

HP Client Automation Starter and Standard

New Features and Release Notes

Software version: 7.80 / November 2009



IMPORTANT NOTE:

With the introduction of Client Automation, version 7.20, HP has simplified and streamlined the installation, configuration, and use of our product by introducing two new server components: the [Core and the Satellite](#). These components provide an end-to-end experience that encompasses all of our product capabilities.

The **Core** and **Satellite** (see the *HPCA Core and Satellite Getting Started and Concepts Guide* in the `Documentation` directory of the HPCA media) are available to new Enterprise, Starter, and Standard license edition customers who use **Windows Servers** as their primary infrastructure platforms or existing customers who are migrating from an earlier version of Core and Satellite implementation.

Existing customers, and new customers who require **UNIX** infrastructure support, should consult the *HPCA Configuration Server, Portal, and Enterprise Manager Getting Started Guide* for information on alternative methods for installing, configuring, and using HP's **Client Automation** infrastructure.

This document provides an overview of the changes made to the HP Client Automation (HPCA) Starter and Standard components for the 7.80 release. It contains a bulleted list of new features and functionality for each component and tables that show current software and hardware support for each product.

Contents

- HP Client Automation Starter and Standard..... 1
 - New Features and Release Notes1
- In This Version..... 3
- Documentation Updates..... 4
 - HPCA Documentation Note4
- Software and Hardware Requirements 5
 - Supported Platforms.....5
 - Hardware Support5
 - Database Servers.....6
 - MS SQL Server Requirements6
- Installation Notes 7
- Migration Notes 7
- New Features and Enhancements 8
 - Core and Satellite Servers.....8
 - Out of Band Management8
 - OS Management.....8
 - Patch Management8
- Fixed Defects 9
- Known Issues 12
- Support 29
- Legal Notices 30

In This Version

Many new features and enhancements have been added to this release. Prominent among the new features introduced in 7.80 are the following:

- Full support for Windows 7
 - Complete management of Windows 7 end-point devices
 - OS migration from Windows 2000, Windows XP, and Windows Vista to Windows 7
 - Preservation of user data and settings during OS migration
- Critical enhancements to Patch Management
 - Identification and marking of superseded Microsoft patches
 - Identification of patches by severity rating: critical, important, moderate
 - Reporting on patch completion progress across all devices
 - Performance and usability improvements
- Remote management of Satellite Servers from the HPCA Console
 - Deployment of Satellite Servers
 - Management of subnets assigned to Satellite Servers
 - List of all installed Satellite Servers and their status
 - Location of installed agents
 - List of devices assigned to Satellite Servers
 - List of all services running on Satellites and log collection
- Availability of Microsoft's Remote Assistance for integrated remote control to connect to remote managed devices (in addition to VNC and RDP)
- New settings for the Migration Manager
 - Replacement of settings based on User State Migration Tool (USMT) 3 and USMT 4

See the section, [New Features and Enhancements](#) on page 8 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.

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), 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 can affect the execution of the command that is being run and produce unexpected results.

Software and Hardware Requirements

Only operating systems explicitly listed in the compatibility table 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

The following table contains the operating system requirements for this release.

Table 1 Platform Support

Vendor	OS Name	OS Version #	Server	Agent
Microsoft	Windows XP	Professional SP3	N	Y
Microsoft	Windows Vista	Business/Ent. SP2	N	Y
Microsoft	Windows 7	Business/Ent.	N	Y
Microsoft	Windows 2003	Server SP2	Y	Y
Microsoft	Windows 2003	Server R2 SP2	Y	Y
Microsoft	Windows 2008	Server SP2	Y	Y
Microsoft	Windows 2008	Server R2	Y	Y

Hardware Support

The following table lists hardware support information.

Table 2 Hardware Support

Model	Support Information
HP Managed Thin Clients	All models supported
Intel 32-bit (x86), 64-bit (x86-64)	Supported
AMD 64-bit (AMD64)	Supported
Itanium Processor	Agent support on Windows; No Server support; No Linux support

Model	Support Information
Sun UltraSPARC	UltraSPARC III, IV, V
VMware	Server/Agent support on ESX 3.x, 4.x; Server support on Server 2.0; Agent support on Workstation 6.5
Microsoft Virtual Server	Agent support on 2005R2

Database Servers

The following table lists the database servers that are supported for HPCA products. Refer to the product documentation for limitations and additional information.



For the supported databases for Intel SCS (required for OOBM functionality), refer to the *Intel AMT SCS Version 5.0 Installation Guide* located in the `Media\oobm\win32\AMT Config Server` directory on the HPCA Core media.

Table 2 Supported Database Servers

Database Server	Version
Microsoft SQL Server	2005
	2008
SQL Express	2005
	2008

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.

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 them on the HP Software Product Manuals web site. See [Documentation Updates](#) on page 4 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 migration notes for information about migrating to the current version of HPCA.

- If your current version is **HPCA Starter** or **Standard**, version 2.11, 7.20 or 7.50, migrate to version 7.80 of the Core and Satellite servers.

Refer to the *HPCA Starter and Standard Migration Guide*. Previous versions of HPCA Starter and Standard, and Client Configuration Manager must be migrated to version 2.11 before they can be migrated to version 7.80 Core and Satellite.

New Features and Enhancements

The following sections describe the new features and enhancements that have been introduced in the 7.80 release of HPCA Standard edition.

Core and Satellite Servers

- HPCA can now manage client devices running Windows 7 and Windows Server 2008 R2.
- Beginning in 7.50 and continuing in 7.8, the HPCA Console has completely replaced the HPCA Portal UI for all administrative tasks.
- Features such as deployment of satellite servers, device deletion, and modification of links, defaults, and overrides that were provided in the deprecated Portal User Interface are now all available in the HPCA Console.

Out of Band Management

- NT LAN Manager (NTLM) V2 authentication support has been added for communication between HPCA and SCS.
- GUI messages have been enhanced to provide better diagnostics for communication between HPCA and SCS.
- OOB discovery and refresh operations have been segregated. The time it takes to discover OOB devices has been greatly improved. You now have the option to incrementally discover just those devices that have been added and/or modified on your network.
- HPCA now allows only one refresh operation at a time thus preventing multiple refresh requests to overload the system. To avoid confusion, the user is notified if the system is already performing a refresh operation.
- Configurable parameters have been added that allow you to specify the IDE-R/SOL time-out sessions. This allows you to fine tune time-out values according to the traffic on your network allowing remote operations performed on vPro devices to succeed even on slower wireless connections.

OS Management

- Support for Windows 7 and Windows 2008 Server R2

Patch Management

- Superseded Microsoft patches are now identified and marked.
- Patches are now identified by severity rating, namely, critical, important, and moderate.
- Report on patch completion progress is now available across all devices.
- Many improvements have been made in performance and usability.

Fixed Defects

Core and Satellite: ****RESOLVED**** Children data grid is cleared when Group management wizard is cancelled out

PROBLEM:	If the Group Management wizard is launched and Cancel is clicked, without a group having been created, the children data grid might be cleared.
CAUSE:	The model that is used to hold the children of the currently visible directory object is cleared in the Group Management wizard.
WORKAROUND:	Click Refresh to refresh the Children data grid view.

Core and Satellite: ****RESOLVED**** Over-length input of data filter in reporting cause SQL error info in GUI

PROBLEM:	Specifying a numeric value that is too long will cause a SQL error.
CAUSE:	Maximum integer length has been reached or exceeded.
WORKAROUND:	Specify a shorter value; filters that are affected don't match the requirement to enter a long numeric value.

Core and Satellite: ****RESOLVED**** Apache Server fails to start after enabling SSL and the install path contains non-Western European characters

PROBLEM:	The Apache server fails to start after a Core or Satellite is enabled for SSL and the install path contains non-Western European characters.
CAUSE:	The version of Apache used by the Core and Satellite servers (Apache 2.2.11) contains a known I18N defect in the OpenSSL certificate code; if the Core or Satellite server is installed in a file system path that contains non-Western European characters (cp1251/iso8859-1) then attempts to enable SSL will fail and the Apache server will be unable to start.
WORKAROUND:	If SSL is required on non-Western European systems, install the Core or Satellite server into a file system path that contains only ASCII characters. If necessary, use Windows Add or Remove Programs to remove a previous Core or Satellite server installation.

Core and Satellite: ****RESOLVED**** Enable SSL- upload certificates crashes Core Apache Server

PROBLEM:	Uploading an incorrect SSL certificate prevents the Apache service from starting.
CAUSE:	The HPCA Console does not properly validate certificates prior to usage.
WORKAROUND:	<ol style="list-style-type: none">1. Open regedit.2. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HPCA-Apache.3. Open the ImagePath value for modification, and remove -D ssl from the end of the command line.4. Start HPCA-Apache Windows service.

Knowledge Base Server: ****RESOLVED**** [HPCA KB Server Administrator may save a Knowledge Base with an incorrect Password entry](#)

PROBLEM:	When using the HPCA KB Server Administrator to add or modify a Knowledge Base, the Knowledge Base can be stored with an invalid password.
CAUSE:	If you create a Knowledge Base name but enter the wrong password, an error window will be displayed with a "wrong credentials" message. If you click Cancel to exit the error message dialog and click Save configuration on the KB Server Administrator, your invalid password entry is stored in the registry for that Knowledge Base.
WORKAROUND:	If an incorrect password entry has been saved with the Knowledge Base, delete that Knowledge Base and create a new one with the correct password.

OOBM on Core: ****RESOLVED**** [Cannot use NTLM as authentication protocol between HPCA Console and the OOBM SCS Server](#)

PROBLEM:	At this time, you cannot use the NT LAN Manager (NTLM) v2 authentication protocol for the authentication mechanism between the OOB Management Console and the SCS Server.
CAUSE:	This is due to a limitation with the Apache HTTP client used by the HPCA Console.
WORKAROUND:	Until further notice, you must use another authentication mechanism to secure the communication between these components.

OOBM on Core: ****RESOLVED**** [Deployment of software list to OOB devices stops the tomcat server service](#)

PROBLEM:	Deployment of the software list stops the Tomcat Server service when OOBM is setup on Windows Server 2008 x64 AMD64T. As a result, the functionality related to Agent Presence is not available on Windows 2008 x64 systems.
CAUSE:	Issue is due to 3rd party dependencies of OOBM.
WORKAROUND:	None.

OOBM on Core: ****RESOLVED**** [Refresh All fails to update OOB DASH device information](#)

PROBLEM:	The Refresh All operation fails to update OOB DASH device information. This will cause a problem when the user is performing the refresh all operation when selecting Operations > Out Of Band Management > Device Management > Refresh All.
CAUSE:	This is a known issue.
WORKAROUND:	Select all of the DASH devices explicitly (DASH devices can be sorted based on device type) and perform the refresh operation.

OOBM on Core: ****RESOLVED**** [Can not manage OOB vPro device when Active Directory is installed on Windows Server 2008](#)

PROBLEM:	vPro devices cannot be managed Out of Band when Active Directory is installed on Windows Server 2008 and SCS is using the domain account. It causes the SCS login to fail. This will cause a problem when the user is trying to modify the SCS credentials by selecting Configuration > Out Of Band Management > Device Type Selection > Manage vPro Device.
CAUSE:	Third-party dependencies of OOBM.
WORKAROUND:	None.

OOBM on Core: ****RESOLVED**** SCS service fails to start on Windows Server 2008

PROBLEM:	On Windows Server 2008 (both 32 and 64 bit), the SCS service (named AMTConfig) fails to start if the user name is specified as <full_domain_name>\<username> . For example, if the domain name is oobm.hp.com and the username is administrator , then the SCS login username should not be given as oobm.hp.com\administrator .
CAUSE:	SCS service will not start and the vPro devices can not be managed.
WORKAROUND:	If the domain name is oobm.hp.com and the username is administrator , then specify the SCS login username as oobm\administrator or use the browse button of the SCS installation wizard to get the appropriate username.

OS Manager: **** RESOLVED **** Offline installation of a Windows Native Install image from CD or cache will fail.

PROBLEM:	Offline installation from CD or from cache of an OS image will not work with a Windows Native image.
CAUSE:	These images are created using the Windows Native Install Packager. A file required for the installation is temporarily converted to a file encoding that is incompatible with the Windows OS installation program. During offline OS installations from CD or from cache, the file format is not restored to its original encoding. This causes the installation to fail.
WORKAROUND:	None

OS Manager for Windows: ****RESOLVED**** Won't go to DESIRED for ImageX/WinSetup if booting to WinPE first w/ policy in RCS

PROBLEM:	The first connect after OS deployment might not work and some clean-up work might not be done for ImageX or WinSetup images when the target machine is new to the HPCA Infrastructure and using WinPE as the default SOS.
CAUSE:	OS Management Agent fails to use the setting specified in the BEHAVIOR instance under certain condition, and use the setting from _NULL_INSTANCE_ , which might lead to the target machines to connect to a wrong or non-existing Configuration Server for its first connect.
WORKAROUND:	Boot to Linux SOS first, which will automatically reboot to WinPE as a part of the process.

Known Issues

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: MP/RMS: IP Address reported in RMP when VMWARE installed on client is incorrect.

PROBLEM:	RMP/RMS:: IP Address reported in RMP when VMWARE installed on client is incorrect. When a satellite server has multiple nics on separate networks, 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:	RMS isn't detecting active IP address, just first one it queries..
WORKAROUND:	Access 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: 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:	There is no workaround for the current release. The ENABLE_BACKUP configuration parameter for the Portal must be kept at 0 (disabled). 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.

Core and Satellite: Date/Time format is not locale sensitive

PROBLEM:	Non-localized schedule-description text is displayed in the Schedule column of the Jobs data grid.
CAUSE:	The text description of the job schedule is stored in the database in the user's locale at creation time.
WORKAROUND:	Drill down to the specific job to see the more detailed job information, including the localized schedule description in the current locale.

Core and Satellite: rmp mc mistake visible when cancelling device discovery job or bad creds

PROBLEM:	Some messages aren't resolving but are, instead, showing the message catalog key in the job details interface.
CAUSE:	Message catalog entry not resolving.
WORKAROUND:	None

Core and Satellite: 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: Core Console access using external Directory Server Accounts may fail when the Directory Host is set to an IP address

PROBLEM:	After specifying the Directory Host as an IP address, the console authentication does not work with your Directory Service Accounts.
CAUSE:	Using an IP address to define the Directory Host has several related requirements; for example, the accounts must have DNS host access, a valid groupname, and in AD each account must have a user principal name.
WORKAROUND:	Specify the Directory Host for external Directory Server Accounts using a fully qualified hostname. Or Ensure all Directory Server Accounts have the userPrincipalName attribute set, a valid groupname, and DNS host access.

Core and Satellite: CA agent would be under "..\HPCA\Agent" when installing SAT in a specific

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: 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: Agent removal wizard job ends in error, if removing a manually installed agent

PROBLEM:	Using the agent removal wizard to remove a manually installed agent will cause the job to end in error.
CAUSE:	Not known
WORKAROUND:	Agent will remove (if installed though setup.standard.cmd), however job will end in error.

Core and Satellite: Duplicate devices are created when using domain discovery as well as manual device imports.

PROBLEM:	Manually importing a device can create a duplicate entry after domain discovery.
CAUSE:	This will always be a possible scenario. When devices are manually added without enough identifying unique attributes like MAC address, dnshostname, etc., when the device discovery is triggered, a new device may not match the manually added one, thus producing the duplicate entry.
WORKAROUND:	Trigger the domain discovery; do not manually add that discovered device.

Core and Satellite: Jobs for deploying and removing infrastructure services both display the same message

PROBLEM:	Both Infrastructure service deployment and infrastructure service removal job details display the same message "Installing and Configuring HPCA Management Agent"
CAUSE:	Both types of jobs attempt to push out the HPCA Management Agent out to the device before triggering the work, thus the common message is being shown.
WORKAROUND:	None.

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: Current Daylight Savings Time (DST) zone is not displayed correctly

PROBLEM:	The current Daylight Savings (DST) time zone is not always displayed correctly and may cause system time mismatches.
CAUSE:	Requires a Microsoft patch.
WORKAROUND:	If the time does not get displayed according to the current DST, check if the Microsoft patch "December 2008 cumulative time zone update for Microsoft Windows operations systems" has been applied. The problems you will see if this patch is not applied are that the time zone settings for your computer's system clock may be incorrect. This may cause system time mismatches in the working of the software.

Core and Satellite: Satellite Synch: Reporting table is not updated when a service is deleted and the synch is run

PROBLEM:	Satellite Synch: Reporting table is not updated when a service is deleted and the synch 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: Remote desktop access failed in IE6

PROBLEM:	<p>When trying to access a device through the Remote Desktop connection using Internet Explorer 6 (IE6), you might get an error:</p> <p>Connecting to:<device name> Unable to launch the Remote Desktop Web Connection ActiveX control (also known as Terminal Services Client Control). Possible causes: The current browser security settings do not allow the ActiveX control to be installed and/or run. The ActiveX control is installed but it has been disabled. The ActiveX control can only run in the 32-bit version of Internet Explorer.</p> <p>For more information, refer to the Troubleshooting section of the online help</p>
CAUSE:	Problems with the required ActiveX control on IE6..
WORKAROUND:	Upgrade to Internet Explorer 7 or use the remote desktop connection outside of the HP Client Automation, meaning directly in the operating system.

Core and Satellite: MP/RMS: IP Address reported in RMP when VMWARE installed on client is incorrect.

PROBLEM:	RMP/RMS:: IP Address reported in RMP when VMWARE installed on client is incorrect. When a satellite server has multiple nics on separate networks, 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:	RMS isn't detecting active IP address, just first one it queries..
WORKAROUND:	Access satellite UI directly

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

PROBLEM:	<p>CLIENT.SAP and POLICY.USER instances are created in Core RCS 10 minutes later than the satellite is manually installed</p> <p>IMPACT: Satellite UI may not function correctly for given server.</p>
CAUSE:	RMStiming 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.

Core and Satellite: 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.

Domain import fails from Win 2008 CAServer

PROBLEM:	Domain import fails to import devices when HPCA Server is installed on Windows 2008.
CAUSE:	Device discovery is not allowed from a system account on Windows 2008.
WORKAROUND:	Specify user account credentials that RMP will use before it scans the network. This is provided via: DD_USER DD_PASSWORD in the rmp.cfg file (i.e. ManagementPortal/etc/rmp.cfg). DD_USER can be the user name or the domain qualified; for example, johndoe or domain\johndoe DD_PASSWORD is the password of that account, clear, DES or AES encryption all allowed in these two configuration parameters. The account specified via DD_USER and DD_PASSWORD must have Administrative privileges for the Device discovery to work.

NO data present in the 24Hour Service Event view in the CA Standard dashboard part

PROBLEM:	Sometimes, 24 Hour Service Events widget in the operational view of the HPCA Operations dashboard is empty, even if there were service events in the last 24 hours..
CAUSE:	Unknown.
WORKAROUND:	Launch the related report by clicking the Launch Report icon in toolbar at the bottom of the widget. The "Service Events (24 hours)" will have the correct data.

CAS UI: 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.

Configuration Management: Migration from 5.x loses Policy Resolution settings

PROBLEM:	When migrating from 5.x to 7.2 or forward policy resolution settings are sometimes lost.
CAUSE:	Current process attempts to preserve the CORE data from being updated and lost by not allowing the existing to get overwritten and have the new data lost. The issue here is that there are some instances where the data should get updated with the customer's changes and this is hard to identify in an automated method.
WORKAROUND:	The output file needs to be reviewed because some data may not get in and will need to be added manually.

Application Manager Agent: 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:	HP will provide the export decks with the fixes that will correct this problem.

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 HP Client Automation Administrator Publisher.
CAUSE	Not known
WORKAROUND:	There is no workaround. Install and Remove operations work as expected with the Publisher. Verify and Repair operations work as expected with all software other than the Publisher.

Application Self-Service Manager: Repairing or Removing the HPCA Agent on Vista may display dialog indicating files are in use

PROBLEM:	During a Repair or Remove operation of the HPCA Agent on Vista, a dialog may be presented that indicates files are in use and must be closed.
CAUSE	Not known
WORKAROUND:	Dispose of the dialog by clicking 'Ignore' or 'OK', depending on the dialog that is presented. The requested repair or remove operation will then proceed normally.

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.

Application Self-Service Manager: Manual install of Agent will set a dynamic port for the HPCA Management Agent service, which may cause connectivity problems if a firewall is present

PROBLEM:	Manual agent installs with setup-standard.cmd will incorrectly use a dynamic port for the HPCA Management Agent service. Should a firewall be configured on the agent system, certain connections from the HPCA Console may be blocked.
CAUSE	Not known
WORKAROUND:	<p>Edit setup-standard.cmd and add the '-port 3463' argument, identified below in red.</p> <p>::Lauch command to install the RMA service along with it's required parameters</p> <p>"%AGENT_DIR%\nvdkit" "%AGENT_DIR%\rma.tkd\bin\rma-mgt.tcl" install -url http://%1:3466/proc/rmp -port 3463</p> <p>This will cause the HPCA Management Agent service to use the proper port, 3463.</p> <p>Note that agent deployments from the HPCA Console will always result in the HPCA Management Agent service listening on port 3463. This modification to setup-standard.cmd is only required when manually installing the agent.</p>

Application Self-Service Manager: Manual upgrade of Agent may detect temp file in use and require user interaction on Vista

PROBLEM:	Manual agent upgrade with setup-standard.cmd displays dialog indicating a .tmp file is in use. Problem only occurs if upgrade is being performed on Vista. Problem does not occur if agent is deployed from the console.
CAUSE	Not known
WORKAROUND:	During the upgrade, dispose of the dialog (by clicking Ignore or OK, depending on the dialog) to continue with the agent install.

Application Self-Service Manager: RALF disappears upon reboot on XPe

PROBLEM:	When installing RALF by itself via HPCARalf75.msi without triggering an HPCA agent installation, and rebooting the ThinClient, the RALF installation disappears.
CAUSE:	Installing HPCA-RALF by itself does not trigger an Enhanced Write Filter (EWF) commit, so no data written is committed to Flash causing the installed bits to disappear upon reboot. If installing the HPCA agent soon after RALF, the HPCA agent installation triggers a commit and thus causes RALF to be persistent.
WORKAROUND:	When installing RALF alone, force an EWF commit to make sure it is persistent.

Application Self-Service Manager: Agent removal on CE unsuccessful

PROBLEM:	The CE Agent removal appears as 'Failed' in console.
CAUSE	The removal of the agent CE leaves behind 2 log files. As a result, unload.exe displays a dialog stating the fact that there are 2 log files left behind.
WORKAROUND:	Pressing OK to dismiss the dialog will successfully end the console job.

Application Self-Service Manager: Default DB has outdated execute.rex in AUDIT.BEHAVIOR

PROBLEM:	UNIX File Audit Behavior Service may not work.
CAUSE	Not known.
WORKAROUND:	Get the latest execute.rex file available at the support site.

Application Self-Service Manager: Checkpoint restart always show 0% and 0 bytes no matter when network connection is lost.

PROBLEM:	0 % is always displayed in the UI irrespective of bytes downloaded.
CAUSE:	Delay in display values.
WORKAROUND:	Ignore the display values. The file will still be valid.

Application Self-Service Manager: File-based Write Filter issues on HP thin client

PROBLEM:	If the File-based Write Filter is present on HP thin client or HP RPOS machines and not used, there may be unexpected behavior by the HPCA Agent and install.
CAUSE:	The HPCA Agent will attempt to manage the File-based Write Filter if it is found to be present.
WORKAROUND:	The File-based Write Filters dlls (FBWFDLL.DLL and FBWFLIB.DLL) should be renamed to something else so that HPCA does not attempt to use them.

Messaging Server: 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: OOB DASH device boots from hard-drive regardless of boot order

PROBLEM:	If the user has included USB in the boot order and if the USB boot source is not bootable, the system will boot from the hard-drive regardless of the other boot sources in the boot order. This will cause a problem when the user is performing boot operations on a DASH device when selecting Operations -> Out Of Band Management -> Device Management -> <DASH Device> -> Remote Operations.
CAUSE:	Issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware.
WORKAROUND:	None

OOBM on Core: OOB DASH device tries all boot sources including ones that are not specified in the boot order

PROBLEM:	If the user selects the persistent boot option, the device will try all the boot sources, including those that are not specified in boot order. This will cause a problem when the user is performing boot operations on a DASH device when selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Remote Operations.
CAUSE:	Issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware.
WORKAROUND:	None

OOBM on Core: Cannot change boot configuration setting for OOB DASH device to default and permanent boot

PROBLEM:	It is not possible to change the boot configuration settings to default and permanent boot. The user cannot change this to one time boot. However, the user can change the settings for second boot configuration setting listed to one time boot. This will cause a problem when the user is performing boot configuration settings on a DASH device when selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Boot Configuration.
CAUSE:	The settings are hard coded to the permanent boot configuration setting for the first boot configuration setting listed.
WORKAROUND:	None

OOBM on Core: Must perform boot order operation before reboot of OOB DASH devices for one time boot setting

PROBLEM:	If the user selects the boot configuration setting of one time boot for a reboot operation on Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware, the user is required to perform the boot order operation before reboot. Otherwise, the remote operation will display erratic behavior. Also note that although the user has performed an explicit boot order operation, after reboot, the boot order will get reset to default boot order. This will cause a problem when the user is performing boot operations on a DASH device by selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Boot Configuration.
CAUSE:	Due to issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware.
WORKAROUND:	None

OOBM on Core: Incorrect network controller set as first boot source for OOB DASH devices

PROBLEM:	For Dash-enabled devices, if you change the boot order to make Network the first boot device, it will set the embedded network controller as the first boot source instead of the Broadcom DASH NIC. As a result, the PXE boot from the Broadcom NIC will fail. This is a known issue. This will cause a problem when the user is performing boot operations on a DASH device by selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Remote Operations.
CAUSE:	Due to issues with the Broadcom NetExtreme Gigabit Ethernet Plus NIC-based hardware.
WORKAROUND:	To work around this issue, go into the F10 Setup Advanced menu. The embedded NIC PXE option ROM can be prevented from loading by disabling the NIC PXE Option ROM Download option in the Device Options list. Retry booting from the Broadcom PXE after you have disabled this option.

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: Deployment of software list to OOB devices throws network error 26 in TLS mode

PROBLEM:	Deployment of the software list to OOB devices causes the network error of 26 to be thrown in TLS mode. This will cause a problem when the user is performing the software list deployment operation by selecting Operations -> Out Of Band Management -> Device Management -> Software List Deployment.
CAUSE:	Client certificate is not properly configured on HP Client Automation install machine.
WORKAROUND:	Install the client certificate on HP Client Automation installed machine and specify the certificate's subject name as the value for the "ca_server_commonname" property in the config.properties file. Refer to the HPCA Out Of Band Management User Guide for information about installing client certificate and the config.properties file location.

OOBM on Core: Cannot go to the next page from the Remote Operations Wizard Task page for OOB devices

PROBLEM:	The Remote Operations Wizard on OOB devices freezes so that you are not able to proceed to the next page. This will cause a problem when the user is performing boot operations on a DASH device by selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Remote Operations.
CAUSE:	Incorrect version of the JRE.
WORKAROUND:	Install JRE version 1.6 or later and select the option in the Internet Explorer to install the JRE plug-in. To select this option, in your Internet Explorer, go to Tools > Internet Options > Advanced and select the Use JRE 1.6 for <applet> (requires restart) option. Restart the Internet Explorer once the JRE is installed and enabled. Note this is a correction for the information provided in the Troubleshooting Chapter of the HP CA Out of Band Management User Guide. The version for JRE is incorrectly stated as 1.5 or later.

OOBM on Core: OOBM remote operations fail on vPro device after changing the provisioned state of the device

PROBLEM:	When changing the provisioned state of a vPro device (including changing TLS mode and re-provisioning the device with a different SCS profile), remote operations on individual or multiple vPro devices fail.
CAUSE:	Inconsistency between the information in the OOBM database and the SCS database.
WORKAROUND:	Select the device for which the provisioned state has changed and click the 'Reload Device Information' button from Operations -> Out of Band Management -> Device Management screen. Alternatively, click the 'Reload Device Information' button (without selecting a device). The latter takes longer but will refresh all device information so that latest information is loaded into OOBM database and is consistent with the information in SCS database.

OOBM on Core: HPCA Cannot connect to SCS and discover vPro devices in some cases involving Windows Server 2008 R2

PROBLEM:	HPCA cannot connect to SCS when HPCA is installed on Windows Server 2008-x64-R2 and SCS and Active Directory are both installed on the same machine running Windows Server 2008-x64.
CAUSE:	Not known.
WORKAROUND:	When HPCA is installed on Windows Server 2008-x64-R2, and it is required that both Active Directory and SCS are on win2k8-x64, then you must install Active Directory and SCS on different physical or virtual machines running win2k8-x64.

OOBM on Core: On OOBM DASH device, one time boot configuration does not reset

PROBLEM:	One time boot configuration on the DASH device is not resetting even after the device reboots. When the one time boot configuration is selected or enabled for any remote operation, it is not unselected or disabled once the remote operation has been successfully completed. Once this problem occurs, all the future remote operations will always use the one time boot configuration. This will cause a problem when the user is setting the one time boot configuration on a DASH device by selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Boot Configuration.
CAUSE:	Issue with the system BIOS.
WORKAROUND:	Change the boot order of the one time one-boot configuration before performing any reboot operation by selecting Operations > Out Of Band Management > Device Management > <DASH Device> > Remote Operations.

OOBM on Core: OOBM groups will fail to reload when the OOBM device database does not have the latest devices

PROBLEM:	OOBM groups will fail to reload and the error "No devices with Given Name" is displayed. As a result, groups will not be updated. This will cause a problem when the user is performing the groups reload operation by selecting Operations > Out Of Band Management > Group Management > Reload.
CAUSE:	OOBM database is not updated with the latest devices.
WORKAROUND:	Perform the OOBM device discovery operation again to update to the latest devices. This will solve the groups reload error.

OOBM on Core: Nothing appears to be happening when performing OOBM remote operations on vPro device

PROBLEM:	When performing a remote operation on a vPro device, no results or error message is displayed.
CAUSE:	<ol style="list-style-type: none">1. Inconsistency between the information in the OOBM database and the SCS database.2. Unavailability of the device on the network
WORKAROUND:	Close the Device Detail window and open a new one. This should allow you to see the error messages. If the problem is caused by an inconsistency between the OOBM and SCS databases, click the 'Reload Device Information' button under Operations > Out Of Band Management > Device Management > Refresh All.

OOBM on Core: Wrong alert subscription status on OOBM device management screen

PROBLEM:	When HPCA is installed on Windows Server 2008 x64 AMD64T, the alert subscription operation, though successful, is incorrectly reported in the status column. This will cause a problem when the user is performing the alert subscription operation on vPro device by selecting Operations > Out Of Band Management > Device Management > Alert Subscription.
CAUSE:	Issue is due to third-party dependencies of OOBM.
WORKAROUND:	None. Alerts, if subscribed to, will be successfully received but status will not be correctly reported.

OOBM on Core: Failure to open telnet session for SOL/IDER operations on OOB vPro devices

PROBLEM:	When HPCA is installed on Windows Server 2008 x64 (AMD64T), the telnet session does not open for SOL/IDER operations. The boot operation however is successful and the machine boots from the correct media. The Heal use case is not fully supported due to this issue. For example, the BIOS updates cannot be performed.
CAUSE:	By default, the telnet client is not installed on Windows Server 2008.
WORKAROUND:	You must install the telnet client by using the server manager option in Windows Server 2008.

OOBM on Core: Telnet session does not open on the client console for OOBM vPro and DASH devices

PROBLEM:	The telnet session fails to open on the client console for vPro and DASH devices on Windows Server 2003 64-bit platforms.
CAUSE:	OOBM is not able to open the telnet connection.
WORKAROUND:	Use HyperTerminal to view the vPro device text console. Configure the PuTTY client to view the DASH device text console.

OOBM on Core: PuTTY client may not show the OOBM DASH client console on Windows 64-bit platforms

PROBLEM:	PuTTY client may not show the DASH client console on Windows 64-bit platforms.
CAUSE:	PuTTY is not able to establish the connection with the client DASH device.
WORKAROUND:	None.

OOBM on Core: I18N issues with OOBM SCS

PROBLEM:	Although HPCA Console can be installed on non English operating systems, there are some restrictions due to dependencies on underlying components and technologies like the hardware BIOS or the Intel SCS. As a result, you cannot enter non English names for several user-defined items, including filters, watchdogs, and policies by selecting Configuration > Out Of Band Management > vPro System Defense Settings. The SOL console for the BIOS setup works only for supported character sets. Similarly, other features may not work as expected in non English locales. Numbers, dates, and time are not being displayed in the format of the non-English operating system's locale.
CAUSE:	Dependencies on underlying components and technologies like the hardware BIOS or the Intel SCS.
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: English path separator is displayed on Japanese locale for OOBM features

PROBLEM:	The HPCA Console shows the English path separator on a Japanese locale. This problem will occur only for the OOBM functionality.
CAUSE:	This limitation is caused by the Intel SCS component.
WORKAROUND:	None.

OOBM on Core: 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 Manager for Windows: Localized message catalogs for Chinese, Japanese, and Korean not supported under LinuxSOS for HPCAS

PROBLEM:	Use of localized message catalog for Chinese, Japanese and Korean is not supported under LinuxSOS for HPCA Starter and Standard license.
CAUSE	Not known
WORKAROUND:	None

OS Manager: Prepviz upload does not check/halt when OSM server is out of disk space

PROBLEM:	The image upload process does not verify that enough free space exists on the OSM 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 OSM server will fail to store the resulting image files. The partial files will be locked for a few minutes until they are automatically deleted.
CAUSE	Out of disk space
WORKAROUND:	Make sure enough free disk space exists on the OSM server so that the image upload may complete successfully.

OS Manager for Windows: 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><settings pass="windowsPE"> <component name="Microsoft-Windows-Setup"> <UserData> <ProductKey> <Key></pre> <p>Example:</p> <pre><UserData> <AcceptEula>true</AcceptEula> <ProductKey> <Key></Key> <WillShowUI>OnError</WillShowUI> </ProductKey> </UserData></pre> <p>Add the Product Key to the following section:</p> <pre><settings pass="specialize"> <component name="Microsoft-Windows-Shell-Setup"></pre> <p>Example:</p> <pre><ProductKey>AAAAA-BBBBBB-CCCCC-DDDDD-EEEE</ProductKey></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 Manager for Windows: Windows 7 – Windows Setup Merge failed to WinXP/Vista with OS+Data partition

PROBLEM:	Deployment of Windows 7 using the Windows Setup method 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. If you are unsure about the partitions on your various targets, always package/deploy Windows 7 using the ImageX deployment method.
CAUSE:	
WORKAROUND:	For customers relying on the Windows Setup deployment method, HPCA will provide a hot fix promptly after the product release.

OS Manager 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 Manager 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">1 Click Start2. Select Settings -> Control Panel3. Click the System Icon4. Select the Memory tab.5. Use the slider on the left to increase the "Storage memory"

OS Manager for Windows: 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">1. Provide the *clean* agent media to publish when you publish an OS.2. Do not change the file name of the MSI file that contains the HPCA agent3. Do not provide multiple versions of the HPCA agent MSI file in the same media directory.

OS Manager for Windows: 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 Manager for Windows: "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 Manager for Windows: 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.

OS Manager for Windows: 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>tcifsredirect.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>http://www.microsoft.com/downloads/details.aspx?familyid=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en</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 Manager for Windows: Windows 2003 R2 SP2 target devices cannot go to desired state after Windows Setup deployment

PROBLEM:	The HPCA Agent is not installed at the end of the OS installation. NOTE: This was observed on Windows 2003 R2 SP2 target devices but may also occur with other pre-Vista versions of Windows.
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"> Navigate to the drive that you selected during the WNI Publisher. Edit <code><drive>:\\$WIN_NT\$.~BT\WINNT.SIF</code> Search for <code>radsetup</code> On the line containing <code>radsetup</code>, replace the first double quote (") with the string <code>command0="C:</code> <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 Manager: In RAID mode, SOS Linux cannot perform legacy capture for a Z600

PROBLEM:	On a Z600 system in RAID mode, booting to a CaptureImage CD behaves as if attempting an image deployment.
CAUSE:	An issue with the Linux SOS ntfs driver results in a failure to be able to access the file system.
WORKAROUND:	Use Windows ImageX image capture.

Patch Management: I18N: Patch Acquisition fails when Core-Standard is installed in Non-ASCII path

PROBLEM:	In Non-English environment, if the DATA_DIR in patch.cfg configuration file contains non-ASCII characters then the Patch Manager Acquisition fails.
CAUSE:	The patch.cfg is in ANSI format and cannot contain any non-ASCII characters.
WORKAROUND:	The patch.cfg has to be saved in UTF-8 format using notepad or any other text-editor and then enter the non-ASCII path in DATA_DIR.

Patch Management: Softpaq 'Bulletin Name' report fails

PROBLEM:	Management > Patch Management > Patches > <Bulletin Name> > Reporting Tab fails
CAUSE:	The Reporting Link is connected to an incorrect report which no longer used.
WORKAROUND:	Use the Reporting tab to view the bulletin reports. Management > Reporting > Patch Compliance Reports > Bulletin Status

Patch Manager Device Compliance Report: 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:	Set -mib option to "Yes". 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.

Proxy: Proxy Server preloading using multicast does not work in UNIX/Linux

PROBLEM:	Proxy server preloading using multicast does not work in UNIX/Linux. The SUSE connect log contains the following error: Error opening control object [MULTICAST] in [/opt/HP/CM/IntegrationServer/etc/rps/] When this occurs, the MULTICAST object is ignored and the connect reverts to unicast.
CAUSE:	Cause not known at this time.
WORKAROUND:	A patch will be issued post-release of this product.

Proxy: RIS-based Proxy Server fails to be installed in Non-Ascii path.

PROBLEM:	Multi-byte characters not written to INI file.
CAUSE:	Using the setup.exe, the installer writes the configuration in the currently active code page. This may become a problem in multi-byte systems if the installation is performed in a English locale and a Multibyte character in the installation path is used.
WORKAROUND:	Use the native locale when installing the software. This will allow for the Multi-byte characters to be written to the INI files with the correct code page.

Usage Manager: Rule Filters are not functional in Standard Edition of Usage Reporting Server

PROBLEM:	In Usage Manager, Rule Filters are not functional in the Reporting Server.
CAUSE:	AUM Admin is not supported for Standard Edition. As a result, Rules cannot be created.
WORKAROUND:	None.

Support

You can visit the HP Software support web site at:

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

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 CD-ROM.

©Copyright 2009 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 DVD.

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.