HP Client Automation Enterprise

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 the HP **Client Automation** infrastructure.

HPCA Portal User Interface

With the advent of the unified Console for HPCA, and the inclusion of a range of upgraded features such as the OS and HPCA agent deployment wizards, and Role-based Access Control, the legacy HPCA Portal *user interface* functionality has been replaced by the HPCA Console.

In a classic HPCA environment, the legacy HPCA Portal *user interface* functionality has been replaced by the Enterprise Manager Console.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.

This document provides an overview of the changes made to the HP Client Automation (HPCA) suite of components for the 7.80 release. It contains a bulleted list of new features and functionality for each component, tables that show current software and hardware support for each component, and tables that show backward compatibility of some of the components of this release with previously released versions of HPCA.

Contents

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)
- Critical enhancements to Security and Compliance
  - Security Certification and Authorization Process (SCAP) certification
  - Additional security benchmarks including CIS (Center for Internet Security) and FDCC 1.2.0.0
  - Multiple additional profiles for reporting and dashboards
- New settings for the Migration Manager
  - Replacement of SMM with Personality Backup and Restore integrated directly into HPCA Enterprise Edition
  - Replacement of settings based on User State Migration Tool (USMT) 3 and USMT 4

See the section, New Features and Enhancements on page 15 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

- With the release of HPCA 7.50, HPCA Starter and Standard are now included as part of the Core and Satellite installation. Depending on your active license, different features will be available from the Core and Satellite console. Refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide* for more information.

- With the advent of the unified Console for HPCA, and the inclusion of a range of upgraded features such as the OS and HPCA agent deployment wizards, and Role-based Access Control, the legacy 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.

- Software and hardware requirements have changed for many products. See Documentation Errata
- The following statement appears in the "Creating the Patch Manager Environment" chapter in the *HP Client Automation Enterprise Patch Manager Installation and Configuration Guide:*

  > **Enable Download Manager:** Check this box to have Download Manager control the download of the required patch files onto the Agent machines using a background, asynchronous process. The Download Manager operates outside of the normal HPCA Agent Connect process.

This statement requires clarification. The Download Manager enables agents to download binary from Proxy Server rather than from Configuration Server. To use the download manager feature, you must configure Proxy Server in your environment. If Proxy Server is not configured in the environment, you can disable the download manager and use the agent connect process to deploy the patches.

- Software and Hardware Requirements on page 7 for details of current support.
- The 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, 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 new product. 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**.

Documentation Library Changes for 7.80

A new user guide was added to the documentation library for this release:

HP Client Automation ThinApp Updater User Guide

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 “Creating the Patch Manager Environment” chapter in the *HP Client Automation Enterprise Patch Manager Installation and Configuration Guide*:

> **Enable Download Manager**: Check this box to have Download Manager control the download of the required patch files onto the Agent machines using a background, asynchronous process. The Download Manager operates outside of the normal HPCA Agent Connect process.

This statement requires clarification. The Download Manager enables agents to download binary from Proxy Server rather than from Configuration Server. To use the download manager feature, you must configure Proxy Server in your environment. If Proxy Server is not configured in the environment, you can disable the download manager and use the agent connect process to deploy the patches.

Software and Hardware Requirements

Only those 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 not withstanding) 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 the operating system requirements for this release, see the HPCA Support Matrix available at the following URL: **http://h20230.www2.hp.com/sc/support_matrices.jsp**

Hardware Support

The following table lists hardware support information.

Table 1 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
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 distribution media.

Table 2 Supported Database Servers

Database Server	Version
Oracle	10.2.0.3
	11.1.0.6
Microsoft SQL Server	2005
	2008
SQL Express	2005
	2008

Oracle Requirements

Required Oracle User Roles

- CONNECT
- RESOURCE

Required Oracle User System Privileges

- CREATE ANY VIEW
- SELECT ANY TABLE
- UNLIMTED 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 7.8 (or 7.5x for version 4.2i customers).

The following tables contain information about the backward compatibility of some components of the HPCA 7.80 release with previously released versions of the product.

Table 3 Backward compatibility for agents and Administrator

Description	CM 4.x RCS \ Database	CM 5.x Configuration Server \ Database	CM 4.x Client Objects	CM 5.x Agent	CM 7.x Agent
CM 4.x, 5.x agents\clients	Y	Y			
CM 4.x System Explorer, Packager, MSI Publisher	Y	N			
CM 5.x Configuration Server Database Editor, Packager, MSI Publisher	N	Y			
CM 4.x Client Explorer			Y	N	N
CM 5.x Agent Explorer			Y	Y	Y
CM 7.x Agent Explorer	N	Y	Y	Y	Y

Table 4 Backward compatibility for packaged applications

Description	Import to 4.x RCS	Import to 5.x Configuration Server	Import to 7.x Configuration Server
Packaged Applications in CM 4.x RCS	Y	Y	Y
Packaged Applications in CM 5.x Configuration Server	N	Y	Y
Packaged Applications in CM 7.x Configuration Server	N	Y	Y

Table 5 Backward compatibility for Patch Agent

Description	CM 4.x Infrastructure, 7.x Patch Manager	CM 5.x Infrastructure, 7.x Patch Manager	CM 7.x Infrastructure, 7.x Patch Manager
Patch Agent 3.x	Y	Y	N
Patch Agent 5.x	Y	Y	Y[1]
Patch Agent 7.x	N	Y	Y

[1] The following patch reports do not work: Product Status, Patch Status, and Release Status

Table 6 Backward compatibility for OS Manager Agent

Description	CM 4.x Infrastructure with 2.1 OS Manager	CM 5.00 Infrastructure with 5.00 OS Manager	CM 5.10 Infrastructure with 5.10 OS Manager	CA 7.x Infrastructure with 7.x OS Manager
OS Manager Agent 2.1	Y	N	Y[1]	N
OS Manager Agent 5.0	Y[1]	Y	Y[1]	N
OS Manager Agent 5.1	Y[1]	Y[1]	Y	Y[2]
OS Manager Agent 7.x	N	N	Y[2]	Y[2]

[1] Except HP-UX re-installs

[2] No support for HP-UX, Solaris, and AIX

Table 7 Backward compatibility for infrastructure components

Description	CM 4.x Infrastructure	CM 5.00 Infrastructure	CM 5.10 Infrastructure	CA 7.x Infrastructure
Enterprise Manager 5.1[1]	N	N	Y	N
Security and Compliance				N
OS Manager 2.1	Y	N	N	N
OS Manager 5.00	N	Y	N	N
OS Manager 5.10[1]	N	N	Y	N
OS Manager 5.11	N	N	Y	Y
OS Manager 7.x	N	N	Y	Y
Configuration Server 5.10	N	Y	Y	N
Publisher 5.00	N	Y	Y	
Publisher 5.10	N	Y	Y	Y
Publisher 5.11	N	Y	Y	Y
Publisher 7.x	N	Y	Y	Y
Messaging Server 5.10	N	Y	Y	N
Messaging Server 5.11	N	Y	Y	N
Messaging Server 7.x	N	Y	Y	Y
Management Portal 5.10	N	Y	Y	N
Application Usage Manager 5.10[2]	N	N	Y	
Application Usage Manager 5.11	N	Y	Y	
Application Usage Manager 7.x	N	Y	Y	Y
Reporting Server	N	N	Y	N

[1] Requires version 5.10 infrastructure

[2] Requires version 5.10 of the Messaging Server and Reporting Server

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 6 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.

Products prior to version 4.2 are now past their end-of-support date. Migration from these unsupported versions to version 7.80 may work, but is not supported.

Migration Strategy

If your current version is:

- **HPCA Core and Satellite 7.20 or 7.5x**, migrate to 7.80 Core and Satellite. Refer to the *HPCA Core and Satellite Migration Guide*.
- **4.2x, 5.x, or HPCA 7.20 Classic,** migrate to HPCA version 7.80 Classic. Refer to the product-specific migration guides on the media.

  When migrating a Classic environment, HP recommends migrating primary infrastructure components (such as Configuration Server, Portal, Messaging Server, Proxy Server, and HPCA agents) before migrating extended infrastructure components (such as Patch Manager, Reporting Server, and Enterprise Manager).

Additional Migration Notes

- **Batch Publisher**: The 7.80 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**: An enhancement has been made to the DB Scanner Utility, `csdbscanner`. This utility can be used in two modes, namely, **on the database** and **on the export decks**. The database scan mode now supports an additional **domain** option that allows you to run a scan for a specific database domain. This enables you to scan different domains in parallel. For more information, refer to the *HP Client Automation Configuration Server: Configuration Server and Database Migration Guide*.
- **Multicast Server**: The 7.80 installation program will upgrade the Multicast Server, so you must follow the instructions below in order to re-apply any customizations that have been made to its configuration file, `mcast.cfg`.

1. Back up (move or rename) your existing `mcast.cfg` file.
2. Install the Multicast Server.
3. Apply the customizations from the pre-7.80 configuration file to the new `mcast.cfg` file.

   Multicast Server configuration file updates are limited to:

   The parameters that are contained in the `mcast::init {}` section.

   The four optional parameters at the end of `mcast.cfg`: `-rimurl`, `-rcsurl`, `-adminid`, and `-adminpwd`.
4. Restart the Multicast Server service, **mcast**.

For more information, refer to the *HP Client Automation Multicast Server Installation and Configuration Guide*.

- **SSL/Certificate Generation Utility**: Make sure that you have the latest version of this utility by copying the contents of the `certificate_mgmt` directory from this HPCA release media and using them to replace your existing certificate-management files. For more information, refer to the *HP Configuration Management SSL Implementation Guide*.
- **Mini Management Server**: The 7.80 installation program will upgrade the Mini Management Server, so you must follow the instructions below in order to re-apply any customizations that have been made to its configuration file.

  1. Back up (move or rename) your existing configuration file, `rmms.cfg`.
  2. Install the latest Mini Management Server.
  3. Apply the customizations from the pre-7.80 configuration file to the new configuration file, `rmms.cfg`.
  4. Restart the Mini Management Server service.

New Features and Enhancements

This section contains a list of new features, enhancements, fixed defects, and known issues for the components in the HPCA 7.80 release.

➤ **HPCA Portal User Interface**: With the advent of the unified Console for HPCA, and the inclusion of a range of upgraded features such as the OS and HPCA agent deployment wizards, and Role-based Access Control, the legacy 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 following sections describe the new features and enhancements that have been introduced in the 7.80 release for the various components in HPCA.

Core and Satellite Servers

- HPCA can now manage client devices running Windows 7 and Windows Server 2008 R2.
- The HPCA Console is the web-based interface with which an HPCA administrator can manage an HPCA environment. 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.
- Advanced policy management is now available through the HPCA Console. This new feature includes the ability to set default and override policies, create policy links, and set policy resolution options.
- LDAP request performance has been improved.
- There are many RMS improvements, which include Foreign key constraints on the DB structure, improved table control, improved speed for table creation, and so on.
- Remote assistance support to HPCA has been added.
- The user experience for HPCA integration with ThinApp has been greatly improved.
- Ability to delete devices from all of the HPCA databases (Patch, Usage, Core and so on) which was previously only in the standard edition.

Configuration Server

- The following REXX scripts are available in `HPCA_InstallDir\ConfigurationServer\rexx`.

  > These are field-developed scripts; they are not supported as part of the official HPCA support process. However, they will be supported and updated in the Client Automation **community content** section on the BSA Essentials Network, www.hp.com/go/bsaenetwork.

  — **BPRERESO**: AD policy support script

  — **RADBMPRT**: RadDBUtil import utility script

  — **RADBXPRT**: RadDBUtil export utility script

  — **RADDBULL**: RadDBUtil PATCHMGR bulletin/ZSERVICE delete utility script

  — **TREEMPRT**: live Configuration Server tree import (CSDB drag/drop)

  — **TREEXPRT**: live Configuration Server tree export (CSDB drag/drop)

- The `MGR_SSL` section now allows you to specify the cipher set to use for the Configuration Server. Use the `edmprof` entry `SSL_CIPHERS`.
- The `MGR_CLASS` section in the `edmprof` entry can now support more than 256 classes because you can now specify wild-cards (& and !) for the domain and class names. However, the number of total entries is still limited to 256.

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 Manager for Windows

- Support for Windows 7 and Windows 2008 Server R2

Patch Manager

- Red Hat and SuSE patch acquisition process has been greatly optimized, reducing the vendor's metadata download and acquisition times. If you select the exclude option when creating an acquisition job, the metadata for the excluded platforms are no longer downloaded This improvement affects all acquisitions of Red Hat and SuSE patches regardless of the Patch Manager distribution method (traditional or metadata model) you use.
- SuSe 11, Red Hat 5.4, Windows Server 2008 SP2, and Windows Vista SP2 support is now available.

- Several items that previously could only be configured by editing a configuration file now have User interfaces. Interfaces have been provided for the following.
  - Internet available
  - Management of Installed Bulletin Behavior (MIB)
  - MIB=None is the default OOTB
- The performance of the Patch Agent has been greatly improved.
- Reports have improved usability in and administrative flow.
- The percentage patched graphs have been added to clearly indicate patch compliance.
- More information has been added to the Patch Reports (MSI version, WUA version, MS criticality ratings, and so on).
- Better support is now available for Microsoft patches which are superseded by newer patches.
- UI support has been added for importing and exporting the gateway cache.

Security and Compliance Manager

- Security and Compliance data injection methodologies have been improve to provide better performance.
- Improved Compliance usability (multiple profile support, etc. in reports, dashboards, and so on) has been introduced.
- Center for Internet Security Content has been added.
- HPCA now has Security Content Automation Protocol (SCAP) certification.
- Control over historical compliance dashboard pane has been improved.

Fixed Defects

The following defects have been fixed in this release.

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** Job Creator is missing if agent or OS deployment job is created by AD users

PROBLEM:	HPCA agent and OS deployment jobs that are created by an external AD user have an empty Creator field.
CAUSE:	AD creator name is not properly extracted for HPCA agent and OS deployment jobs.
WORKAROUND:	If tracking the creator is important, use the Portal to create HPCA agent and OS deployment jobs.

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:	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.

Core and Satellite: **RESOLVED** 7.5 Does not match certificate is seen in dmabatch.log on SSL Mode

PROBLEM:	The following syntax error is observed in some logs. `Error: main: Background Error: wrong # args: should be "syslog level msg ?tag? ?ts?" while executing "syslog note “$tag unable to parse subject for valid dns name – skipping man in the middle check”"` Note: This error occurs only when SSL is enabled.
CAUSE:	Incorrect man-in-the-middle check.
WORKAROUND:	None. If this error appears in a log, ignore it.

Configuration Server: **RESOLVED** RadDBUtil no longer honors the {-logmode a} for appending to logs

PROBLEM:	`RadDBUtil` in 7.20 RC2 no longer honors the `{-logmode a}` for appending to logs. New logs are generated for each instance of `RadDBUtil` regardless of `{-logmode a}`.
CAUSE:	An enhancement to expose the LOGROLL capabilities to be able to be set from the command line introduced a situation where the “`–logmode a`” (append log) no longer works.

WORKAROUND:	Although there is no quick workaround as `log.roll` is being unconditionally invoked by `raddbutil.exe` and `logmode` has be disabled, You can develop a script that will direct output to a different log file and then append the contents on that log to another log so in essence, doing the append.
	Example:
	if today you run from a script:
	`raddbutil.exe export -output foo -walk 0 PRIMARY.POLICY.USER.RPS`
	Which updates the ../log/raddbutil.log
	If you change this command line in your custom scripts to:
	`raddbutil.cmd export -output foo  -walk 0 PRIMARY.POLICY.USER.RPS`
	The following being the content of raddbutil.cmd –
	`@set logfile=..\log\raddbutil.log`
	`@del /F /Q %logfile%.new`
	`raddbutil.exe %1 -logfile %logfile%.new %2 %3 %4 %5 %6 %7 %7 %9 %10 %11`
	`@type %logfile%.new >> %logfile%`
	`@del /F /Q %logfile%.new`

Enterprise Manager: **RESOLVED** Users with a UTF-8 password cannot log on

PROBLEM:	When internal (PORTAL) users have UTF-8 passwords, they are unable to log on.
WORKAROUND:	ASCII passwords must be used.

Enterprise Manager: **RESOLVED** Disabled DTM Job can still be downloaded to agent during synchronization

PROBLEM:	After disabling DTM jobs using the Disable icon, the jobs can still be downloaded to HPCA agents when they synchronize with the DTM server.
CAUSE:	A defect in the DTM server allows Disabled jobs to remain available to HPCA agents.
WORKAROUND:	Use the Delete icon (rather than Disable) to delete DTM jobs that should not be available to HPCA agents.

Enterprise Manager: **RESOLVED** Target missing in Target Details panel for Agent or OS Deployment Jobs

PROBLEM:	For HPCA agent or OS deployment jobs that are targeted to a list of devices, when drilling down the job, the Target Details panel for the job shows no targets.
CAUSE:	A temporary group was used to contain the list of devices, and that temporary group was deleted after the job completed.
WORKAROUND:	No workaround; this has no impact to the functionality of the deployment jobs.

Enterprise Manager: **RESOLVED** When Agent or OS Deployment is Running or Scheduled, the target is 0

PROBLEM:	When an HPCA agent or OS deployment job is running or scheduled, the Target column of the Current Job list will show "0 Target Devices."
CAUSE:	The job engine does not return target information when a job is active.
WORKAROUND:	No workaround; this has no impact to the functionality of the deployment jobs.

Enterprise Manager: **RESOLVED** Communication to job process engine is not encrypted (Problem occurred in Classic only)

PROBLEM:	Communication between the Enterprise Manager and the job process engine that executes the Notify commands is not encrypted by default.
CAUSE:	The default setting for `opeurl` in `<InstallDir>/CM-EC/tomcat/webapps/em/WEB-INF/Console.properties` is as follows: `http\://localhost\:8080/ope/resources`, This is an unencrypted channel.
WORKAROUND:	Modify the `Console.properties` file, and change the `opeurl` property to: `https\://localhost\:8443/ope/resources`.

Enterprise Manager: **RESOLVED** HP Live Network connection error when HPCA Core is installed in a path containing non-ASCII characters

PROBLEM:

When HPCA Core is installed to a directory path that contains non-ASCII characters, any attempt to perform an update from HP Live Network using the console or using the Vulnerability Server command line utility, `content-update.bat`, will result in an error. When you look at the `vms-server.log` or `vms-commandline.log` files in the `<install-dir>\VulnerabilityServer\logs` directory, you may see an error similar to this:

```
UnicodeDecodeError: 'ascii' codec can't decode byte
```

CAUSE:

The embedded HP Live Network Connector will not function properly if it is installed in a path that contains non-ASCII characters.

WORKAROUND:

Relocate the embedded HP Live Network Connector to a directory that does not have non-ASCII characters in the path, and then configure HPCA to point to the new location:

1. Go to the HPCA installation directory, and locate the sub-directory named `LiveNetwork`.
2. Copy the `LiveNetwork` directory and all of its contents to the root path on your system (for example, `C:\LiveNetwork`)
3. Open the HPCA Console. Go to the **Configuration** tab. Expand **Infrastructure Management**, and select the **Live Network** settings section.
4. In the **HP Live Network Connector** field, change the path to the location where you copied the embedded HP Live Network Connector. Be sure that you include the full path to the `live-network-connector.bat` file (for example, `C:\LiveNetwork\lnc\bin\live-network-connector.bat`).
5. Click **Save**.

Enterprise Manager: **RESOLVED** Compliance scans fail on Vista Simplified Chinese platforms

PROBLEM:

Executing the compliance scanner on a Vista Simplified Chinese platform results in the below error being displayed in the `scap-director.log` file:

```
2008-10-28 15:57:45] Scanner did not complete normally: Code (CHILDSTATUS
2216 255) : STDERR Traceback (most recent call last):
  File "scapscanner.py", line 325, in <module>
  File "scapscanner.py", line 294, in main
  File "ovalparser.pyc", line 1703, in evaluate
  File "ovalparser.pyc", line 1539, in addAndPrintError
  File "ovalparser.pyc", line 1532, in printError
UnicodeDecodeError: 'ascii' codec can't decode byte 0xd3 in position 84:
ordinal not in range(128)
[2008-10-28 15:57:45] Scan failed, aborting
```

CAUSE:

The compliance scanner is not able to correctly parse returned data from a Vista Simplified Chinese (SCH) platform.

WORKAROUND:

Currently none. This may be fixed in a future version of the compliance scanner available through HP Live Network updates.

Enterprise Manager: **RESOLVED** The content-update.bat command line utility does not work if the directory path contains parentheses

PROBLEM:

Executing `content-update.bat` results in an error similar to:

```
\Hewlett-Packard\HPCA\VulnerabilityServer\bin\..\..\tomcat\webapps\vms\WEB-INF\lib was
unexpected at this time.
```

CAUSE:

The `content-update.bat` utility will exit with an error if the installation path for Enterprise Manager contains a parenthesis character. The `content-update.bat` utility does not properly handle directory paths that contain parentheses.

WORKAROUND:

Install Enterprise Manager to a directory that does contain any parentheses.

Enterprise Manager: **RESOLVED** CVE definition is truncated when written to the database

<table>
<tr><td>PROBLEM:</td><td>The <code>vms-server.log</code> file will list exceptions from the database indicating that a record could not be updated due to size limits being exceed. Additionally, in various CVE/OVAL reports a CVE entry may be displayed with a severity of “Unknown,” when there is an actual severity associated with that CVE.</td></tr>
<tr><td>CAUSE:</td><td>The CVE description is larger than the supported 2000 characters.</td></tr>
<tr><td>WORKAROUND:</td><td>If a CVE is displayed with a status of “Unknown,” and there is a known status, you can take either (or both) of the following actions:
<ul>
<li>Look up details about the CVE from either NIST or MITRE.</li>
<li>Update the data base directly with the missing CVE contents using a SQL update statement such as the following:
<pre>
UPDATE VM_CVE
   SET
      description = '... customer selected description text...',
      severity = 'High',
      cvss = '9.3',
      cvssimpact = '10.0',
      cvssexploit = '8.6',
      cvssvect = '(AV:N/AC:M/Au:N/C:C/I:C/A:C)'
   WHERE cveid = 'CVE-2008-4841'.
</pre></li>
</ul></td></tr>
</table>

Enterprise Manager: **RESOLVED** Enterprise Manager console does not open from installed shortcuts (or during installation process)

PROBLEM:	The launched browser window directed to the Enterprise Manager console during installation, from the desktop shortcut, or from the program group icon will redirect to the local system IP address on port 80. If a web server is running on port 80 of the local system, that web server's default page is shown. Otherwise, the browser will display a 404 error.
CAUSE:	The browser on the Enterprise Manager server is not configured to bypass the proxy server for local addresses.
WORKAROUND:	The browser must be configured to bypass the proxy server for local addresses. For Internet Explorer, this setting is accessed in the Tools → Internet Options → Connections Tab → LAN Settings button. Select Bypass proxy server for local addresses. For Firefox 2.x, this setting is accessed in the **Tools → Options → Advanced Settings → Network Tab → Settings** button. The **No Proxy For** box must contain: `localhost, 127.0.01` For Firefox 1.x, this setting is accessed in the **Tools → General Section → Connection Settings** button. The **No Proxy For** box must contain: `localhost, 127.0.01`

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 for Windows: **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 ** Database not up to date after migration

PROBLEM:	When the Configuration Server Database is migrated to v7.50 by following the steps in "Upgrading a Windows Database" chapter of the Configuration Server and Database Migration Guide, some of the resources in OS domain will not be the latest.
CAUSE:	The database deck used for migration doesn't contain the latest files.
WORKAROUND:	After completing the database migration perform the following steps: 1. Copy os.xpi and os.xpr from <Configuration Server install media>\management_infrastructure\configuration_server\dbdecks\osmgr to <Configuration Server install directory>\bin directory 2. Stop the Configuration Server service if it is running. 3. Open a command prompt and change the directory to <Configuration Server install directory>\bin. 4. Run the following command: ZEDMAMS VERB=IMPORT_INSTANCE,FILE=os.xpi,XPR=os.xpr,TIME=OLD,PREVIEW=NO, DUPLICATES=MANAGE,CONTINUE=YES,REPLACE=YES

OS Manager for Windows: ** RESOLVED ** Can't get to desired state if agent was installed under non-ascii path

PROBLEM:	If 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 CA Agent under a non-ASCII path.

OS Manager for Windows: ** RESOLVED ** Localized message catalogs for Chinese, Japanese, and Korean not supported under LiInuxSOS for HPCAS

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

NOTE: The following languages are now supported: Simplified Chinese, Japanese, English, French, German, Spanish, and Brazilian Portuguese.

OS Manager for Windows: **RESOLVED** Fail to set keyboard mapping with fr in WinPE SOS

PROBLEM:	For the WinPE Service OS, setting keyboard was only supported with product versions that supported "de" and "fr" completely; that is, they provided "de_DE" and "fr_FR" message catalogs. The OS.BEHAVIOR instance attribute, KBDMAP was not supported.
CAUSE	Not known
WORKAROUND:	To switch keyboard and messages, use the OS.BEHAVIOR attribute LANG. When the OS.BEHAVIOR instance attribute is set to either LANG=de_DE or LANG=fr_FR, both localized messages and keyboard are enabled for the associated language. The behavior of ROMA under WinPE SOS is the following: ROMA will display messages in English until it has downloaded the BEHAVIOR.LANG setting from the infrastructure. Upon receiving the BEHAVIOR.LANG setting. ROMA will detect the change and trigger the WinPE SOS to change locale and then restart. Upon restarting, all messages will be in the specified language. This does not affect setting the keyboard on the more general basis: The keyboard can be set using a "KBDMAP=de" parameter added to the PEAPPNED line of the PXE configuration file or the ROMBL.cfg file on the ImageDeploy or Capture CDs.

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.

Patch Manager: **RESOLVED** Patch Manager: Download Manager - Initialization Delay is supposed to be in seconds and not minutes

PROBLEM:	The ‘Delay initialization’ attribute says (Minutes), instead of saying (Seconds) on this page in the Patch Administrator Console: Configuration > Environment Settings > Agent Options page > Download Manager Options
CAUSE:	The user interface is not converting the ‘Delay Initialization’ value into seconds, which is required when it is written to the Configuration Server Database > PRIMARY (file) > PATCHMGR (domain) > CMETHOD (class) > DISCOVER (instance).
WORKAROUND:	Manually convert from Minutes to Seconds and enter a Download Manager ‘Delay Initialization’ attribute value in seconds.

Patch Manager: **RESOLVED** Configuration Server PUSHBACK is not honored by Patch Agent

PROBLEM:	The Patch Connect ‘Retry’ option may not work as desired due to the pushback from Configuration Server not being honored.
CAUSE:	For the Retry option to work properly there are two components that need modifications: patchagt.tkd and nvdkit.
WORKAROUND:	Check these sites for fixes to `patchagt.tkd` and `nvdkit` and apply them when available: 1. The fix for `patchagt.tkd` will be posted to the HP Patch Manager Update web site and later as part of Agent Updates. Agent Updates are obtained during an acquisition and the fix is automatically published and distributed. 2. The fix information for `nvdkit` will be posted to the Agent Update Information page.

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: 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: 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 can not edit that in the UI.
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:	You will need to edit HPCA/dcs/dmabatch.rc to manually change the port to match the upstream port.

Core and Satellite: Downloads from Satellite Data Cache is Slow in 7.8

PROBLEM:	Download speed from satellites are 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: 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 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', synching 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 synched with the PRODUCTS class and the reports will correctly display the list of applicable products.

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 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: 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 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:	When trying to access a device through the Remote Desktop connection using Internet Explorer 6 (IE6), you might get an error: 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. For more information, refer to the Troubleshooting section of the online help
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:	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:	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 is 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 is 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: Mac Agent install bits are not available in the Core and Satellite installation media

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.

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

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.

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 overwitten 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.

Adapter for Service Desk: Service Desk does not work with new data directory

PROBLEM:	Service Desk does not work with a new “data” directory in HP OpenView Service Desk Management Server 5.10 patch 7.
CAUSE:	In OVSD5.10 patch 7, the data directory is changed to `c:\Documents and Settings\All Users\Application Data\HP\HP BTO Software\`. As a result, Service Desk cannot load the configuration file from the new directory.
WORKAROUND:	When you install HP OpenView Service Desk Management Server 5.10 patch 7, in the step “Choose the data folder”, set the new data folder to `C:\Program Files\HP OpenView\data`.

Administrator/Admin Packager: Component Select mode needed to package links and registry keys

PROBLEM:	Need to enable Component Select mode in the Packager to package links or registry keys.
CAUSE:	The Packager no longer enables component selection mode by default.
WORKAROUND:	To enable component selection mode in the Packager, add a variable to ZMASTER called PKGCOMP and set the value to 'Y'. Component Selection mode will then be enabled for the Packager.

Administrator/Admin Packager: 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: 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: 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: 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: 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 Publisher: 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: 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: 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: 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 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: 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:	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. For example for the RAM_WIN32_NT_7_8 PRDMAINT instance do the following: 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 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.

Application Self-Service Manager: Data download via SSL requires 7.5 agent upgrade patch

PROBLEM:	The 7.50 HPCA agent is unable to perform a data download using **HTTPS** without an upgrade patch. The HTTPS handshake closes the connection prior to any data transfer. HPCA agent SSL support over a **TCP/IP** connection is functional; it is not part of this Known Limitation.
CAUSE:	The latest HPCA agent code requires an additional update to enable HTTPS support.
WORKAROUND:	A 7.50 HPCA agent patch is required to enable HTTPS connections.

Application Self-Service Manager: Problems uninstalling the Windows CE agent

PROBLEM:	You cannot uninstall the Windows CE agent from the Control Panel's Add/Remove programs after a machine reboot.
CAUSE:	The HP Client Automation Agent.unload file is missing from the Windows folder
WORKAROUND:	Reinstall the agent

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: RALF disappears upon reboot on XPe

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

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 **Ignore** or **OK**, depending on the dialog) to continue with the agent install.

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: 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: RADSVMAN GPFs when running req=un-install

PROBLEM:	RADSVMAN GPFs when req=un-install is passed on the command line.
CAUSE	Not known.
WORKAROUND:	Remove the ZSERVICE instance of the particular application from the policy.

Application Self-Service Manager: Agent shows up as uninstalled when running Thinpro image 31

PROBLEM:	If a device registered with the CAS Server has a previously installed Agent running Thinpro image 31, the Agent will show up as "NOT INSTALLED" under agent status, even though the Agent is properly installed. If you try to redeploy the Agent, you will get an error.
CAUSE	Image 31 has an older version of the registration and loading facility (RALF), which does not rescan for agent presence.
WORKAROUND:	Uninstall the agent and redeploy it. The status will be correctly set as installed.

Application Self-Service Manager: 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: 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: 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: Unable to read catalog when migrated from 4.08 to 7.80

PROBLEM:	Error message is displayed after Agent migration.
CAUSE	Not known.
WORKAROUND:	Ignore the error message because the Agent seems to be appropriately migrated. After the migration is complete, launching the 7.80 Agent and performing install/verify/remove of a service works fine. Inspecting Agent modules for date/time stamp indicates that all Agent modules are from 7.80.

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: 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: 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: Agent Install for Macintosh PowerPC does not run

PROBLEM:	Install for Mac PowerPC (MacPPC) will not run.
CAUSE:	File in Windows format
WORKAROUND:	Run `sudo ./setup` instead of `sudo ./install` from terminal window. Enter the admin password. The installer will appear behind terminal window and will need to be brought to the front.

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: 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.

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: After deferral in CDF, radsched log shows insufficient buffer size errors.

PROBLEM:	Radsched log reports insufficient buffer size errors after a deferral in CDF.
CAUSE:	CDF creates a ZTIMEQ entry to defer the connection to a later date. The ZOBJID that CDF uses is an eye catcher that causes a buffer resize to occur when the scheduler processes the entry.
WORKAROUND:	This is a warning in the log and should cause no problems with operation of the scheduler.

Application Self-Service Manager: RSM GPFs if RGB values are used for colors

PROBLEM:	If RGB values are used for the custom colors in the RADUICFG instance for RSM, RSM may GPF.
CAUSE:	RSM expects the RGB values to be in a very specific format. The code does not do a validation before attempting to use the RGB value.
WORKAROUND:	When specifying the color for customization, use either a text literal ("red", "blue") or an RGB value that is formatted "R,G,B", for instance - 255,255,255. If using the RGB format, decimal numbers must be specified as hex representation is not supported.

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: Remote Control from Console not available for Linux thin clients running Debian

PROBLEM:	The remote control feature in the HPCA Console uses HTTP to communicate with a VNC Server. This does not work with the latest HP Linux thin clients running Debian or ThinPro.
CAUSE:	The HP Linux-based thin client does not include support for HTTP with the VNC Server. It requires a VNC Viewer to make a remote connection.
WORKAROUND:	Download a VNC viewer such as TightVNC for remote control for these devices.

Application Self-Service Manager: Factory default password required for TPM Enablement

PROBLEM:	Configuring the Trusted Platform Module (TPM) enabled chip on compatible HP devices requires use of factory default password
CAUSE:	Password resets are not enabled.
WORKAROUND:	Use the factory default password or leave the BIOS Admin Password setting as blank when configuring TPM Enablement in the Console.

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: 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: 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.

Enterprise Manager: It is possible to restart a disabled directory service

PROBLEM:	When the Startup type for a directory service is set to Disabled, that service can still be started using the Restart button on the **Configuration → Directory Services** tab.
CAUSE:	The HPCA Portal allows the Restart operation to be performed on a disabled directory service.
WORKAROUND:	Use Start and Stop operations instead of Restart.

Enterprise Manager: Error occurs when running Enterprise Manager using Internet Explorer 6 with SSL

PROBLEM:	You cannot run Enterprise Manager using Internet Explorer 6 with SSL if HTTP1.1 is enabled.
CAUSE:	Limitation of Internet Explorer 6.
WORKAROUND:	In Internet Explorer 6, clear the **Use HTTP1.1** option in **Tools→Internet Options→ Advanced→HTTP 1.1 Settings**. Then, close Internet Explorer, and open a new browser window. Simply refreshing the current Internet Explorer window will not fix the problem. Alternative Workaround: Upgrade to Internet Explorer 7.

Enterprise Manager: Cannot start Virtual Machines

PROBLEM:	Virtual Machines will not power on.
CAUSE:	A licensing defect in ESX version 3.5 Update 2 (build number 103908), prevents Virtual Machines from being started after a certain date.
WORKAROUND:	Upgrade to ESX version 3.5 Update 2 build 110268 (or later).

Enterprise Manager: Wizard screens do not scroll properly

PROBLEM:	When you resize a wizard screen small enough for scroll bars to appear, dragging the scrollbar may not work correctly. You may need to drag it farther than expected.
CAUSE:	The scroll bar does not drag correctly.
WORKAROUND:	Click the scroll bar buttons ▲, ▼, ▶, or ◀ to scroll to a new area of the wizard screen, or click a specific location in the scroll bar itself to have the bar jump to that location.

Enterprise Manager: HP Live Network Announcements dashboard pane fails when HP Passport requires update

PROBLEM:	HP Passport credentials are not current for HP LiveNetwork Announcements widget.
CAUSE:	Credentials for a 7.2 or 7.5 HP Passport require update for 7.8.
WORKAROUND:	1. Visit HP BSA Essentials Network web site (https://www.www2.hp.com/) and complete the one time confirmation step before using the HP Live Network announcements widget. 2. If continue to see a connection failure for the HP Live Network Announcements widget, visit the HP Live Network RSS Feed : https://h20033.www2.hp.com/servlets/WebFeed?artifact=news&version=rss_2.0&cookieCheck=off, Complete the one-time confirmation step if you are asked for it.

Enterprise Manager: HP Live Network Announcements dashboard pane fails when SSL enabled

PROBLEM:	When you enable SSL in an HPCA Enterprise classic installation, the HP Live Network Announcements (RSS feed) dashboard pane throws an exception during the initial SSL handshake. This message which appears when you mouse over the red “RSS query failed” text, and it indicates that the “PKIX Path Building failed.”
CAUSE:	The SSL handshake fails to properly exchange certificates during the connection initiation. The certificate provided by the HP Live Network RSS feed is not accepted as legitimate by the HP Client Automation Enterprise Manager service, which has initiated the conversation.
WORKAROUND:	The HP Live Network Announcements (RSS feed) dashboard pane will not work in an HPCA Enterprise classic installation when SSL is enabled. Either move to an HPCA Core and Satellite installation, or access the RSS feed outside of the Enterprise Manager UI by using a browser.

Enterprise Manager: 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:	HPCA agent and OS Deployment jobs can only be deleted via an aging mechanism. 1. Open `ManagementPortal_InstallDir/etc/rmp.cfg.` 2. Add or change the following parameter to indicate the job history in days to keep: **`JOBHISTORYTTLDAYS 30`** 3. Save the file. 4. Restart HPCA Portal service. The default location of the `rmp.cfg` file is: Core server: `c:\Program Files\Hewlett-Packard\HPCA\ManagementPortal\etc` HPCA Legacy: `c:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc`

Enterprise Manager: Errors are present in the <*InstallDir*>/CM-EC/tomcat/logs/ope.log file

PROBLEM:	Many errors and stack traces are displayed in the `ope.log` file
	`ERROR GraphElement : action threw exception: Connection to host timed out: <hostname>`
	`ERROR GraphElement : action threw exception: Could not resolve host: <hostname>`
	`ERROR GraphElement : action threw exception: Connection to client has been dropped`
	`ERROR JobExecutorThread : exception in job executor thread. waiting 5000 milliseconds`
	`ERROR DbPersistenceService : hibernate commit failed`
	`ERROR Services : problem closing service 'persistence'`
	`ERROR JDBCExceptionReporter : Deadlock found when trying to get lock; try restarting transaction`

CAUSE:	Various processes generate errors in the log file to indicate a potential problem.
WORKAROUND:	No workaround. These errors can be safely ignored.

Enterprise Manager: 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 `sectools-director.log` 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.

Enterprise Manager: 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).

Enterprise Manager: Job timing settings in the Console.properties file are ignored

PROBLEM:	The following job timing settings are included in the `<`*`InstallDir`*`>\CM-EC\webapps\em\WEB-INF\Console.properties` file:
	`group.processing.threads`
	`group.processing.target.delay.ms`
	The Enterprise Manager, however, displays default values for these settings based on the Device Notification Type when a job is created. It does not use the settings in this file. This can be confusing.

CAUSE:	Enterprise Manager chooses default values based on the notification type.
WORKAROUND:	No workaround available.

Enterprise Manager: Installer Repair does not repair services or database

PROBLEM:	The installer **Repair** option does not fix all installation and set-up issues with Enterprise Manager. Specifically, the repair option does not fix issues with the HP Client Automation Enterprise Manager service, the operational process engine database, or java security settings.
CAUSE:	The repair operation only reinstalls files into the default installation location. No configuration (post-install) actions are performed.
WORKAROUND:	1. Make a copy of the following file: `<install-dir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties` Place this copy outside of the `<install-dir>` directory. 2. Uninstall the Enterprise Manager. 3. Install the Enterprise Manager. 4. Stop the “HP Client Automation Enterprise Manager” service by using the Services utility. 5. Restore the following file from the copy that you made in step 1: `<install-dir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties` 6. Start the “HP Client Automation Enterprise Manager” service. NOTE: If the `Console.properties` file does not exist in step 1 – or if you believe that the file is corrupt – only steps 2 and 3 are required. The Enterprise Manager must be reconfigured after step 3.

Enterprise Manager: 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 Enterprise Manager is not returning the appropriate status code when a restart request fails.
WORKAROUND:	Check the refreshed status on the details page, or the Directory Service list to see the actual status.

Enterprise Manager: Migration from 5.x to 7.20 does not set URLs correctly

PROBLEM:	The URLs for Operational Process Engine (OPE) and the Vulnerability Management Server (internal components used by the Enterprise Manager) are not set correctly in the `Console.properties` file when you migrate from HP CM 5.x to HPCA 7.20.
CAUSE:	If you have disabled the non-SSL HTTP port connector in the `server.xml` file according to the “Disabling Non-SSL Access” procedure in the *HP Client Automation SSL Implementation Guide*, you must ensure that the following things are true: The `Console.properties` file specifies the opeurl and vulnerability_management_server_url settings. The opeurl and vulnerability_management_server_url settings point to the port used for SSL communication with the Enterprise Manager.
WORKAROUND:	Specify the correct ports and protocol for SSL communication after the upgrade, as described in the *HP Client Automation Enterprise Manager Migration Guide*.

Enterprise Manager: Deleting a virtual device does not delete that device from the Devices list

PROBLEM:	The Delete operation fails when you attempt to delete a Virtual Machine that is running.
CAUSE:	The Delete Virtual Machine operation does not delete the device from the All Devices container in the HPCA Portal.
WORKAROUND:	Manually delete the device from the HPCA-CS Devices category.

Enterprise Manager: A VM image must be shut down before it can be deleted

PROBLEM:	The Delete operation fails when you attempt to delete a Virtual Machine that is running.
CAUSE:	VMware ESX Server requires virtual machines to be powered off before you can delete them.
WORKAROUND:	Power off the Virtual Machine using the Power Off action. You can delete the Virtual Machine once it is successfully turned off.

Enterprise Manager: Unable to connect via SSL on Microsoft Windows 2003 server

PROBLEM:	An expired certificate in `cert_mgr` causes Win2003 server to fail when Enterprise Manager communicates with the Portal via HTTPS. If you used the HP CM version 5.0 `cert_mgr` tool to generate a certificate, you will experience this problem when you try to access the Portal. If you remove the `Console.properties` file and try to configure HTTPS, the connection will fail. If you use an existing `Console.properties` file, an error will occur while loading directories.
CAUSE:	An expired certificate authority used by `cert_mgr` to generate keys is no longer valid. Windows 2003 rejects expired certificate chains while establishing HTTPS communication.
WORKAROUND:	Regenerate your certificates using the latest version of `cert_mgr` after migration.

Enterprise Manager: 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.

Enterprise Manager: Vulnerability Management data acquisition using the HP Live Network Connector (LNc) reported as successful even if the acquisition fails due to invalid login credentials

PROBLEM:	If the HP Live Network Connector (LNc) is executed on a Windows 2000 platform, and invalid login credentials for the HP Live Network content site are provided, the results of the acquisition will be displayed as Successful in the Vulnerability Management Acquisition Report even though HPCA was unable to connect to HP Live Network. The Vulnerability Management Acquisition report shows the acquisition as being Successful, but no vulnerability data is loaded into the databases or displayed in the reports. Additionally, the Vulnerability Management Server (VMS) and HP Live Network Connector log files display an error message indicating that the credentials failed. No error messages detailing the number of vulnerabilities that were downloaded are present in the log file, however.
CAUSE:	LNc does not return an error code if the login fails.
WORKAROUND:	Be sure to provide the correct HP Live Network User ID and Password when you configure the Live Network settings. In the following log files, verify that the vulnerability data was, in fact, downloaded: CAE: `<`*`InstallDir`*`>\VulnerabilityServer\logs\vms-server.log` Core and Satellite: `<`*`InstallDir`*`>\HPCA\VulnerabilityServer\logs\vms-server.log` Both: `<`*`LNc-InstallDir`*`>\lnc\log\live-network-connector.log`

Enterprise Manager: 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 Enterprise Manager 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. The Enterprise Manager has no visibility to the additional members.
WORKAROUND:	Use the Console's Search Parameters to fine tune and narrow your search.

Enterprise Manager: Security Tools Management and Compliance Management dashboard panes may display the incorrect time zone in non-English locales

PROBLEM:	In many non-English locales, the time that is displayed in the Compliance Management and Security Management dashboard panes will be displayed using Greenwich Mean Time (GMT) instead of the local time zone. There is no indicator that the time is being displayed in GMT.
CAUSE:	Time is displayed in GMT and not the local time zone.
WORKAROUND:	None

Enterprise Manager: Dashboard panes may stop responding

PROBLEM:	The dashboard panes may stop responding to requests for updates and refresh. Additionally, toolbar buttons in the dashboard panes may appear to be overlapping.
CAUSE:	A null pointer exception is being processed in the underlying Adobe Flex code.
WORKAROUND:	Log out of the console, and then log back in. Future downloads of Adobe Flex may resolve this problem.

Enterprise Manager: 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.

Enterprise Manager: Migration from 5.11: Installer indicates upgrade status inconsistently

PROBLEM:	When you upgrade from HP Configuration Management version 5.11 to HPCA version 7.20, the status reported during the upgrade sometimes says “install” and sometimes says “upgrade.” This is confusing.
CAUSE:	The Enterprise Manager installer package name changed between version 5.11 and 7.20.
WORKAROUND:	None. The upgrade works correctly. Only the status reporting during the upgrade is affected.

Enterprise Manager: Migration from 5.1x to 7.20 does not preserve job history

PROBLEM:	Past job history is no longer available after migrating to HPCA version 7.20.
CAUSE:	The database used by the job process engine has been changed from HSQLDB in version 5.1x to MySQL in version 7.20. This change was made to increase the stability and performance of the job process engine.
WORKAROUND:	No workaround is available.

Enterprise Manager: Device Import Wizard does not refresh tables after it commits an import

PROBLEM:	The Device Import Wizard does not automatically refresh the navigation tree for the **Device Categories → VM Services → ESX Server** after the device is imported.
CAUSE:	The Children table for the Devices container is the only area that gets automatically refreshed when the Device Import Wizard is completed.
WORKAROUND:	Click **Refresh** on the Children table for **Device Categories → VM Services → ESX Server** to ensure that the current tree is up-to-date after the Device Import Wizard is used.

Enterprise Manager: Enterprise Manager may run slowly

PROBLEM:	Requests from the Enterprise Manager client (console) to the Enterprise Manager server (an internal component) may take a long time to return under certain circumstances.
CAUSE:	By default, the maximum number of concurrent connections allowed by Internet Explorer and Firefox is set to two.
WORKAROUND:	For Internet Explorer: Edit the following registry key: `My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\InternetSettings` Add the following DWORD Value: `MaxConnectionsPerServer` with a Value of 8 (recommended). For Firefox: Edit the Firefox configuration page (type about:config in the browser window). Change the value for `network.http.max-persistent-connections-per-server` from 2 (default) to 8 (recommended).

Enterprise Manager: Enterprise Manager does not support current object substitution syntax for attribute names

PROBLEM:	The Portal, Policy Manager, and Enterprise Manager do not support current object substitution for attribute names for extended attributes defined for policy entitlement. This syntax has never been supported. The following are examples of supported Policy Entitlement syntax.
	`+SOFTWARE/ZSERVICE < version = 1>`
	`+SOFTWARE/ZSERVICE < version=<<in.version>> >`
	`+SOFTWARE/ZSERVICE < version = 1> ; <<in.os>> == "XP"`
	`Not supported syntax:`
	`+SOFTWARE/ZSERVICE < <<in.version>> = 123 >`

CAUSE:	This syntax has never been supported.
WORKAROUND:	If this syntax is mistakenly applied to Policy Entitlement, the instance can be edited using the Portal.

Enterprise Manager: The Vulnerability Management Server cannot connect to SQL Server

PROBLEM:	The `vms-server.log` or `vms-commandline.log` file displays a message with a `com.microsoft.sqlserver.jdbc.SQLServerException` and various informational messages about not being able to connect to SQL Server.
CAUSE:	The Vulnerability Management Server configuration requires the specification of the Reporting database server, port, database name, user name, and password. There can be numerous reasons why the Vulnerability Management Server is not able to connect. The most likely fixes are listed below.
WORKAROUND:	In SQL Server, the default static port is 1433. However, it is possible that the SQL Server installation is set up with a different static port or with a dynamic (non-specified port). Verify your SQL Server port settings, and update the SQL Server port information in the following places: Core and Satellite installation: Configuration > Infrastructure Management > Database Settings Traditional installation: Configuration > Live Network > Databases tab For an HPCA Core installation, you must use a static port. For a traditional (component-based) HPCA installation, you may use a static port or a dynamic port. The following pertains only to a traditional (component-based) HPCA installation: On the Configuration > Live Network page, verify the following settings on the Databases tab: The **Database Server** should be the hostname where the database resides. For example: mydbserver.mycompany.com If the SQL server setup is using something other than the default database instance, the instance needs to be appended to the server name. For example: mydbserver.mycompany.com\HPCA The **Database Name** field requires that you enter the specific database name in that instance. Check your authentication settings in SQL Server. If you are using Windows authentication, try to use SQL Server authentication, and then update the Reporting Database Configuration appropriately. If SQL Server is using a dynamic port, be sure that the **Port** field in the Reporting Database Configuration section is blank.

Enterprise Manager: Unable to connect via SSL on Microsoft Windows 2003 server

PROBLEM:	An expired certificate in `cert_mgr` causes Win2003 server to fail when Enterprise Manager communicates with the Portal via HTTPS. If you used the HP CM version 5.0 `cert_mgr` tool to generate a certificate, you will experience this problem when you try to access the Portal. If you remove the `Console.properties` file and try to configure HTTPS, the connection will fail. If you use an existing `Console.properties` file, an error will occur while loading directories.
CAUSE:	An expired certificate authority used by `cert_mgr` to generate keys is no longer valid. Windows 2003 rejects expired certificate chains while establishing HTTPS communication.
WORKAROUND:	Regenerate your certificates using the latest version of `cert_mgr` after migration.

Enterprise Manager: Browser gets stuck at 80%

PROBLEM:	When upgrading a system running SSL communications to the Portal the browser gets stuck at 80%.

CAUSE:	The following files are over-written during the installation:
	`<`*`InstallDir`*`>/nonOV/jre/b/lib/security/cm-ec.keystore`
	`<`*`InstallDir`*`>/nonOV/jre/b/lib/cm-ec.truststore`

WORKAROUND:	Replace the two files that have been over-written with the correct versions for the server. These files would have been generated as described in the *HP Configuration Management SSL Implementation Guide.*

Infrastructure: When Agent or OS Deployment is Scheduled, the target is 0

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.
CAUSE:	Unknown.
WORKAROUND:	

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:	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: 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 *Application and Application Self-service Manager Guide.*

OS Manager for Windows: Configuration Server Installed on Solaris – additional steps required for OS Management

PROBLEM:	OS Management does not work correctly with a Configuration Server installed on Solaris.
CAUSE	Not known
WORKAROUND:	1. Correct the value of PORTAL_ZONE in the [MGR_ROM] section of edmprof. If you had entered the ZONE value during install as “hp” the PORTAL_ZONE will be set as “hp”. Change the PORTAL_ZONE to “cn=hp,cn=radia”. This value should match with the value in the etc\rmp.cfg found under the HPCA Portal install location. 2 - Copy the required missing modules from a Windows Radia Configuration Server’s `management_infrastructure\configuration_server\win32\media\modules\` folder to the Solaris `<RCS installdir>/modules` directory.

OS Manager 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 Manager 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:	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." 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.
WORKAROUND:	Follow the steps below to successfully capture an image running FBWF. 1. Disable FBWF (Reboot). To disable FBWF, go to the DOS prompt from Windows and enter the following command: fbwfmgr /disable and reboot. 2. Manually install XPE agent. 3. Copy Etprep to \Windows and FBReseal to \Windows\FBA directory. 4. Begin executing prepwiz.exe as normal. When this captured image is used to deploy to other target units, the FBWF will be in its normal "ENABLED" state.

OS Manager for Windows: Can't 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 Manager for Windows: 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 Manager 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 Manager for Windows: No prompt info during image uploading, if OSM is down

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

OS Manager for Windows: WinCE: Job turn successful when replied NO to OS prompt

PROBLEM:	When user has chosen not to deploy OS when prompted on WinCE, OS deployment job on the Enterprise Console shows success.
CAUSE:	WinCE is not returning a correct return code to notify that job was canceled.
WORKAROUND:	None

OS Manager for Windows: Image Preparation Wizard 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. In a CAE Classic environment, the upload fails and the OSM server will fail to store the resulting image files. The partial files will stay locked until the OSM server is restarted.
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. If you experience locked image files in the \upload folder of the OSM server and you are running CAE Classic, then you must restart the OSM server to unlock the files so they may be deleted. In a Core/Satellite environment, the locked image files will be unlocked and deleted automatically.

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.

OSManager for Windows: Migrating Infrastructure components from 4.2, OS Manager connect fails

PROBLEM:	When migrating CM infrastructure components from 4.2 to 7.8, the 4.2 agent is unable to perform an OS Manager connect and it will fail.
CAUSE:	Migration/backward incompatibility between CM infrastructure 7.8 and CM agent 4.2 OSM client method.
WORKAROUND:	Migrate agent to version 7.8 and then perform an OS Manager connect.

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” 1 Click Start 2. Select Settings -> Control Panel 3. Click the System Icon 4. 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:	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 agent 3. Do not provide multiple versions of the HPCA agent MSI file in the same media directory.

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 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. 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."
CAUSE:	
WORKAROUND:	Disable the creation of the System partition – install Windows 7 into a single partition. Set the SYSPSPCE attribute in the OS.DISKMAP class to 0. For further information please refer to “Allocating Disk Space for Partitions” in the *HPCA OS Manager System Administrator User Guide*. For customers relying on Windows Setup deployment, HPCA will provide a hot fix promptly after the product release.

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:	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 `conhost.exe` can pop up. This is most likely to happen if ALT+TAB is hit early in the initialization phase of SOS WinPE. Pressing "OK" on the message window allows the process to continue. The deployment process is not affected.
CAUSE:	This is a known issue with the new Windows 7 system service `conhost` that gets started to handle console window output.
WORKAROUND:	Do not press ALT+TAB during the deployment.

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:	Remove the Product Key from this section of unattend.xml: <settings pass="windowsPE"> <component name="Microsoft-Windows-Setup"> <UserData> <ProductKey> <Key> Example: <UserData> <AcceptEula>true</AcceptEula> <ProductKey> <Key></Key> <WillShowUI>OnError</WillShowUI> </ProductKey> </UserData> Add the Product Key to the following section: <settings pass="specialize"> <component name="Microsoft-Windows-Shell-Setup"> Example: <ProductKey>AAAAA-BBBBB-CCCCC-DDDDD-EEEEE</ProductKey> (replace AAAAA-BBBBB-CCCCC-DDDDD-EEEEE with your Product Key) Full details on placing Product Keys in unattended answer files can be found in the Windows Automated Installation Kit documentation on unattended Windows installations.

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 `tclfsredirect.dll` fails to load because of missing Microsoft Visual C++ 2005 runtime redistributable files.
WORKAROUND:	Download this package from Microsoft at the following URL: http://www.microsoft.com/downloads/details.aspx?familyid=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en 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.

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:	Option 1: Use the ImageX deployment type through the Image Preparation Wizard. Do not use the Windows Native Install Packager.
	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.
	Follow these steps:
	a. Navigate to the drive that you selected during the WNI Publisher.
	b. Edit `<drive>:\$WIN_NT$.~BT\WINNT.SIF`
	c. Search for `radsetup`
	d. On the line containing `radsetup`, replace the first double quote (`“`) with the string `command0=“C:`
	For example, change:
	`“\Program Files\Hewlett-Packard\HPCA\Agent\RADsetup\RAMINSTALL.CMD"`
	To:
	`command0="C:\Program Files\Hewlett-Packard\HPCA\Agent\RADsetup\RAMINSTALL.CMD"`

Patch Manager: 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 Manager: 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 Manager: 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 Manager: 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 Manager: 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 Manager: HPCA Patch Manager Service on the Core Server fails to start under certain conditions

PROBLEM:	The HPCA Patch Manager Server Service fails to start when the following operations occur simultaneously: 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: 1.1 Network issue 1.2 Web Proxy issue 1.3 Vendor site maintenance 2. During the above situation, the service for the HPCA Patch Manager Server is restarted due to one of the following reasons: 2.1 A user updates any of the Configuration settings for Patch Management from the Core Console. 2.2 A user manually restarts the service from the Windows Service Management Console.
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 `patchgw.mk,` 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 `patchgw.mk` file under [*`HPCA CORE Install Directory`*]`\Patch Manager\etc\patch` and restart the HPCA Patch Manager Server Service.

Patch Manager: 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 Manager: Portal installed on Core: 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.

Patch Manager: 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 Manager: 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 Reporting Server 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.

Patch Manager: 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 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.

Portal: Self-maintenance fails to upgrade a Portal Agent (RMA) installed into a path containing spaces

PROBLEM:	When migrating the Portal to version 7.20, the self-maintenance feature cannot be used to upgrade the Portal Agents if the Portal Agents were installed into a path containing spaces, such as C:\Program Files\Hewlett-Packard\CM\ManagementAgent.
CAUSE:	The self-maintenance feature requires a fix to support the upgrade of Portal Agents whose installation path contains spaces.
WORKAROUND:	Check the HP Software Support Online website for a downloadable software patch for the Portal self-maintenance feature. Or Use the Install Portal Agent task from the Portal console to deploy the latest version of the Portal Agent to all of the devices in your Zone.

Portal: Portal from Version 2.1 fails to migrate edmpolicy attributes

PROBLEM:	Migration of RMP Version 2.1 to Version 7.5 can cause edmpolicy attributes to be lost after the migration.
CAUSE:	The edmpolicy attribute is not migrated from 2.1 (metakit) causing device policies to be lost. HP has identified a fix that was applied to the 7.2 migration script that now needs to be applied to the 7.5 migration script (rmp_migrate.tkd).
WORKAROUND:	Until HP makes a fix available for the 7.5 rmp_migrate.tkd, the workaround is to first migrate the 2.1 Portal data to 7.2, then migrate the 7.2 Portal data to 7.5.

Portal: No job executions are shown in Enterprise Manager Console target view when Network Discovery is enabled in the Portal

PROBLEM:	When a Portal has Network Discovery enabled, no job executions are shown from the Enterprise Manager Console Target drill down view.
CAUSE:	A certain field is null for the Portal Network Discovery job, which causes an exception when job executions are displayed.
WORKAROUND:	Drill down from the individual job to see the job executions. or Turn off Network Discovery when installing or after installing the Portal. For details, refer to the *Portal Installation an Configuration Guide*. Note that turning off Network Discovery has no impact on Portal functionality.

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 [MULTCAST] in  [/opt/HP/CM/IntegrationServer/etc/rps/]` When this occurs, the MULTCAST 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 is 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.

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 Manager: Non CM Usage Agent un-installation throws 'Files in use' error dialog

PROBLEM:	In Non-CM, during the AUM agent uninstall process, the wizard throws the 'Files in use' dialog error on Windows 7 OS systems.
CAUSE:	AUMStatus services are running in the task manager.
WORKAROUND:	Click the Ignore option during AUM Agent uninstall. The uninstall process will complete successfully.

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 media.

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