HP Client Automation Enterprise

Software Version: 8.10

Release Notes

Document Release Date: April 2012

Software Release Date: February 2012

Legal Notices

Warranty

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.

Restricted Rights Legend

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.

For information about open source license agreements, see the *License* directory on the product installation media.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

Oracle is registered trademark of Oracle Corporation and/or its affiliates.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Documentation Updates

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and log on. To register for an HP Passport ID, go to:

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

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

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

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

HP Software online 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 web 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 register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Client Automation Release Notes

This document is an overview of the changes made to Client Automation (HPCA). It contains important information that is not included in books or Help.

Note: HP Client Automation version 8.10 is the next minor release following the version 7.90. There is no HPCA 8.00 major version.

You can find information about the following in this document:

What's New in This Release?

The HP Client Automation Enterprise Edition contains new features, feature enhancements, and other changes.

- **Role-based access control**
  Enhanced access control framework that provides granular access control level for performing administrative tasks in Client Automation. You can distribute administrative tasks by creating roles with appropriate capabilities, and then assigning these roles to users and groups. You can also leverage external directories (such as LDAP and Active Directory) to add users and groups, and configure their access control levels.
- **Satellite management**
  Client Automation now provides simplified and streamlined Satellite server administration. You can manage and deploy a Satellite, assign Satellite to Server Pools and Locations from the HPCA Console. The Server Pools enable you to load balance the client connections on the Satellite servers.
- **Enhanced internal resource caching**
  An improved feature to preload the resources (data files) available on the upstream server cache to the Proxy Server static cache on the Satellite. The Tcl-based Proxy Server is used as the proxy cache service instead of the Apache server, and enables static and dynamic cache support based on the Configuration Server resolution process. You can preload the static cache with all the entitled resources during off hours so that the required resources are available when requested by an HPCA agent. The Proxy Server desired state can be configured to include the

required resources. Using the Proxy Server dynamic caching, the resources are cached on the Satellite server when they are requested by the agents.

- **Software and patch policy resolution available when the Core is down**
  The dependency on the Core server is reduced, ensuring continuity in Core server functionality and the data services. The policy resolution for software and patches is available even if the Core server is unavailable.
- **Monitoring CA infrastructure**
  HPCA now provides the SiteScope solution template that includes a pre-configured set of monitors that you can deploy to monitor multiple aspects of HPCA components in the infrastructure. This solution performs proactive and periodic tests, enabling administrators to ensure the availability of components across the enterprise. The documentation lists the HPCA services and parameters that you should monitor if you plan to integrate another monitoring solution in your HPCA environment.
- **Microsoft App-V support**
  HPCA 8.10 extends the support for application virtualization to include Microsoft Application Virtualization (Microsoft App-V) based virtual applications. You can now publish, deploy, and upgrade Microsoft App-V applications in your HPCA environment.
- **Patch Manager Gateway preload on Satellite**
  In the Metadata Patch Management model, the synchronization with upstream server preloads the patch binaries from Core Patch Manager Gateway cache to the Satellite cache. This ensures that the patch binaries are distributed to the agents even when the Core server is not reachable. You can use this feature to preload the Satellite with the tested patch binaries from the Core, scheduled overnight.
- **OS Management**
  - **Enhanced thin client provisioning**
    The thin client provisioning now eliminates the requirement for having the Microsoft utilities etprep and fbreseal in the image before capturing the image.
  - **Enhanced Configuration Server resolution**
    OS Manager Server performs full Configuration Server resolution when acquiring SAP objects to resolve any symbolic substitution defined in the metadata.
  - A new progress bar has been added for uploading (capture) and downloading (deployment) of images when using WinPE. The progress bar shows the number of bytes transferred, bytes remaining, and the current speed of the transfer.
  - Support for Microsoft Windows Embedded Standard 7 (WES7) on HP thin clients.
  - Upgrade to Windows PE 3.1 (Available as a supplement over Windows Automated Installation Kit (Windows AIK 3.0).
  - Support for hard drives greater than one TB. Support for Advanced Format Drives (AFD). These are supported through Windows PE 3.1 released as part of Windows Automated Installation Kit (Windows AIK 3.0) supplement for Windows 7 Service Pack 1 (SP1).
  - Support for provisioning 64-bit Microsoft Windows 7 using Winsetup
- **Agent**
  - **Reboot Deferral Facility (RDF)**
    A new Reboot Deferral Facility has been added that enables you to defer a required reboot to

a more convenient time. It allows the administrator to configure the maximum number of days allowed to defer and/or the maximum number of times a user can cancel the reboot before being required to reboot the device.

- **Enhanced Connect Deferral Facility (CDF)**
  Various enhancements has been made to the CDF, such as you can assign display names for custom domains, use of Catalog expressions (CATEXP) on command line, show only master service for service groups, and support agent lockdown mode, and include previously failed installations in action list.
- **WinHTTP as a new protocol**
  WinHTTP has been added as additional HTTP protocol to facilitate the use of Branch Cache.
- **Enhanced processing of Patch Management objects**
  Processing of Patch Management objects in the outbox now reduces any redundancy in the data being sent up to the HPCA Core Server and minimizes the bandwidth needed for the data transfer.
- Command line arguments `MNAME`, `DNAME`, and `STARTDIR` have been added to the Synopsis object to better track the type of connect performed.
- Drag and drop notify in the CSDB Editor has been removed as notify is performed through the HPCA Console.
- The UNDO operation has been removed from Application Self-Service Manager.

- Removed Radia Extensions for Windows Installer (REfWI) that was used by administrators to manage Windows Installer packages for multiple users of a machine.
- Removed Configuration Analyzer used to view, store, and compare patches and application data.

Client Automation Support Matrix

You can find the Support Matrix for this product that lists all software and hardware requirements at this location: HP Support matrices. For information about the backward compatibility of some components of the HPCA 8.10 release with previously released versions of the product, refer to the HPCA Support Matrix.

Note: Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to Access levels.

To register for an HP Passport ID, go to HP Passport Registration.

Migration and Upgrade

HPCA version 8.10 includes only the Core-Satellite installation model and does not include the Classic configuration. Based on your current configuration, you can migrate to HPCA 8.10 using the procedures listed in one of the following guides:

- **Classic to Core-Satellite Migration**: You can migrate from the HPCA Classic model to the Core-Satellite model. HP recommends that customers employ the HP Professional Services organization to assist with this migration. For more information on migrating from the Classic to the Core and Satellite model, see the *HP Client Automation Enterprise Migration Planning and Best Practices Guide* at the HP Live Network URL, https://www.www2.hp.com/. The migration

scripts include improved RDBMS data migration processes that increase the data migration performance when migrating from Classic model to the Core-Satellite model.

- **Core-Satellite to Core-Satellite Migration**: For more information on migration from the previous HPCA version with Core-Satellite model to the latest HPCA 8.10, see the *HP Client Automation Enterprise Migration Guide* that is available on the distribution media under `Documentation\HPCA Enterprise\Migration Guides` directory.

Installation Requirements

You can find requirements and steps to install Client Automation in the *HP Client Automation Enterprise Edition Getting Started and Concepts Guide* on the product installation media at the following location:

`\Documentation\HPCA Enterprise\CoreSat_GSG_Concepts.pdf`

Note: 8.3 file names must not be disabled on Windows systems in your HPCA environment for HPCA to function properly.

After installation, the *HP Client Automation Enterprise Edition Getting Started and Concepts Guide* is available at the following URL:

`http://HPCA_Host:3466/docs`

where, *HPCA_Host* is the name of the server where HPCA server is installed.

Hardware and Software Requirements

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

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

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

In addition, HP Software support for operating systems no longer supported by the original operating system vendors (custom support agreements 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.

Fixed Defects

The section lists the defects fixed in this release. This list may apply to HPCA Standard, HPCA Enterprise, or both. Some of the items may not pertain to your particular implementation of HPCA. For more information about fixed defects, visit HP Software Support Online, or contact your HP Support representative directly.

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

PROBLEM:	Not all of the startup timers that are configured to execute once when the system is rebooted are actually processed upon reboot.
CAUSE:	This issue can occur when multiple startup timers are configured on an agent machine to execute once when the system is rebooted. However, timers that are not processed initially are eventually processed in subsequent reboots. This is not desirable. All startup timers that are configured to execute once should be processed upon reboot.

Application Manager Agent: Unable to install application on Agent when NATVHTTP enabled for win7 and vista 64 bit OS

PROBLEM:	Unable to install an application on Agent when NATVHTTP is enabled for Windows 7 and Windows Vista 64- bit OS.
CAUSE:	The memory allocation for the relativeURL buffer in the hpcahttp.c file causes the problem.

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

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

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.

Core: Quick Search does not apply filter when using Firefox

PROBLEM:	When using the home page Quick Search feature on Firefox, the value you enter does not get applied properly making quick search unusable.
CAUSE:	Defect in code.

Core and Satellite: An LDAP 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.

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.

Core and Satellite: Service list does not refresh automatically

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

Core and Satellite: Virtual Management Reporting View is not localized

PROBLEM:	The Virtualization Management report view always appears in English regardless of locale.
CAUSE:	The localized message file is missing.

OOBM on Core: Automatic synchronization feature does not work

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

OOBM on Core: OOB detailed online help is not localized

PROBLEM:	OOBM detailed online help pages are not localized. Online help will be displayed in

	English even in non-English locales.
CAUSE:	OOBM online help is hardcoded to use English online help.

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

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

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

PROBLEM:	In some cases, OOBM detailed online help pages do not show the correct help context section.
CAUSE:	Some of the OOBM detailed online help pages are not linked correctly.

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

PROBLEM:	Microsoft bulletins previously published to the CSDB (not using Metadata) are deleted if they are re-acquired using Metadata.
CAUSE:	There is an issue in the MSFT Acquisition which is wiping out the published bulletins from the CSDB.

Patch Management: Export URL Requests will not list the URLs which encountered an error during download

PROBLEM:	For a Patch Gateway with Internet access, the Export URL Requests feature will not list the URL requests that encountered an error when downloading.
CAUSE:	The Export URL Request will only list the URL requests made when the INTERNET option is set to N in patch.cfg. Export URL Request is meant only for an environment where the Internet is not made available to the server hosting the primary Patch Gateway. The Export URL Request list (of unfulfilled URLs) that is created a Gateway without internet access can be downloaded after using Import URL Requests on another Gateway server that has Internet connectivity. Later the downloaded files can be copied back to the gateway folder on the primary Patch Gateway server.

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

PROBLEM:	The patch binary download fails at the patch gateway server at times when smaller files are requested for download. As a result, the bulletin will not be patched during the patch connect.
CAUSE:	When very small binaries are requested a 'state not set' entry is seen in the log file, and an incorrect entry is recorded in the patchgw.mk file. This causes the agent to not deploy the particular bulletin.

Patch Management: Some applicable products for the bulletins are listed under the generic 'Microsoft Products' in the Patch manager Reports

PROBLEM:	Some applicable products for the bulletins are listed under the generic 'Microsoft Products' in the Patch manager Reports.
CAUSE:	When the length of the 'Product String' for a bulletin is greater than 32 characters in length, the product is reported as 'Microsoft Products'.

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

PROBLEM:	Application Usage Count is incremented by one whenever a collection notification is performed through the HPCA Console even though the launched application is not closed.
CAUSE:	The AUM Service is restarted whenever a collection notification is performed through the HPCA Console.

Usage Management: Error occurs when applying Optional Feature utility

PROBLEM:	While applying the Optional Feature utility, an error is encountered during Execution of "Step5_Define Filter Mat Tables and Indexes.sql" which can be found under HPCA\Media\Usage\Optional Features\SQL Server.
CAUSE:	The column name used in the script during creation of index IX_ matvWindowsComputers_4 does not have a space character in it.

Known Problems

The section lists the known problems in this release. This list may apply to HPCA Standard, HPCA Enterprise, or both. Some of the items may not pertain to your particular implementation of HPCA. For more information about open defects, visit HP Software Support Online, or contact your HP Support representative directly.

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

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

Administrator: Lockdown: Installation of HPCA_ADMINTOOLS service revokes the lock from the lib folder in lock down mode.

PROBLEM:	If HPCA Administrator is installed on a system where HPCA Agent is already installed in Lockdown mode, the HPCA_AdminTools service revokes the lock from the LIB folder.
CAUSE:	HPCA Administrator and HPCA Agent are installed on same system. The Lockdown mode is not supported for HPCA Administrator.
WORKAROUND:	HP recommends not to install HPCA Administrator and HPCA Agent on the same system.

Application Self-service Manager: MULTICAST feature has limited functionality.

PROBLEM:	The MULTICAST feature has limited functionality.
CAUSE:	MULTICAST requires all the DATA SAPs to be disabled.
WORKAROUND:	None. The MULTICAST feature has known limitation. Refer documents for more details.

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:	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: Agent migration to 8.1 -- a message box appears and remains on the desktop during the agent migration from 7.80.7 lockdown to 8.1 lockdown

PROBLEM:	During the migration of HPCA Agent from 7.80.7 Lockdown mode to 8.10 Lockdown mode, a message box appears with the following message: radkill : error opening log file
CAUSE:	Code problem
WORKAROUND:	Ignore the message box. It does not impact the migration process. Migration completes successfully.

Application Manager: RIM - Error: could not read object [WBEMCURR] into memory

PROBLEM:	WBEMCURR object is not created when the following Audit services are installed. UNIX_WBEM_COMPUTERSYSTEM UNIX_WBEM_PROCESS UNIX_OPERATINGSYSTEMS
CAUSE:	Design problem
WORKAROUND:	On a Linux 32-bit system, to make Agent Audit services that use WBEM services to work successfully, create a softlink libssl.so.0.0.1 and libcrypto.so.0.0.1 with libssl.so and libcrypto.so respectively. Also make sure that the CIM Server is started before running the Audit services.

Application Manager: Expired certificate in cacert.pem causes ssl-enabled Agent connect to fail.

PROBLEM:	SSL-enabled agent connect fails.
CAUSE:	The expired certificate in the cacert.pem causes the connection failure.
WORKAROUND:	Verify the first public key in the cacert.pem file. It must be a valid key and not expired. If the first public key is expired, replace it with a valid public key which is not expired.

Core and Satellite: CSDB port upstream is non-configurable, DCS sync from satellite fails.

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

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

PROBLEM:	After 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: Reports home page is throwing up error and also the reports are breaking for few other pages

PROBLEM:	If the ORACLE user configured in HPCA has access to multiple other schemas, then home page throws an error – “unable to find the tables”
CAUSE:	Unhandled scenario
WORKAROUND:	Perform the following steps: 1. Add the following property in "..\HPCA\VulnerabilityServer\conf\hibernate-base.cfg": <property name="hibernate.default_ schema">myCustomSchema</property> where myCustomSchema is the name of the schema to qualify the tables with. 2. Restart the Tomcat Server.

Core and Satellite: Satellite synchronization fails from SSL enabled Core

PROBLEM:	Satellite synchronization fails from SSL enabled Core for both Full Service and Streamline Satellites.
CAUSE:	The SSL Certificate of Satellite is not imported to HPCA Core’s JRE Trust store.
WORKAROUND:	To synchronize Satellite from SSL enabled Core, follow these steps: 1. Create the Satellite certificate with FQDN as Server Name (CN).

	2. Export the Satellite certificate as <mycert.cer>, and then save it on Core machine at the following location: <HPCA InstallDir>\jre\lib\security To export the certificate using Internet Explorer, follow these steps: a. Launch the SSL enabled Satellite console. b. Open Satellite console page Properties to launch the Properties window. c. Click Certificates. The Certificate window opens. d. Click the Details Tab. e. Click Copy to File to launch the Certificate Export Wizard, and then click Next. f. Select the Export File Format as DER encoded binary X.509 (.CER) (default selection), and then click Next. g. Enter the complete path and name (for example, mycert) for the file to Export. The suffix for the file indicating its file type (.cer) is automatically generated. h. Click Next and review the settings. To proceed, click Finish. A message displays indicating that the export was successful. i. Click OK. You are returned to the Details tab on the Certificate window. j. Click OK to close the Certificate window. 3. Before importing the certificate into Core's jre, make sure to create a backup of the cacerts file located in the <HPCA InstallDir>\jre\lib\security directory. 4. Run the following commands from the Core machine: cd <HPCA InstallDir>\jre\bin keytool -import -trustcacerts -keystore ..\lib\security\cacerts -storepass changeit -noprompt -alias mycert - file ..\lib\security\<mycert.cer> 5. Restart the HPCA Tomcat service on Core server.

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

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

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

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

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

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

Core and Satellite: The Satellite Server Deployment Wizard shows an additional option **ccm enableds when installing a Satellite in Custom deployment mode

PROBLEM:	The Properties page in the Satellite Server Deployment Wizard displays an additional **ccm.enableds option if you select Custom Satellite deployment mode.
CAUSE:	Code problem
WORKAROUND:	Do not select the **ccm.enableds option in the Properties page of the Satellite Server Deployment Wizard.

Core and Satellite: There is no “Security” service displayed in “Service domain” of” ”Launch Policy Management Wizard(Policy)” on FE/DE/ES/PT/IT locales

PROBLEM:	For supported European locales, the Security domain is not available in the Service Domain list of the Policy Management Wizard.
CAUSE:	Code problem
WORKAROUND:	Complete the following steps: 1. Open the DSN that is configured to the HPCA Core server. 2. In the SQL/Oracle editor, run the following statement: CREATE TABLE dbo.HPCA_Schema (name NVARCHAR (32), version NVARCHAR (32), mtime DATETIME, description NVARCHAR (255), released DATETIME, PRIMARY KEY(name, version)) 3. Restart the HPCA Tomcat Server service. 4. Log out and login again to the HPCA Core Console.

Core and Satellite: For a Streamlined Satellite, if you click Synchronize satellite now from the Satellite Console, the Task Notification dialog box displays Not Running message

PROBLEM:	To synchronize a Streamlined Satellite with a Full-Service Satellite from the Satellite Console, click the Synchronize satellite now option. Although the cache is updated, the Task Notification box intermittently displays the synchronization status as Not Running.
CAUSE:	Unknown
WORKAROUND:	Refresh the Client Automation Satellite Console web page.

OS Management for Windows: Capturing Images using FBWF

PROBLEM:	When working with FBWF (File Based Write Filter), there is no "Commit" state like its counterpart, EWF.
CAUSE:	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 Management for Windows: Window requesting networking option to be used opens

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

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

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

OS Management for Windows: Add partition functionality is not available during LSB deployments using Imagex or Winsetup

PROBLEM:	A partition cannot be added during the LSB deployment. If you try to add partition during deployment, the deployment fails.
CAUSE:	Code problem
WORKAROUND:	Add the partition post deployment using manual method or alternatively use unattend.xml or runonce.cmd to get the partition created during/post deployment.

OS Management for Windows: LSB OS Deployment with SSL Enabled on Core Fails to deploy the OS

PROBLEM:	Enabling SSL using Core console updates URIs of all SAP instances corresponding to Core with TYPE=ROM to use HTTPS as the URI scheme. During an OSM connect, lsb.tkd looks for HTTP as the scheme in the URI attribute of the SAP instances in the Agent LIB directory and if it does not find a SAP instance with HTTP, it does not update the ISVR attribute in ROMBL.CFG with a valid IP address and a port. This causes LSB deployment to fail.
CAUSE:	SAP.URI is updated to use HTTPS scheme instead of HTTP, for SAP.TYPE=ROM server.
WORKAROUND:	Edit the SAP.URI of the SAP instance with SAP.TYPE=ROM and change the URI scheme from HTTPS to HTTP.

OS Management for Windows: Deploy of OS to machine brought under management results in a no-op

PROBLEM:	If a device with a pre-installed OS image is brought under management by installing HPCA Agent, and if an OS migration is triggered through LSB deployment method, the OS installation is not honored. The message "No OS installation required" is displayed on the Service OS splash screen and the machine reboots back to the original installed OS.
CAUSE:	Query to LDAP to retrieve the device and policy information provides incorrect information.
WORKAROUND:	On the HPCA Core server, perform the following steps. **For OS Manager Server**:

	• Stop the OS Manager Service. • Edit the roms.cfg file located under OS Manager Server installation location. The default location is C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\etc\roms.cfg. • Disable LDAP_DIRECT_ENABLED. Set the value to 0. • Start the OS Manager service **For Configuration Server OS Manager components**: • Stop the Configuration Server service. • Edit the edmprof.dat file located under Configuration Server installation location. The default location is C:\Program Files\Hewlett-Packard\HPCA\ConfigurationServer\bin\edmprof.dat. • Disable LDAP_DIRECT_ENABLED. Set the value to 0. This setting is available in the [MGR_ROM] section. • Start the Configuration Server service. **NOTE:** LDAP_DIRECT_ENABLED is enabled by default on the HPCA Core server and disabled by default on the HPCA Satellite server.

OS Management for Windows Thin Clients: Capture of OS image on a thin client with disk size greater than 4 GB is not supported

PROBLEM:	Capturing an OS image on a thin client device with disk size greater than 4 GB is treated as regular legacy capture and the deployment of this image to a thin client fails.
CAUSE:	The tools used to deploy the thin client OS images do not handle spanned files. These spanned files are created if the OS image size is greater than 4 GB
WORKAROUND:	Capture the thin client OS image from a device that has disk size of 4 GB or less. Publish and deploy that image to a device that has higher disk size.

OS Management for Windows: LSB Deployment of Windows 7 over Windows 7 fails if the drive layout is changed for System Reserved Partition

PROBLEM:	If a Windows 7 device does not have a System Reserved partition, you cannot deploy a Windows 7 image with System Reserved partition. Similarly, if the Windows 7 device has a System Reserved partition, you cannot deploy a Windows 7 image without System Reserved partition.
CAUSE:	Drive layout has to be maintained for System Reserved Partition.
WORKAROUND:	Retain the drive layout for System Reserved Partition.

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

PROBLEM:	The Patch Agent Download Manager options for ‘Network Bandwidth’ and ‘Network Utilization in Screensaver mode’ may not work as desired, and may

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

Reporting Server: Links of patch management on "Dashboard" tab can't open when set "Perspectives" to "Mobile" or "Virtual".

PROBLEM:	The Patch Management links on the Dashboard tab in the HPCA Console do not work when "Perspectives" are set to "Mobile" or "Virtual".
CAUSE:	Code problem
WORKAROUND:	Complete the following steps: 1. Create a copy of the DSN that is configured in the HPCA Core console. For example, DSN is configured in HPCA Core console as HPCA_CORE. Create a copy of the DSN with name HPCA_CORE1 that points to same server and database as HPCA_CORE. 2. Use a text editor to edit the rpm.cfg file, located in the etc folder of the Reporting Server directory. 3. Update the parameter DSN with the DSN name that you created in step 1. For example, if the default value for the parameter DSN is "HPCA_CORE", update this value to "HPCA_CORE1". 4. Save and close the rpm.cfg file. 5. Refresh the dashboard reports.

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

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

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

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

Limitations

The section lists the limitations in this release. For more information about open defects, visit HP Software Support Online, or contact your HP Support representative directly.

Application Manager: RIM - Error: could not read object [WBEMCURR] into memory

PROBLEM:	The Agent Audit functionality is not available on a Linux 64-bit system.
CAUSE:	Design problem

Truncation found in the publisher summary package description field.

PROBLEM:	The Package Description entered by users while publishing is not shown complete in the Description field in the Publisher Summary UI.
CAUSE:	UI Display problem. The service gets published to the CSDB without truncating the text in the Package Description field.

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

PROBLEM:	Messages in the vms-server.log file are displayed with an incorrect character set when non-English language browser settings are used. As a result, certain logged database values will be unreadable in non-English locales.
CAUSE:	VMS logs non-English text with incorrect localization settings.

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.

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

PROBLEM:	OOB Group Management functionality fails when it operates in environments with large number of devices.
CAUSE:	Architectural limitation.

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

Security and Compliance:STM (Anti-spyware) Profile is not triggering update definitions with two Anti-spywares on Client machine

PROBLEM:	STM (Anti-spyware) Profile is not triggering update definitions when two Anti-spyware products are installed on client machine.
CAUSE:	When two Anti-spyware products are installed, the Scanner is not able to identify the products to initiate the update definitions.

Usage Management: Delay while trying to see individual links for usage reports

PROBLEM:	Viewing individual links for usage reports is taking more than 10 to 15 minutes.
CAUSE:	As database grows, the time for fetching the individual reports increases.

Documentation Updates

The first page of this document identifies the:

- Version number for the software.
- Software release date.

To check for recent updates or to verify that you are using the most recent edition, visit the HP Software Product Manuals web site.

To retrieve a document, select the:

1. **Product** name.
2. **Version** list.
3. **Operating System**.
4. Preferred **Language**.
5. Document title.
6. Click **Open** or **Download**.

You must have Adobe® Reader installed to view files in PDF format (*.pdf). To download Adobe Reader, go to the Adobe web site.

Documentation Errata

The documentation contains the following incorrect or missing information:

- Consider the following content added to the *Publishing and Deploying OS Images* section in *Appendix G, Capturing Windows XP and Windows Server 2003 OS Images* of the *HP Client Automation Core and Satellite Enterprise Edition User Guide*.
  For legacy Windows XP deployments on Advanced Format Drives (AFD), if the image is already captured, you must modify the .PAR file as shown in sample below and republish the image.

  ```
  Original - /dev/sda1 : start= 63, size= 2762752, Id= 7, bootable

  AF aware - /dev/sda1 : start= 2048, size= 2762752, Id= 7, bootable
  ```

  Note the change in start value 63/2048 and make sure that the .PAR file line endings are preserved.

- Consider the entire section, *Directory Services*, deleted from *Chapter 9, Configuration* of the *HP Client Automation Core and Satellite Enterprise Edition User Guide.*

  Directory Services

  The Directory Services area is available on Satellite Consoles only.The HPCA Directory Services database is a repository of information, such as device and policy data, which are used by various HPCA processes such as OS Management and Policy Services. This database is stored and maintained on the HPCA Core server.

  When Directory Services are enabled on the Satellite, the Directory Services database on the HPCA Core server will be replicated to this Satellite. Client requests to this Satellite that require access to the Directory Services database will be handled locally by this Satellite instead of

being forwarded to the HPCA Core Server. This offers load balancing of client connections and increased fault tolerance, at the expense of replication traffic.

It is recommended that you enable Directory Services on all Full Service Satellites where Configuration and ROMS are both enabled. It is not recommended that you enable this on every Satellite, as it could cause additional and unnecessary network traffic.

NTP Time synchronization between Satellite and Core is required when enabling this feature. Even if different time zones are involved, times must be synchronized. Times will still use local time, but their time difference based on GMT must be synchronized.

- Consider the following content deleted from the *Enable and disable Directory Services on the Satellite* section in *Chapter 2, Installing HPCA* of the *HP Client Automation Enterprise Edition Getting Started and Concepts Guide*.

  Enable and disable Directory Services on the Satellite

- Consider the entire section *Satellite Direct Injection Settings Template* in the topic *Configuring a Full-Service Satellite for SQL Data Injection* updated for the following publications:
  - English and localized online help
  - Localized *HP Client Automation Core and Satellite Enterprise Edition User Guide*

  HP provides a settings template that you can customize and deploy to your Satellite servers to automatically implement the direct injection feature. Complete the following tasks to deploy the Satellite Direct Injection template to the Satellite servers in your environment.

  Task 1: Download the HPCA Satellite Direct Injection template

  a. Log on to the HP Live Network using the following URL: https://www.www2.hp.com/. The HPLN Portal web page opens.

  b. In the Products tab, click **Client Automation**. The Client Automation web page opens that provides the details on the content available on the HP Live Network.

  c. In the Client Automation area, click **CONTENT**.

  d. In the Community column, click **Application Management Profiles for Client Automation**.

  e. In the Application Management Profiles for Client Automation area, click **Content**. The Application Management Profiles for Client Automation - Content area is updated with the list of downloadable items available on the HP Live Network.

  f. Expand **AMPs - HP Contributed**, click **Solutions**, and then click `HPCA Satellite Direct Injection.zip`. The File Download window appears. Save this `zip` file to the location where the HP Live Network Connector downloads content.

  Task 2: Update the HP Live Network content manually

  a. Log on to the HP Client Automation Core Console.

  b. Click **Operations** tab.

  c. Expand **Infrastructure Management** in the left pane, and then click **Live Network**. The Live Network section appears in the right pane.

  d. Click **Update Now** tab.

e. In the HP Live Network Immediate Update area, click **From the File System** and provide the path for the `HPCA Satellite Direct Injection.zip` file that you downloaded and saved in Task 1.

f. Click **Update Now**.

Task 3: Configure the <HPCA Satellite Direct Injection> profile

After you update the HP Live Network, the profile <HPCA Satellite Direct Injection> is available under the Settings Templates. In this template, specify the SQL/Oracle reporting database details where the Satellite servers should directly inject the data.

a. On the Operations tab, expand **Settings Management** in the left navigation pane and click **Settings Templates**.

b. In the Display Name column, click **<HPCA Satellite Direct Injection>** profile. The <HPCA Satellite Direct Injection> window opens with the Profiles and Details tabs.

c. Click **<HPCA SAT DIRECT INJECTION>** to edit the profile properties. The <HPCA SAT DIRECT INJECTION> window opens with the Summary and Properties tabs.

d. Click the **Properties** tab and provide the following details under the Parameters area:
   i. DSN: Enter the DSN for the SQL/Oracle reporting
   ii. User Name: Enter the user name for the DSN
   iii. Password: Enter the password for the ODBC user name

e. Click **Save** to save your changes.

You can deploy this profile on all the Satellites in your environment.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to docfeedback@hp.com.

Product name and version: HP Client Automation, 8.10

Document title: Release Notes

Feedback: