HP Client Automation Enterprise

Software Version: 9.00

Release Notes

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

© Copyright 2008 - 2012 Hewlett-Packard Development Company, L.P.

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).

This product includes software written by Daniel Stenberg (daniel@haxx.se).

This product includes OVAL language maintained by The MITRE Corporation (oval@mitre.org).

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) 9.00. It contains important information that is not included in books or Help.

You can find information about the following in this document:

- What's New in This Release

- Support Matrix

- Migration Notes

- Installation Requirements

- Enhancement Requests

- Fixed Defects

- Known Problems

- Limitations

- Documentation Updates

What's New in This Release?

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

- **Mobile device management**
  You can now manage mobile devices in your enterprise using HPCA. You can publish mobile applications and entitle these applications to mobile devices. You can also perform audits on these mobile devices to collect the latest inventory details. HPCA currently supports Android and iOS-based mobile devices. If you are upgrading to HPCA 9.00, contact HP Support for a new license to access the mobile device management (MDM) feature.

- **Enhanced Role-based access control**
  Enhanced reporting and dashboard capabilities for access control framework that provides more granular access control level for performing administrative tasks in HPCA. You can assign the capabilities of a role to specific targets. Targets determine an OU or a group of managed devices on which users can perform the capabilities assigned to them based on their roles.

- **Full support for Windows 8**
  - Complete management of Windows 8 end-point devices

  - OS migration from Windows XP, Windows Vista, and Windows 7 to Windows 8

  - Preservation of user data and settings during OS migration

- **Support for IPv6 on HPCA Agent**
  HPCA now supports Internet Protocol version 6 (IPv6) for external communication among Core, Satellite, and Agent on Windows systems. The internal communication among these components takes place using IPv4. IPv6 is not supported on Agents on Linux and Macintosh

systems. For more information on HPCA support for IPv6, see the *IPv6 Networking Support* section in the *HP Client Automation Enterprise User Guide.*

- **Managing Internet Devices**
  You can now manage the devices that are outside your corporate network as you would manage the devices over corporate network. The devices are managed according to the policies you set in your environment. You can manage inventory, software deployment, patching, and vulnerabilities for the devices.

- **Enhanced Patch Management**
  Client Automation now enables you to scan the managed devices for any vulnerability for Adobe and Java vendors and remediate the vulnerable devices. The applications that you can remediate are listed on HPCA Console UI under Configuration->Patch Management->Vendor Settings.

- **OS Management**
  - Support for capturing and deploying Microsoft Windows Embedded Standard 7 (WES7) images on HP thin clients.

- Support for Red Hat Enterprise Linux 6.3

- Support for SUSE Linux Enterprise 11

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 9.00 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 9.00 includes only Client Automation Enterprise edition and does not include the Classic configuration. Based on your current configuration, you can migrate to HPCA 9.00 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://hpln.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 9.00, see the *HP Client Automation Enterprise Installation and Upgrade Guide* that is available on the distribution media under `Documentation\HPCA Enterprise` directory.

Localization Details

This release of HP Client Automation is an English only release for server side components, HPCA Core server and HPCA Satellite server. However, the HPCA Agent is available in all supported languages.

Installation Requirements

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

`\Documentation\HPCA Enterprise\HPCA_Installation_Upgrade.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 Installation and Upgrade 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.

Enhancement Requests

This section lists the enhancement requests addressed in this release. For more information about pending enhancement requests, visit HP Software Support Online, or contact your HP Support representative directly.

Administrator Publisher: Publisher cannot publish files > 4.2 GB

PROBLEM:	In HPCA, an Administrator cannot manage resources that are greater than 4.2 GB. For example, using the HPCA Administrator Publisher, an administrator cannot publish files that are greater than 4.2 GB to the CSDB.

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.

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: 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.

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.

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: 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: 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.

Application Manager: In CLIENT.SETTINGS.DEFAULT_SETTINGS REMUNINS is not proper, it shows as "Allow Remote Notify Uninstall [Y/N/".

PROBLEM:	In HPCA CSDB Editor CLIENT.Core Settings(SETTINGS).Default Core Settings class, REMUNINS is described as 'Allow Remote Notify Uninstall [Y/N/' instead of 'Allow Remote Notify Uninstall [Y/N/A]'.
CAUSE:	The maximum number of characters that can be added to the description field are 37.
WORKAROUND:	None. This does not impact any functionality.

Application Self-Service Manager: Application Self-Service Manager does not work on Microsoft Windows Server 2012.

PROBLEM:	The following error appears when you open the Application Self-Service Manager on Microsoft Windows Server 2012.
	
	`The following feature couldn't be installed:`
	
	`.NET Framework 3.5 (Includes .NET 2.0 and 3.0)`

CAUSE:	Code Problem
WORKAROUND:	Create a configuration file named RadUIShell.exe.config with the following contents and save it into the `IDMSYS` folder. ```<?xml version="1.0"?> <configuration> <startup> <supportedRuntime version="v4.0"/> </startup> </configuration>```

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: In the First Time Setup Wizard the Previous button does not work properly in the Mozilla (Firefox) browser

PROBLEM:	User is not able to go to the previous page without providing values in the mandatory fields in First Time Setup Wizard with Mozilla (Firefox) browser.
CAUSE:	Firefox limitation
WORKAROUND:	Provide sample value for the mandatory fields and then click the Previous button.

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. The following error message appears when you synchronize SSL-enabled Core server and full-service or streamlined Satellite server: 'Synchronization Failed"
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).

<table>
<tr><td>

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.

</td></tr>
</table>

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: 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.

Core: Notify Job Last execution time for Mobility connects and Normal Software connects shows 1/1/1970 when the job is scheduled or running

PROBLEM:	Notify Job Last execution time for Mobility connects and Normal Software connects may show 1/1/1970 when the job is scheduled or running.
CAUSE:	The job is in running state.
WORKAROUND:	Wait until the job is complete.

HPCA Console: HTTP error 12030: when logging into HPCA Core Console

PROBLEM:	The following error appears when you login to the HPCA console. HTTP error 12030
CAUSE:	The Tomcat server has not started completely.
WORKAROUND:	Refresh the browser and try to login to the HPCA console again.

HPCA Console: TypeError: Error #1034: Type Coercion failed: cannot convert mx.messaging.messages:: when session expired in console

PROBLEM:	When you click the **Close** button for an expired HPCA Core console session, the following error message appears:

	Error #1034: Type Coercion failed: cannot convert mx.messaging.messages::
CAUSE:	Unknown
WORKAROUND:	Close the browser and login to the HPCA Core Console again.

Core and Satellite: HPCA Console displays an exception when refreshing the subnets list.

PROBLEM:	HPCA Console displays an exception when refreshing the subnets list.
CAUSE:	A SUBNET6 instance has been created using the CSDB Editor.
WORKAROUND:	Create the SUBNET6 instance using the HPCA Console only.

Core and Satellite: HPCA Satellite Console becomes inactive after performing synchronization between HPCA Core and Satellite servers.

PROBLEM:	HPCA Satellite Console becomes inactive after performing synchronization between HPCA Core and Satellite servers.
CAUSE:	This problem occurs if you have installed HPCA Satellite server in the streamlined mode on Windows 8 system and you open the Satellite Console in Internet Explorer version 10.
WORKAROUND:	The synchronization process completes successfully. Click the Operations or Configuration tab on the Satellite Console to make the Console active.

HPCA Core: RBAC: Dashboard and Reporting tabs display exception error when you configure HPCA with two databases and login as RBAC user with patch capabilities.

PROBLEM:	When the Core data and the Patch data (or Usage Data) are stored in a different databases and you log on as user with patch or usage capabilities, the Dashboard and the Reporting tabs show exception error.
CAUSE:	Code Problem
WORKAROUND:	For Microsoft SQL database: Copy the table deviceAdInfo from the Core database to the Patch (or Usage) database. Make sure that the contents of these tables are always synchronized. Use the following schema to create the table: CREATE TABLE deviceAdInfo (device_id nvarchar(50), containerdn nvarchar(255), userdn nvarchar(128),) CREATE UNIQUE INDEX DeviceAdInfoUniqueIndex ON DeviceAdInfo (device_id, containerdn,userdn)

	CREATE INDEX DeviceAdInfoIndex ON DeviceAdInfo (containerdn,userdn)
	For Oracle database:
	If the Core data and the Patch data (or Usage data) are available on the same physical server, grant all access to the Patch (or the Usage) RDBMS database users for the DeviceAdInfo table available in the Core database.

HPCA Core: RBAC: Login as RBAC user who has inventory, mobility and patch role with targets assigned respectively. Inventory report count shows incorrectly.

PROBLEM:	Inventory report on the Reporting tab shows does not show mobile devices when you login as a user with inventory, mobility, and patch roles and respective targets assigned.
CAUSE:	Code Problem
WORKAROUND:	None. Click on link View Managed Devices to view both mobile and non-mobile devices.

HPCA Core: RBAC: Reports are not displayed under the under Management->Services->Reporting tab when a user with patch capabilities logs on to the HPCA Console.

PROBLEM:	Reports are not displayed under the Management->Services->Reporting tab when a user with patch capabilities logs on to the HPCA Console.
CAUSE:	Code Problem
WORKAROUND:	Assign the report.InventoryManagment.all capability to the user to view the reports.

HPCA Core: Clicking on Device Id does not show device details under Push Registration Details Report.

PROBLEM:	When you click the Device Id column for a device in the Reporting View>Mobile Management Reports>Registration Reports>PUSH Registration Detail Report, on the Reporting tab, the device details are not displayed.
CAUSE:	Code Problem
WORKAROUND:	To view the device details: 1. Log on to the HPCA Core Console and click Reporting tab. 2. Click View Managed Devices in the Mobile Management Information. The Managed Devices report opens; you can view the device details in this report.

OS Management for Windows: Capturing Images using FBWF

PROBLEM:	When working with File Based Write Filter (FBWF), no "Commit" state is available.
CAUSE:	Design Problem
WORKAROUND:	Complete the following steps to 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. *For WES 2009 and XPE only*: Copy Etprep to \Windows directory and FBReseal to \Windows\FBA directory. 4. Run the prepwiz.exe file. 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: 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: Agent is not installed in conjunction with Win PE-based OS Installation from Cache partition

PROBLEM:	If you install the operating system using WinPE service OS from the cache partition, HPCA agent does not get installed.
CAUSE:	Design problem
WORKAROUND:	Install the HPCA Agent manually or deploy it through HPCA Core server.

OS Management for Linux: Unix file publisher in -X mode does not process full path to initrd and kernel

PROBLEM:	When you run Unix Publisher in GUI mode, the path provided to vmlinuz (Linux Kernel) and initrd (Initial RAM disk) selections are excluded.
CAUSE:	Code problem

WORKAROUND:	You can resolve this problem by using either of these methods:
	
	• Run the Unix Publisher in text mode.
	
	• If you are publishing using the GUI mode, perform the following steps:
	   ▪ Open the CSDB Editor and navigate to the PRIMARY.OS.UNIXCFG.<INSTANCE_NAME> that was just published.
	
	   ▪ Double-click INITRD and add the path or location of the initrd file on the OS Manager Linux Server.
	
	   ▪ Double-click KERNEL and add the path or location of the vmlinuz file on the OS Manager Linux Server.
	
	Note: The vmlinuz and initrd files are located in the TFTP root location.

OS Management for Windows: Deploying a WES7 flash image will result in a "Window Setup Configuration Error", thus the OS becomes unusable

PROBLEM:	The following error message appears when you deploy a WES7 Build 252 flash image using the legacy method and the OS becomes unusable. `Window Setup Configuration Error`
CAUSE:	Unknown
WORKAROUND:	You can resolve this problem by using either of these steps: • Use the WES 7 Build 233. • Use the ImageX method for WES7 Build 252 devices with the HDD size greater than 4 GB.

OS Management for Windows: Capture error in log file for legacy capture

PROBLEM:	During legacy capture using Linux SOS, several errors are logged in the `<InstallDir>\HPCA\OSManagerServer\Upload\<imagename>.log` file. Sample error message: `Error: main: Background Error: couldn't open "x:/tmp/curl_upload.log": no such file or directory`
CAUSE:	Unknown
WORKAROUND:	None. Ignore the error messages.

OS Management for Windows: WinPE SOS initialization fails if connected to RIS-based OSM

PROBLEM:	WinPE SOS initialization fails when you install OSM server and Boot server on a separate machine than CORE using OSM Media.
CAUSE:	Code Problem
WORKAROUND:	Enable OSM Server and Boot Server on the Satellite server.

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: Reporting Server Error: Invalid column name 'SESSIONID' if the DB collation is "SQL_Latin1_General_CP437_BIN".

PROBLEM:	When creating case sensitive server collation, reporting queries fail.
CAUSE:	HPCA supports case insensitive server collation only.
WORKAROUND:	Change the default server collation to case Insensitive and recreate the HPCA database.

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.

Core and Satellite: iOS MDM server method HTTPS does not send request for the registered iOS device.

PROBLEM:	HPCA does not support HTTPS server method for Satellite server communications between the built-in iOS agent and HPCA agent on an iOS mobile device. You must not modify the default Server Method settings in the Configuration>iOS MDM Settings>Advanced Settings view of the MDM Satellite server in Client Automation Satellite Console. Make sure that you provide the HTTP port only in the Server Port field.
CAUSE:	Code Problem.

Core and Satellite: When multiple users register on the same device, push notification does not trigger any notify jobs for that device.

PROBLEM:	If more than one user is registered on a mobile device, the HPCA server cannot trigger any push notifications for that device.
CAUSE:	Code Problem

Core and Satellite: Mobile user is not able to register again to a different device of same type on iOS platform

PROBLEM:	If mobile user who is already registered with HPCA , registers with the same credentials on another iOS-based device of same type, the device registration fails.
CAUSE:	Code Problem

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

RBAC : Assign internal or external groups as target. Reporting doesn't show any devices.

PROBLEM:	No devices are visible on HPCA Console when internal or external groups are assigned as target.
CAUSE:	Internal and external groups are not supported as targets.

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.

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, 9.00

Document title: Release Notes

Feedback: