftwaresupport">http://www.hp.com/go/hpssoftwaresupport</a> and submit a support case to obtain the hotfix.

### Application Self-service Manager: Migration: MACX86 RSM UI not upgraded to 7.90

PROBLEM:	For MAC OSX, the RSM fails to upgrade from previous versions of HPCA to HPCA 7.90.
CAUSE	The MAC OSX, upgrade deck contains the setup.cfg file. This file contains a flag set (1 or 0) for each agent component that needs to be upgraded. A sample setup.cfg contains the following:  SelectComponent Ram 1 SelectComponent Rsm 0  By default, the RSM flag is set to 0 in the setup.cfg file and therefore the RSM upgrade fails.
WORKAROUND:	Set the RSM flag to 1 in the setup.cfg file before performing the upgrade.

Application Self-service Manager: Verify and Repair operations in the Self-service Manager do not work correctly for the Publisher

PROBLEM:	A Verify or Repair operation in the Self-service Manager will not be able to detect and repair problems with an install of the HPCA Admin Tools.
CAUSE	Not known
WORKAROUND:	There is no workaround. Install and Remove operations work as expected with the HPCA Admin Tools. Verify and Repair operations work as expected with all software other than the HPCA Admin Tools.

Application Self-service Manager: MULTICAST not at an acceptable functional level on Agent

PROBLEM:	The MULTICAST feature does not work properly.
CAUSE	MULTICAST requires all the DATA SAPs to be disabled.
WORKAROUND:	None currently available.

Application Self-service Manager: CSDB Editor 'Notify subscribers' fails by saying 'No Users/Machines in the audience list'

PROBLEM:	CORE CSDB Editor 'Notify subscribers' fails by saying 'No Users/Machines in the audience list'.
CAUSE	Not known.
WORKAROUND:	Use Core Console for notification.

Application Self-service Manager: Reboot does not accept OK and agent is not rebooted after migration when the flag is set to AI=HA

PROBLEM:	Reboot does not accept OK and agent is not rebooted after migration when the flag is set to AI=HA.
CAUSE	Agent does not reboot after migration.
WORKAROUND:	Do not use the AI=HA flag setting in the Agent upgrade service. NOTE: The Agent migration works fine irrespective of what the AI flag is set to.

Application Self-service Manager: Missing connection in LOCATION class for new Connect Deferral Manager (CDF) configuration class CDFCFG

PROBLEM:	There is not a dedicated connection in the LOCATION class for the new CDFCFG class.
CAUSE:	By default, CDF is disabled. Therefore, there is no default connection provided in the LOCATION class for CDF.
WORKAROUND:	To enable CDF, the administrator must create an instance in the CDFCFG class and connect it to the LOCATION class by using one of the existing, unused _ALWAYS_ connections in the appropriate LOCATION instance.

### Application Self-service Manager: Agent maintenance fails to apply while running Application Self-service Manager on Vista

PROBLEM:	Agent maintenance fails to apply while running the Application Self-service Manager on Vista.
CAUSE:	This issue occurs when maintenance is launched in user mode on Vista.
WORKAROUND:	Maintenance for the agent can be applied using Application Manager via a notify, scheduled connect, or login script.

### Application Self-service Manager: The Schedule timed-event feature of Application Self-Service Manager does not support services with non-ASCII names

PROBLEM:	Schedule timed-event feature is not functional in the Application Self-Service Manager for non-ASCII named Services.
CAUSE:	The Schedule timed event feature of the Application Self-Service Manager does not support non-ASCII names. Schedules are not saved for these services.
WORKAROUND:	User should periodically perform a Refresh Catalog on the Application Self-Service Manager to determine if application updates are available for services with non-ASCII names, and then install the updates.

### Configuration Server: Configuration Server fails to respond to SSL TCPS requests on port 444

PROBLEM:	If the SSL Certificate Authority (CA) certificates being used with the Configuration Server have an expired certificate, the Configuration Server will not start up in SSL mode.
CAUSE:	The SSL CA certificates are not valid or expired.
WORKAROUND:	Use valid and non-expired certificates in the CA certificate bundle.

### HPCA Console: HP Live Network Announcements dashboard pane fails when HP Passport requires update

PROBLEM:	HP Passport credentials are not current for HP Live Network Announcements widget.
CAUSE:	Credentials for HP Passport require update.
WORKAROUND:	<ol style="list-style-type: none"><li>1. Visit HP BSA Essentials Network web site (<a href="https://www.www2.hp.com/">https://www.www2.hp.com/</a>) and complete the one time confirmation step before using the HP Live Network announcements widget.</li><li>2. If you continue to see a connection failure for the HP Live Network Announcements widget, visit the HP Live Network RSS Feed at: <a href="https://h20033.www2.hp.com/servlets/WebFeed?artifact=news&amp;version=rss_2.0&amp;cookieCheck=off">https://h20033.www2.hp.com/servlets/WebFeed?artifact=news&amp;version=rss_2.0&amp;cookieCheck=off</a>, Complete the one-time confirmation step if you are asked for it.</li></ol>

### HPCA Console: Cannot delete Completed Agent or OS Deployment jobs

PROBLEM:	After deleting the HPCA agent or OS deployment jobs using the Delete icon, the jobs remain listed in the UI.
CAUSE:	Manual deletion of these jobs is currently not supported.
WORKAROUND:	<p>HPCA agent and OS Deployment jobs can only be deleted via an aging mechanism.</p> <ol style="list-style-type: none"><li>1. Open <i>ManagementPortal_InstallDir/etc/rmp.cfg</i>.</li><li>2. Add or change the following parameter to indicate the job history in days to keep: <b>JOBHISTORYTTLDAYS 30</b></li><li>3. Save the file.</li><li>4. Restart HPCA Portal service.</li></ol> <p>The default location of the <i>rmp.cfg</i> file is:</p> <p>Core server: <i>c:\Program Files\Hewlett-Packard\HPCA\ManagementPortal\etc</i></p>

### HPCA Console: Error when viewing reports if the Oracle database user name begins with a number

PROBLEM:	When you attempt to view a report, Oracle "invalid table name" errors appear.
CAUSE:	The Oracle database user name for the Reporting database begins with a number. This can lead to unpredictable errors and failed reports.
WORKAROUND:	Use an Oracle database user name that does not start with a number (it can, however, contain a number after the first character).

### HPCA Console: The Directory Services restart is reported as successful when it is not successful

PROBLEM:	On the Directory Services configuration page, a Directory Services restart is reported as successful even when it is not successful.
CAUSE:	The appropriate status code is not being returned when a restart request fails.
WORKAROUND:	Check the refreshed status on the details page or the Directory Service list to see the actual status.

### HPCA Console: Initial display of an Active Directory object is limited to 1500 members

PROBLEM:	When browsing an Active Directory object that has more than 1500 members from the HPCA Console, only the first 1500 members are returned in the "member" attribute by the Directory.
CAUSE:	For scalability, the underlying Portal engine and Web Services that are used to communicate with Active Directory initially returns the first 1500 Active Directory members.
WORKAROUND:	Use the Console's Search Parameters to fine tune and narrow your search.



### HPCA Console: When an Agent or OS Deployment is scheduled to occur in the future, the target is displayed as 0 Target Devices

PROBLEM:	When an OS or agent deployment is scheduled to happen in the future, the target is incorrectly listed in the job list as 0 Target Devices.
CAUSE:	Unknown.
WORKAROUND:	None, This is a cosmetic issue, The job will run normally.

### OOBM on Core: DASH devices not showing as OOB devices in groups

PROBLEM:	DASH devices are not listed as OOBM devices in groups under Operations > Out of Band Management > Group Management even though the devices belong to the HPCA static groups. As a result, DASH devices can not be managed as Out Of Band devices through OOBM Group Management.
CAUSE:	Design restriction.
WORKAROUND:	None.

### OOBM on Core: OOB Group Management functionality not supported in non English locales

PROBLEM:	The HPCA Console does not support the OOB Group Management functionality in non English locales. Although you are able to see the listing of non English groups, no operations can be performed on these groups.
CAUSE:	Architectural limitation
WORKAROUND:	None.

### OOBM on Core: OOB detailed online help is not localized

PROBLEM:	OOBM detailed online help pages are not localized. Online help will be displayed in English even in non-English locales.
CAUSE:	OOBM online help is hardcoded to use English online help.
WORKAROUND:	The OOBM User Guide is localized. It contains all of the information available in the online help.

### OOBM on Core: OOB online help does not show correct help context

PROBLEM:	In some cases, OOBM detailed online help pages do not show the correct help context section.
CAUSE:	Some of the OOBM detailed online help pages are not linked correctly.
WORKAROUND:	All online help is available even though some pages are not indexed correctly. Search for the particular context in the online help to find the corresponding section.

### OOBM on Core: OOB Group Management functionality fails on large number of devices

PROBLEM:	OOB Group Management functionality fails when it operates in environments with large number of devices.
CAUSE:	Architectural limitation.
WORKAROUND:	None.

### OOBM on Core: OOB KVM session idle time-out is restricted to 4 minutes

PROBLEM:	OOB is not able to setup a KVM session if the idle time-out value is specified as more than 4 minutes.
CAUSE:	vPro devices do not allow an idle time of more than 4 minutes.
WORKAROUND:	Use a KVM session idle time-out value of 4 minutes or less.

### OOBM on Core: Automatic synchronization feature does not work

PROBLEM:	The automatic synchronization feature that is enabled by using a non-zero value for the "device_synchronization_timeperiod" parameter in the config.properties file does not work. This feature is meant to allow automatic reloading of the device list, synchronizing it with the SCS repository.
CAUSE:	Synchronization of the HPCA OOBM and SCS repositories during automatic synchronization does not work properly.
WORKAROUND:	Manually reload the device list to synchronize it with the SCS repository.

### OS Management for Windows: Thin Client devices require RALF and HPCA Agent

PROBLEM:	When preparing thin client devices for OS image capture, the Agent must be installed along with the HP Registration and Loading Facility (RALF)
CAUSE	N/A
WORKAROUND:	Refer to the Thin Client Agent installation instructions in the <i>Application and Application Self-service Manager Guide</i> .

### OS Management for Windows: Re-upload of ImageX/WinSetup image might fail after the first upload attempt failure

PROBLEM:	When creating an ImageX/WinSetup image and the first upload attempt fails, rebooting the machine might not start the upload process again.
CAUSE:	If uploading ImageX/WinSetup image fails, the SOS is no longer available to restart the upload process.
WORKAROUND:	None. If the second upload attempt doesn't boot to SOS, you must run Image Preparation Wizard again.

## OS Management for Windows: Capturing Images using FBWF

PROBLEM:	When working with FBWF (File Based Write Filter), there is no "Commit" state like its counterpart, EWF.
CAUSE:	<p>When working with FBWF (File Based Write Filter), there is no "Commit" state like its counterpart, EWF. There are two states with FBWF, "Enable" or "Disable."</p> <p>During image capture, when prepwiz.exe executes, a prepwiz.ini file is created to guide the capture operation. Under normal operation, the OS is in the "Enabled" state during image capture. This means that even though the prepwiz.ini file was written to the flash, it will not be kept when the unit reboots because of the "ENABLED" FBWF state. When the capture CD boots, it will look for the prepwiz.ini file, which at this point, is not found. When it cannot find the prepwiz.ini file, it will revert to running as a Service CD.</p>
WORKAROUND:	<p>Follow the steps below to successfully capture an image running FBWF.</p> <ol style="list-style-type: none"><li>1. Disable FBWF (Reboot). To disable FBWF, go to the DOS prompt from Windows and enter the following command: fbwfmgr /disable and reboot.</li><li>2. Manually install XPE agent.</li><li>3. Copy Etprep to \Windows and FBReaseal to \Windows\FBA directory.</li><li>4. Begin executing prepwiz.exe as normal.</li></ol> <p>When this captured image is used to deploy to other target units, the FBWF will be in its normal "ENABLED" state.</p>

## OS Management for Windows: Window requesting networking option to be used opens

PROBLEM:	When a target device boots into Vista following a deployment of the install.WIM file from the Vista media, a window appears requesting the networking option to be used.
CAUSE	Not known
WORKAROUND:	This is due to a known Microsoft bug and the user will have to make the appropriate selections based on the enterprise's environment.

## OS Management for Windows: No prompt info during image uploading, if OSM is down

PROBLEM:	If the OS Manager Service is not running at the time the image is being uploaded, the upload fails with the wrong error message.
CAUSE:	This error condition is not caught properly and the process continues which leads to a different error.
WORKAROUND:	Start the OS Manager Service and re-boot the machine to re-upload the image.

## OS Management for Windows: Image Preparation Wizard upload does not check/halt when Core server is out of disk space

PROBLEM:	The image upload process does not verify that enough free space exists on the Core server to successfully complete the upload. If not enough free space is available the upload will fail. In a core/satellite environment, the upload completes successfully but the Core server will fail to store the resulting image files. The partial files will be locked for a few minutes until they are automatically deleted. The upload fails and the Core server will fail to store the resulting image files. The partial files will stay locked until the Core server is restarted.
CAUSE	Out of disk space
WORKAROUND:	Make sure enough free disk space exists on the Core server so that the image upload may complete successfully.

### OS Management for Windows: LSB files installed on both the system reserved and local disk partitions

PROBLEM:	As part of the installation of the Local Service Boot, the service OS files will be installed on both the System Reserved and the OS partition.
CAUSE:	
WORKAROUND:	None. Do not delete these files from either the System Reserved or the OS partition.

### OS Management for Windows: OS deployment of Windows CE image 6.31 fails when using LSB

PROBLEM:	OS deployment of windows CE fails when using image 6.31
CAUSE:	This is due to insufficient allocated "Storage Memory." There is not enough space to install and extract the LSB service. The OS service detects the change in policy and causes the machine to reboot, but ROMBL fails to boot to Linux SOS because the LSB is not installed.
WORKAROUND:	Increase the allocated "Storage Memory" to at least 10MB. Steps to increase the allocated "Storage Memory" <ol style="list-style-type: none"><li>1 Click Start</li><li>2. Select Settings -&gt; Control Panel</li><li>3. Click the System Icon</li><li>4. Select the Memory tab.</li><li>5. Use the slider on the left to increase the "Storage memory"</li></ol>

### OS Management for Windows: Factory OS images should not be published for thin client devices

PROBLEM:	Factory OS images should not be published for thin client devices. All thin client images must be captured before they are deployed to target devices.
CAUSE:	During the OSM capture process additional information about the OS is retrieved and later used for image deployment. As a result, the administrator should not publish a factory image directly, as required information would be unavailable and the deployment would not succeed.
WORKAROUND:	All thin client images must be captured before they are deployed to target devices. For more information on capturing a thin client image, refer to the "Preparing and Capturing Thin Client OS Images" section in the "Preparing and Capturing OS Images" chapter in the <i>HPCA Core and Satellite Enterprise Edition User Guide</i> for more information.

### OS Management: SOS Linux cannot perform Image Capture for systems with RAID0 configured SATA boot devices

PROBLEM:	On systems which have their hard drive configured for RAID0 through SATA drive controller, an image capture process behaves as if attempting an image deployment.
CAUSE:	The SOS Linux processes do not correctly assemble the drives that comprise a RAID0 SATA device and thus cannot mount the file system for image capture.
WORKAROUND:	Use Windows ImageX image capture.

### OS Management for Windows: Cannot connect to desired Agent if it is installed under non-ASCII path

PROBLEM:	If the HPCA Agent is installed under a non-ASCII path in the legacy image, the first connect after OS deployment will fail.
CAUSE:	Linux SOS cannot resolve the non-ASCII path and fails to locate RUNONCE.CMD
WORKAROUND:	Do not install the HPCA Agent under a non ASCII path.

### OS Management: Deploying image to HP 4320t mobile thin client may cause first boot loop

PROBLEM:	Deploying an image to the HP 4320t mobile thin client may result in a first boot loop.
CAUSE:	This condition can be caused by a timing issue related to processing of the EWF filter.
WORKAROUND:	Perform a bare metal deployment.

### Patch Management: Patch binary download fails at patch gateway server at times when smaller files are requested for download

PROBLEM:	The patch binary download fails at the patch gateway server at times when smaller files are requested for download. As a result, the bulletin will not be patched during the patch connect.
CAUSE:	When very small binaries are requested a 'state not set' entry is seen in the log file, and an incorrect entry is recorded in the patchgw.mk file. This causes the agent to not deploy the particular bulletin.
WORKAROUND:	Stop the HPCA Patch Manager Server service. Delete the patchgw.mk file (under PatchManager/etc/patch). Restart the HPCA Patch Manager Server service. The patch connect on agent will be successful.

### Patch Management: Existing bulletins in the CSDB are deleted if they are re-acquired using Metadata

PROBLEM:	Microsoft bulletins previously published to the CSDB (not using Metadata) are deleted if they are re-acquired using Metadata.
CAUSE:	There is an issue in the MSFT Acquisition which is wiping out the published bulletins from the CSDB.
WORKAROUND:	None.

### Patch Management: Download Manager (RADSTGRQ): Network Utilization may not work as desired

PROBLEM:	The Patch Agent Download Manager options for 'Network Bandwidth' and 'Network Utilization in Screensaver mode' may not work as desired, and may negatively affect the Patch Manager Agent.
CAUSE:	These Download Manager options are not working as expected.
WORKAROUND:	No workaround. Do not use the options to control the network bandwidth to be used by the Download Manager. When configuring the Download Manager options on the Patch Agent Options page, do not enter anything in the 'Network Bandwidth' and 'Network Utilization' fields.

[Patch Management: Connect Deferral UI shows the service's reboot flag as blank for Patch](#)

PROBLEM:	Connection Deferral UI does not show the Reboot Required Option for Patch correctly.
CAUSE:	Reboot flag in service is blank or incorrectly represented.
WORKAROUND:	None at this time. Do not utilize the reboot required field as the basis for deciding to defer Patch Manager activities.

[Patch Management: Export URL Requests will not list the URLs which encountered an error during download](#)

PROBLEM:	For a Patch Gateway with Internet access, the Export URL Requests feature will not list the URL requests that encountered an error when downloading.
CAUSE:	The Export URL Request will only list the URL requests made when the INTERNET option is set to N in patch.cfg. Export URL Request is meant only for an environment where the Internet is not made available to the server hosting the primary Patch Gateway. The Export URL Request list (of unfulfilled URLs) that is created a Gateway without internet access can be downloaded after using Import URL Requests on another Gateway server that has Internet connectivity. Later the downloaded files can be copied back to the gateway folder on the primary Patch Gateway server.
WORKAROUND:	None.

[Patch Management: Criticality rating for MS09-044 bulletin is displaying as Important.](#)

PROBLEM:	The Severity Rating displayed in the Research by Bulletins and Acquisition By Bulletins Reports may not match with the Microsoft Security Bulletin Summary Page in the case where the bulletin contains patches not supported by WSUS and where their severity is higher than that of the other patches within the same bulletin.
CAUSE:	The Severity rating for the bulletin is determined by the severity of the patches that it contains. If the bulletin contains legacy patches which would not be supported by WSUS, those will be excluded when the severity rating is determined.
WORKAROUND:	None.

[Patch Management: Some applicable products for the bulletins are listed under the generic 'Microsoft Products' in the Patch manager Reports](#)

PROBLEM:	Some applicable products for the bulletins are listed under the generic 'Microsoft Products' in the Patch manager Reports.
CAUSE:	When the length of the 'Product String' for a bulletin is greater than 32 characters in length, the product is reported as 'Microsoft Products'.
WORKAROUND:	None

### Security and Compliance: Vulnerability Scanning does not produce results for 64 bit operating systems

PROBLEM:	Vulnerability Scanning does not produce results for 64 bit operating systems.
CAUSE:	Vulnerability Scanning is not supported for 64-bit operating systems from HPCA 7.80 at the time of release. The available vulnerability definitions from the National Vulnerability Database have not yet been updated to reflect the differences between 32-bit and 64-bit redirection on Microsoft operating systems.
WORKAROUND:	The Discover Vulnerability service will be updated via HP Live Network at a future point in time to support scanning 64-bit operating systems. This will be done when the content available from the National Vulnerability Database is appropriately updated to handle 64-bit paths. This will only be available to Security and Compliance subscribers. The Limited Edition service will not be updated.

### Usage Management: Application Usage Count is incremented by one whenever a collection notification is performed through the HPCA Console even though the launched application is not closed

PROBLEM:	Application Usage Count is incremented by one whenever a collection notification is performed through the HPCA Console even though the launched application is not closed.
CAUSE:	The AUM Service is restarted whenever a collection notification is performed through the HPCA Console.
WORKAROUND:	None. However, the scheduled usage collection does not have this issue.

### Usage Management: Error occurs when applying Optional Feature utility

PROBLEM:	While applying the Optional Feature utility, an error is encountered during Execution of "Step5_Define Filter Mat Tables and Indexes.sql" which can be found under HPCA\Media\Usage\Optional Features\SQL Server.
CAUSE:	The column name used in the script during creation of index IX_matWindowsComputers_4 does not have a space character in it.
WORKAROUND:	In the "Step5_Define Filter Mat Tables and Indexes.sql " under Optional Features\SQL Server\ in the Index IX_matWindowsComputers_4 Creation Command, change FirstCollection to [First Collection] and LastCollection to [Last Collection] and execute the script.

### Usage Management: Usage By Product reports show product name as [undefined] for non-English operating system

PROBLEM:	Usage By Product reports show the product name as not being defined [undefined] for non-English operating systems.
CAUSE:	The application product name string is not localized.
WORKAROUND:	None. However, you can see application usage details, if you drill down in the report.

---

# Support

You can visit the HP Software support web site at:

**[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

This Web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

To register for an HP Passport ID, go to:

**<http://h20229.www2.hp.com/passport-registration.html>**



---

## Legal Notices

For information about third-party license agreements, see the `License` directory on the product installation media.

©Copyright 2010 Hewlett-Packard Development Company, L.P.

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

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.

The information contained herein is subject to change without notice.

For information about third-party license agreements, see the `License` directory on the product installation media.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

The Apache Software License, Version 1.1

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)  
Copyright © 1999-2001 The Apache Software Foundation. All rights reserved.

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER

Copyright © 1996-1999 Intel Corporation.

TFTP SERVER

Copyright © 1983, 1993

The Regents of the University of California.

OpenLDAP

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.

Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License

Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar

Copyright Mihai Bazon, 2002, 2003

## Lab PullParser

Copyright © 2002 The Trustees of Indiana University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- 1) All redistributions of source code must retain the above copyright notice, the list of authors in the original source code, this list of conditions and the disclaimer listed in this license;
- 2) All redistributions in binary form must reproduce the above copyright notice, this list of conditions and the disclaimer listed in this license in the documentation and/or other materials provided with the distribution;
- 3) Any documentation included with all redistributions must include the following acknowledgement:  
"This product includes software developed by the Indiana University Extreme! Lab. For further information please visit <http://www.extreme.indiana.edu/>" Alternatively, this acknowledgment may appear in the software itself, and wherever such third-party acknowledgments normally appear.
- 4) The name "Indiana University" and "Indiana University Extreme! Lab" shall not be used to endorse or promote products derived from this software without prior written permission from Indiana University. For written permission, please contact <http://www.extreme.indiana.edu/>.
- 5) Products derived from this software may not use "Indiana University" name nor may "Indiana University" appear in their name, without prior written permission of the Indiana University. Indiana University provides no reassurances that the source code provided does not infringe the patent or any other intellectual property rights of any other entity. Indiana University disclaims any liability to any recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise.