# HP Client Automation

## New Features and Release Notes

**Software version**: 7.50 / May 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 a version 7.20 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HPCA agent deployment wizards, and Role-based Access Control, the legacy HPCA Portal *user interface* functionality has been replaced by the HPCA Console.

In a classic HPCA environment, the legacy HPCA Portal *user interface* functionality has been replaced by the Enterprise Manager Console.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 products for the 7.50 release. It contains a bulleted list of new features and functionality for each product, tables that show current software and hardware support for each product, and tables that show backward compatibility of some of the components of this release with previously released versions of HPCA.

# In This Version

- 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.
- **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.
- Many new features were added and consolidated into the Core and Satellite Consoles. For detailed information about Core and Satellite servers, refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide.*
- Software and hardware requirements have changed for many products. See Software and Hardware Requirements on page 5 for details of current support.
- The BSA Essentials 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**.
- Out of Band Management (OOBM) features are now available in the HPCA Console. They allow you to discover, heal, and protect your managed vPro and DASH-enabled devices regardless of their system power or operating system state.

# 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 7.50

The following changes were made to the documentation library for this release.

- Added new user guides for Core and Satellite servers for Windows:
  - *HP Client Automation Core Starter User Guide*
  - *HP Client Automation Core Standard User Guide*
  - *HP Client Automation Core and Satellite Enterprise User Guide*
- Existing information was combined to create a single installation and concepts guide for HPCA Core and Satellite for Starter, Standard, and Enterprise license users:
  - *HP Client Automation Core and Satellite Getting Started and Concepts Guide*
- Included the user guide for Out of Band Management, which is newly supported by Core and Satellite servers:
  - *HP Client Automation Out of Band Management User Guide*

# Software and Hardware Requirements

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

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

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

Table 1 contains the software and hardware requirements for this release.

**Table 1** **CAE v7.5 Infrastructure**

| | | | | | HPCA Satellite Installation | Configuration Server | Distributed Configuration Server | Messaging Server | Proxy Server | Policy Server | Multicast Server | OS Manager Server | HPCA Core Installation | Reporting Server | Enterprise Manager | Portal | Patch Manager Server | Enterprise Mgr + OPE/VMS | OOBM Server | CA Standard Server (CCM) | CA Standard Agent (CCM) | Application Manager | Application Self-service Manager | Portal Agent (RMA) | AMPs Agent | Patch Manager Agent | Security And Compliance Manager | OS Manager Agent | OOBM Agent | Inventory Manager | Application Usage Manager | Extensions for Windows Installer | WTS & Citrix Support | Administrator | Batch Publisher | AMPs Editor | Extensions for Windows Installer | Configuration Analyzer | Knowledge Base Server |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Vendor** | **OS Name** | **OS Version #** | **bits** | **chipset** | | **CA Satellite** | | | | | | | | **CA Core** | | | | | | **CAS** | | **CA Agents (Enterprise)** | | | | | | | | | | | | **CA Admin** | | | | | |
| Microsoft | Windows 2000 | Professional SP4 | 32 | x86 | N | N | N | N | Y | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | N | Y | Y | Y | N | N | N |
| Microsoft | Windows XP | Professional SP3 | 32 | x86 | Y* | N | N | Y* | Y | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | N | N | N |
| Microsoft | Windows XP | Professional SP2 | 64 | AMD64/EM64T | Y* | N | N | Y* | Y | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | N | Y | Y | Y | N | N | N |
| Microsoft | Windows Vista | Business/Ent. SP1 | 32 | x86 | Y* | N | N | Y* | Y | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | N | N | N |
| Microsoft | Windows Vista | Business/Ent. SP1 | 64 | AMD64/EM64T | Y* | N | N | Y* | Y | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | N | N | N |
| Microsoft | Windows 2000 | Server SP4 | 32 | x86 | Y | Y | Y | Y | Y | Y | Y | Y | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Microsoft | Windows 2003 | Server SP2 | 32 | x86 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Microsoft | Windows 2003 | Server SP2 | 64 | AMD64/EM64T | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Microsoft | Windows 2003 | Server SP2 | 64 | Itanium | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | Y | Y | Y | Y | N | N | N |
| Microsoft | Windows 2003 | Server R2 SP2 | 32 | x86 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | N | N | N |
| Microsoft | Windows 2003 | Server R2 SP2 | 64 | AMD64/EM64T | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | N | N | N |
| Microsoft | Windows 2003 | Server R2 SP2 | 64 | Itanium | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | Y | Y | Y | Y | N | N | N |
| Microsoft | Windows 2008, SP2 | Server Std/Ent | 32 | x86 | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | N | N | N |
| Microsoft | Windows 2008 | Server Std/Ent | 64 | AMD64/EM64T | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | Y | Y | Y | Y | Y | Y | Y | N | N | N |
| Microsoft | Windows 2008 | Server Std/Ent | 64 | Itanium | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | Y | Y | Y | Y | N | N | N |
| HP | HP-UX | 11.23, 11.31 | 64 | PA-RISC 2.0 | N | Y | Y | Y | Y | Y | Y | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| HP | HP-UX | 11.23, 11.31 | 64 | Itanium | N | Y | Y | Y | Y | Y | Y | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Sun | Solaris | 9, 10 (Update 6??) | 64 | SPARC | N | Y | Y | Y | Y | Y | Y | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Sun | Solaris | 9, 10 | 32 | x86 | N | N | N | N | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Sun | Solaris | 9, 10 | 64 | AMD64/EM64T | N | N | N | N | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Novell | SuSE Linux Entrprs Desktop | 9 SP4, 10 SP1 | 32 | x86 | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Novell | SuSE Linux Entrprs Desktop | 9 SP4, 10 SP1 | 64 | AMD64/EM64T | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Novell | SuSE Linux Entrprs Server | 9 SP4, 10 SP1 | 32 | x86 | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Novell | SuSE Linux Entrprs Server | 9 SP4, 10 SP1 | 64 | AMD64/EM64T | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Novell | SuSE Linux Entrprs Server | 10 | 64 | Itanium | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |
| Red Hat | Enterprise Linux Desktop | 4.7, 5.3 | 32 | x86 | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Red Hat | Enterprise Linux Desktop | 4.7, 5.3 | 64 | AMD64/EM64T | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Red Hat | Enterprise Linux Server, AP | 4.7, 5.3 | 32 | x86 | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Red Hat | Enterprise Linux Server, AP | 4.7, 5.3 | 64 | AMD64/EM64T | N | Y | Y | Y | Y | Y | N | Y | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | N | Y | N | Y | N | N | N | Y | Y | N | N | N | N |
| Red Hat | Enterprise Linux Server, AP | 4.7, 5.3 | 64 | Itanium | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | N | N | N | N | N | Y | N | N | N | Y | Y | N | N | N | N |
| Apple | Mac OS X | 10.4, 10.5 | 32/64 | Intel | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | N | N | N | N | N | N | N | N | N | N | Y | N | N | N | N | N |
| Apple | Mac OS X | 10.4, 10.5 | 32/64 | PowerPC | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | N | N | N | N | N | N | N | N | N | N | Y | N | N | N | N | N |
| IBM | AIX | 5.3 | 64 | PPC | N | Y | Y | Y | Y | N | N | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N |

Y* Limited support for streamlined Satellite on Workstation editions in "proxy server" mode

# Backward Compatibility

## End of life

Version 4.2, 4.2i and 5.0 are entering an end-of-life program. Details will be available of the EOL on the HP Software support portal at http://support.openview.hp.com/prod-sppt-lifecycle/index.jsp. We recommend that customers upgrade to version 7.5 (or 7.51 for version 4.2i customers).
The following tables contain information about the backward compatibility of some components of the HPCA 7.50 release with previously released versions of the product.

**Table 2 Backward compatibility for agents and Administrator**

| Description | CM 4.x RCS \ | CM 5.x Configuration | 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 3 Backward compatibility for packaged applications**

| Description | Import to 4.x RCS | Import to 5.x | Import to 7.x |
|---|---|---|---|
| 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 4 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 *** |
| Patch Agent 7.x | N | Y | Y |

*** The following patch reports don't work: Product Status, Patch Status and Release Status.

**Table 5 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** |
|---|---|---|---|
| OS Manager Agent 2.1 | Y | N | Y[1] |
| OS Manager Agent 5.0 | Y[1] | Y | Y[1] |
| OS Manager Agent 5.1 | Y[1] | Y[1] | Y |

1 Except HP-UX re-installs

**Table 6 Backward compatibility for infrastructure components**

| **Description** | **CM 4.x Infrastructure** | **CM 5.00** | **CM 5.10** | **CA 7.x** |
|---|---|---|---|---|
| Enterprise Manager 5.1[1] | N | N | Y | N |
| Seurity and Compliance | | | | N |
| OS Manager 2.1 | Y | N | N | N |
| OS Manager 5.00 | N | Y | N | |
| OS Manager 5.10[1] | N | N | Y | |
| OS Manager 5.11 | N | N | 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 5.10 infrastructure

2 Requires version 5.10 of the Messaging Server and Reporting Server

## Thin Client Support

The following table lists supported Thin Client devices and operating systems.

**Table 2 Supported Thin Client Devices**

| Model | Operating System |
|---|---|
| T5720 | XPE |
| T5725 | Debian |
| T5730 | XPE |
| T5735 | Debian |
| T5530 | Win CE 6.0 |
| T5630 | WES, XPE |
| T5545 | ThinPro |
| T5540 | WinCE 6.0 |
| gt7720 | WES, XPE |
| gt7725 | ThinPro GT |

## 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 3 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 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 7.5 (or 7.51 for version 4.2i customers).

The following tables contain information about the backward compatibility of some components of the HPCA 7.50 release with previously released versions of the product.

# 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 3 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 v7.5 may work, but is not supported.

If your current version is:

- **HPCA Core and Satellite 7.20**, migrate to 7.50 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 7.50 "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 7.50 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*.
- **Multicast Server**: The 7.50 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-7.50 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*.
- **Distributed Configuration Server (DCS)**: There were no changes to this product for this release.
- **Mini Management Server**: The 7.50 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-7.50 configuration file to the new configuration file, `rmms.cfg`.

  4 Restart the Mini Management Server service.
- **Out of Band Management**: No migration path exists from previous standalone versions of the Out of Band Management Console to the Out of Band Management component that is now included as part of the 7.50 Core Console. As a result, there is no way to retain your existing OOBM System Defense configuration data (filters, policies, heuristics, and watchdogs) for the vPro devices on your network. Refer to the latest *HP Client Automation Out of Band Management User Guide* and *HPCA Core and Satellite User Guide* for additional details.

# Enhancements and Known Issues

This section contains a list of HPCA products with information about new features and functionality, resolved issues and known problems.

## HPCA Documentation

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

## Core and Satellite Servers

**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.

- With the release of HPCA 7.50, HPCA Starter and Standard are now included as part of the Core installation. Depending on your active license, different features will be available from the Core and Satellite Consoles. Refer to the *HP Client Automation Core and Satellite Getting Started and Concepts Guide* for more information.
- **HPCA Console**: The web-based interface with which an HPCA administrator can manage an HPCA environment. In this release, it replaces the HPCA Portal UI for Portal-based tasks.
- **Role-based Console Access**: An HPCA administrator can assign role-based “access levels” to users that are working in the HPCA Console. There are three roles that define the authorized level of access for users: *Administrator*, *Operator*, and *Reporter*; each of which can perform different tasks, based on their access rights.
- **Unattended Configuration and Installation of Satellite**: The Satellite server contains an XML file that can be accessed after the Satellite is installed, and then used to specify custom configuration parameters for subsequent Satellite server installations.

- **Out of Band Management in the HPCA Console**: There are new features that allow an HPCA administrator to perform management operations regardless of their system power or operating system state.
- **OS Management Interface**: Remote control auditing; new group interface for targeting; AD can be used for management operations; vulnerability management, compliance management, and security tools management capabilities.
- **Reporting Tab**: Initial page loading improvements; Limits for time/size of results of query; LDAP filter performance improvements; Search scope enhancements.
- The HPCA Console's **default timeout value** is `20` (minutes). This value (`http.session.timeout.minutes`) can be changed in *`InstallDir`*`/tomcat/webapps/sessionmanager/web-inf/sessionmanager.properties`.
  - The minimum valid value is **2** (minutes).
  - There is no maximum allowed value, but the session timeout should be of reasonable duration in order to ensure HPCA Console security.
  - After changing this value, restart the **HPCA-Tomcat** service.
- **Patch Management**
  - Supports Patch Management on devices running Windows and Linux operating systems, and adds support for HP Softpaqs.
  - Allows all configuration, acquisition, operations, and access to reports and dashboards that are related to Patch Management to be performed from the HPCA Core Console.
  - Adds support for the Patch Agent option for Download Manager: This new ability allows for the transfer of content that is required in order to apply the designated patches to a managed device outside of the usual HPCA agent connection process. The transfer process occurs passively, per the configured constraints. For more information refer to the Configuration chapter in the *HPCA Core Enterprise User Guide*.
  - Adds support for the Metadata Distribution Model for Patches: This option provides an alternative method for distributing Microsoft patches throughout an enterprise. Initial acquisition and patch discovery uses patch metadata only. A new component, the Patch Gateway, is used to download the patch binary data upon initial request from the HPCA agent. This content is cached for use by other agents in your enterprise but not stored in the Configuration Server Database. For more information, refer to the Patch Management using Metadata chapter in the *HPCA Core Enterprise User Guide*.
- **Distributive Task Management** (**DTM**): A new job subsystem for Windows operating systems. It offers a pull-model, and its main advantage can be summarized as "centrally managed, distributed scheduling." Using DTM, an HPCA administrator can schedule jobs for agents and have visibility to the details of the jobs.
- **Group Management**: This feature allows an HPCA administrator to create new groups, and modify and delete existing groups.
- **IPv6 Support**
  - Communication is possible using IPv6 as an option between Core and Satellite servers, and between these servers and an external LDAP server.
  - For details and limitations, refer to the IPv6 Networking Support appendix in the *HPCA Core and Satellite Enterprise User Guide*.
- Application Usage Manager, KB Server, and Configuration Analyzer are supported in this release.

- The following Client Automation components that are provided on the media are *not supported* in a Core/Satellite environment due to alternate HP solutions or deprecated support. However, they are still supported in the Client Automation legacy environment.
  - Service Desk Adapter
  - Proxy Server: The Core/Satellite environment makes exclusive use of the Apache-based Proxy Server. The legacy Integration Server-based Proxy Server, which is available on the HP CAE 7.50 media, is redundant in a Core/Satellite environment.
- **Additional Improvements and Innovations**
  - High priority defect fixes and enhancements, such as: non-destructive imaging; ROMS security; fixing of post-7.20 release defects.
  - Mobile and virtual perspectives that enable an HPCA administrator to limit the information that is displayed in the dashboard panes.
  - New compliance scanning, reporting, and dashboards.
  - New mobility-compliance dashboard feature.
  - Application virtualization support through integration with VMWare ThinApp.

## REXX Scripts

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)

### **RESOLVED** Core/Satellite with OS Mgr: Deploying a Linux image that spans multiple resource files is not supported

| | |
|---|---|
| PROBLEM: | Deploying a legacy image created under Linux SOS that is spanned will fail; any image that requires spanning and is put in more than one resource file (such as `ImageName.img`, `ImageName.002`, `ImageName.003`, etc.) will fail. |
| CAUSE: | In the Core/Satellite environment, the files being downloaded are not being properly handled. |
| WORKAROUND: | Resolved in version 7.50. |

### **RESOLVED** Core/Satellite with OS Mgr: Install from CD/DVD option fails

| | |
|---|---|
| PROBLEM: | Using the **Install from CD/DVD** option from the `ImageDeploy.iso` will fail. |
| CAUSE: | In the Core/Satellite environment, files cannot be correctly expanded on the disk due to an invalid header. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core/Satellite with OS Mgr: “Boot steering failed” message appears when WinPE SOS runs

| | |
|---|---|
| PROBLEM: | On internationalized platforms, such as Traditional Chinese, deploying Windows based images from the WinPE service OS may fail if the system initially booted into the Linux service OS.<br>This may happen if the Linux service OS is unable to deploy the OS service (for example, a `.WIM` image that must be deployed by WinPE). Any image deployment or hardware configuration element that references an internationalized OS service name or hardware configuration (LME) name which must be handled under the WinPE service OS requires that the system boot into the WinPE service OS first to identify and handle the internationalized OS or Hardware Configuration object name. |
| CAUSE: | The XML document that includes the Hardware Configuration Element (LME) and OS service names, provided with the CA infrastructure, is not encoded consistently when switching between the WinPE service OS and the Linux service OS. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core: Upgrading a license file from the Core console Settings page does not update all component service licenses

| | |
|---|---|
| PROBLEM: | After using the Core console Settings page to upgrade the license file, a component service may still report that the license is invalid. For example, this is a known issue with Patch Manager. |
| CAUSE: | The component modules that require the updated license file may not be receiving the new license contents that were supplied through the Core console Settings page. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Installing the Core or Satellite onto a server with TCP port 3466 in use will fail

| | |
|---|---|
| PROBLEM: | The Core and Satellite installations will fail (without any indication of the error) if the default TCP port 3466 is already in use. |
| CAUSE: | The installation programs are not validating that the required TCP port 3466 is available. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Satellite with SSL and Configuration Services: After a synch, dmabatch log includes errors that can be ignored

| | |
|---|---|
| PROBLEM: | On Satellites enabled for SSL and Configuration Services, the `\DCS\ dmabatch.log` contains Background Error messages after a successful sync with its upstream host. These errors will exist in each domain that the dmabatch program prepares. For example:<br>`Note: =============== Preparing Databases ===============`<br>`Error: main: Background Error: can't read "dns": no such variable`<br>`    while executing`<br>`"syslog note "$tag host <$host\|$dns\|$ip> does not match certificate""` |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Satellite is unable to forward messages to an upstream host after an entry on Settings page, Settings area is saved

| | |
|---|---|
| PROBLEM: | Pressing Save in the Settings area of the Satellite's Settings page results in the Satellite being unable to forward messages to its upstream server. This means any Agent-reported data does not get reported to the Core server and databases.<br>The Settings area contains the check box to enable SSL and the entries for the upstream server and the license file. |
| CAUSE: | Whenever Save is pressed in the Settings area, Satellite processing code places an invalid entry in the URL parameter of the `rms.cfg` file's register forward section. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Thin Client Service required for Windows CE Thin Client support also named the Mini Management Service

| | |
|---|---|
| PROBLEM: | The HP Client Automation Thin Client service that is required to support Windows CE Agents on a Core or Satellite server is named the Mini Management Service in the traditional Client Automation environment. |
| CAUSE: | The rmms service required for Windows CE Thin Client support was assigned different display names in different product areas. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core: Connection errors may be seen if default configuration for Enterprise Manager and BSA Essentials Network is not reviewed

| | |
|---|---|
| PROBLEM: | The Core configuration automatically places default settings in the Enterprise Manager configuration of the BSA Essentials Network reporting database. Using these default settings as is may result in connection errors. |
| CAUSE: | The default configuration for the BSA Essentials Network reporting database may not be accurate for all database configurations, such as a SQL Server database using dynamic ports. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Configuration file error causes Multicast Server to not work

| | |
|---|---|
| PROBLEM: | The HPCA Multicast Server does not work. |
| CAUSE: | The `mcast.cfg` configuration file needs to be modified. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core and Satellite: WinCE Agent support fails due to incorrect port numbers in the RMRAM.INI file

| | |
|---|---|
| PROBLEM: | After installing the WinCE Agent, some of the port numbers in the RMRAM.INI file are configured incorrectly for a Core and Satellite environment. |
| CAUSE: | A single CAB file is used to install WinCE Agents in both the CAE and Core and Satellite environments. The default values for RPD_PORT and RIM_PORT in the RMRAM.INI file are correct for a CAE environment, but not correct for a Core and Satellite environment. These RPD_PORT and RIM_PORT numbers must be manually changed to 3466 after the HPCA Agent is installed. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core/Satellite with large files: Very slow downloads

| | |
|---|---|
| PROBLEM: | In certain cases, you may experience very slow downloads of large files, such as OS images or other large files. |
| CAUSE: | The Apache web server that is acting as the proxy server for all resource downloads may need additional tuning to optimize it for faster transfer of large files. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core with Reporting Server: Error page is displayed when setting data filters as Operating System

| | |
|---|---|
| PROBLEM: | The column width of `devicecache.filtervalue` created for the Reporting database table `rrs_devicecache` is too short. |
| CAUSE: | The Prerequisite scripts used by the Core server to create this column have the wrong value. If the table is created directly using the Reporting Server, the column is defined correctly. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core enabled for SSL: Enterprise Manager is available using HTTP on port 3466, but is not enabled for https://core_server:443/em

| | |
|---|---|
| PROBLEM: | After enabling the Core for SSL processing, the Enterprise Manager (EM) is not available on the Core's HTTPS port of 443 (https://core_server:443/em) but remains available on the HTTP port of 3466 (http://core_server:3466/em). |
| CAUSE: | The httpd-ssl.conf file is missing the correct configuration for EM to be enabled for SSL. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Core and Satellite: "Authentication not changed" displays after setting Console Access for Directory Service Accounts

| | |
|---|---|
| PROBLEM: | After specifying Console Access for Directory Service Accounts using an IP address in the Directory Host field, the message "Authentication not changed" appears. |
| CAUSE: | IP addresses cannot be specified in the Directory Host field for the Directory Service Accounts. This is a correction to the text in the July 2008 version of the *Core and Satellite Getting Started and Concepts Guide*. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** Portal Installed on Core: 'No install media present' displays when installing the Client Automation Agent to a Linux device

| | |
|---|---|
| PROBLEM: | When using the Portal "Install Client Automation Agent" task to a Linux device, a message states that the installation media is not present, followed by a path location of where it expects to find the media. |
| CAUSE: | The Core installation program is not copying the installation media for Linux agents to the appropriate Portal location. |
| WORKAROUND: | Resolved in version 7.50. |

## 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.<br>Note: HPCA agent SSL support over a **TCP/IP** connection is functional; it is not part of this Known Limitation. |
| CAUSE: | The latest agent code requires an additional update to enable HTTPS support. |
| WORKAROUND: | A 7.50 HPCA agent patch is required in order to enable HTTPS connections. |

## 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).<br>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 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, only the first 1500 members are returned in the "member" attribute by the Directory and displayed on a Core console. |
| 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 Core Console and Enterprise Manager have no visibility to the additional members. |
| WORKAROUND: | Use the Console's Search Parameters to fine tune and narrow your search. |

## 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 service in the HPCA Console and the SCS Server. This will cause problems when the user tries to set SCS Properties by selecting Configuration > Out of Band Management > Device Type Selection > Manage vPro Device. |
| 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. |

## 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 |

## 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. |

## 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. |

## 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, 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. |

## Users with a UTF-8 password can't login

| | |
|---|---|
| PROBLEM: | Internal (Portal) users with UTF-8 passwords are unable to logon. |
| CAUSE: | Issue in Portal handling of UTF-8 passwords. |
| WORKAROUND: | Use an ASCII password. |

## "Empty" shows up in task notification when using the first time setup windows

| | |
|---|---|
| PROBLEM: | When downloading logs, the message "Unable to find flex application" displays. |
| CAUSE: | This is typical after a fresh installation of Macromedia Flash Player without closing and restarting the browser. |
| WORKAROUND: | Note: This condition occurs sporadically—only after a certain series of steps has occurred.<br>Close the browser and re-launch the console application. |

## 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. |

## Reporting: Memory Range sort does not function correctly

| | |
|---|---|
| PROBLEM: | Summary Reports, "count by memory" sort order is incorrect. |
| CAUSE: | Values are being represented as strings. |
| WORKAROUND: | None. |

## Reporting Data Filters for Memory Less/More Than misleading

| | |
|---|---|
| PROBLEM: | The Reporting Server "memory less than" and "memory more than" filters do not work as expected. |
| CAUSE: | Filters will operate as "memory more than or equal to" and "memory less than or equal to." |
| WORKAROUND: | To get desired results, use the filters with the understanding that they will work as described in CAUSE. |

## 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 |

## Searching by IP Address under Device Management

| | |
|---|---|
| PROBLEM: | Sorting by IP address (including IPv6) requires a custom method. |
| CAUSE: | IP Addresses are represented as strings. |
| WORKAROUND: | None |

## 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.<br>1. Open *ManagementPortal_InstallDir*/etc/rmp.cfg.<br>2. Add or change the following parameter to indicate the job history in days to keep:<br>**JOBHISTORYTTLDAYS 30**<br>3. Save the file.<br>4. Restart HPCA Portal service.<br>The default location of the rmp.cfg file is:<br>Core server: c:\Program Files\Hewlett-Packard\HPCA\ManagementPortal\etc<br>HPCA Legacy: c:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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 |

## 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 |

## 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 |

## 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. |

## 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. |

## 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. 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: | Issue is due to 3rd party dependencies of OOBM. |
| WORKAROUND: | None. |

## 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. |

## 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 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. |

## Failure to establish SOL/IDER session on wireless network for OOBM vPro devices

| | |
|---|---|
| PROBLEM: | OOBM server uses Intel supplied libraries for SOL/IDER operations. The Intel library opens a TCP connection on port 16994-nonTLS/16995-TLS to the remote vPro machine for SOL/IDER operations. This library accepts a number of timeout parameters when establishing a SOL session as well as accepts a number of timeout parameters when establishing an IDER session. On occasion, in a wireless network, the Intel library fails to establish a SOL session while using the default timeout parameters values. This will cause a problem when the user is performing boot operations on a vPro device by selecting Operations > Out Of Band Management > Device Management > <vPro Device> > Remote Operations. |
| CAUSE: | The vPro device takes a long time to communicate with the OOBM server on wireless communication. This will sometimes cause a timeout for the SOL/IDER operations. |
| WORKAROUND: | None. |

## 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 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. |

## 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.<br>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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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 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.<br>Or<br>Ensure all Directory Server Accounts have the userPrincipalName attribute set, a valid groupname, and DNS host access. |

## Core/Satellite and CAE Classic with OS Mgr: Prepwiz 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. |
| 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. |

## Core/Satellite and CAE Classic with OS Mgr: 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. |

## Satellite: "URL error" results when entering an IPv6 address in Authentication Wizard for Directory Server Account host

| | |
|---|---|
| PROBLEM: | An error flashes: "Unable to establish LDAP connection; bad URL" from the Authentication Wizard of an IPv6-enabled Satellite when using a global IPv6 address to define the Directory Host for the Directory Service Account. |
| 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. |

## TCL Setup on Multibyte character with alternate code page fails

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

## 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`.<br>2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HPCA-Apache`.<br>3. Open the ImagePath value for modification, and remove `-D ssl` from the end of the command line.<br>4. Start HPCA-Apache Windows service. |

## 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. |

## 7.5 Does not match certificate is seen in dmabatch.log on SSL Mode

| | |
|---|---|
| PROBLEM: | The following syntax error is observed in some logs.<br>`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”"`<br>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. |

## Patch Distribution using Metadata: 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 Agent Option: 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:<br>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 Agent Option: 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 Agent: 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:<br>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.<br>2. The fix information for `nvdkit`  will be posted to the Agent Update Information page. |

## Core and Satellite: 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. |

## 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 Gateway: 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 Gateway: 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:<br>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:<br>1.1 Network issue<br>1.2 Web Proxy issue<br>1.3 Vendor site maintenance<br>2. During the above situation, the service for the HPCA Patch Manager Server is restarted due to one of the following reasons:<br>2.1 A user updates any of the Configuration settings for Patch Management from the Core Console.<br>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. |

## 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. |

## Portal installed on Core: HPCA Agents installed from Portal are unable to connect to Configuration Server

| | |
|---|---|
| PROBLEM: | When using the Portal installed on a Core Server, the values that are specified in the HPCA Configuration Server Host and Port fields of the Install Client Automation Agent task are ignored if the default `Install.ini` file is used. This is by design, as discussed below. |
| CAUSE: | The default `Install.ini` that is provided with the HPCA agent media in the Core has been pre-configured to enable all HPCA agent installations to initially contact the Core to synchronize the Client Operational Profiles (COP) settings. These settings will direct the HPCA agent to an appropriate set of Satellites for subsequent activities. Because of this, when deploying an HPCA agent using the Portal, the Configuration Server Host and Port values that were provided in the Portal UI wizard are ignored. |
| WORKAROUND: | If you need more flexibility upon initial HPCA agent deployment:<br>1. Comment out the values `resolutionport` and `resolutionmanager` from the `Install.ini` file, which is located in *`InstallDir`*`/Media/client/default/win32`.<br>2. Save your changes.<br>3. Use the Portal to specify the Configuration Server Host and Port values during the Install Client Automation Agent task. |

## Core 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. |

## 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. |

## 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: | |
| WORKAROUND: | Use "reboot after install, do not prompt user" as the reboot setting. |

### Agent removal wizard job ends in error, if removing an manually installed agent

| | |
|---|---|
| PROBLEM: | Using the agent removal wizard to remove a manually installed agent will cause the job to end in error. |
| CAUSE: | |
| WORKAROUND: | Agent will remove, however job will end in error. |

### 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. |

### 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. |

### 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. |

## 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. |

### 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. |

## 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'. |

### 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. |

## 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. |

### 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. |

### 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 Management Profiles

- AMP Agent: The Application Manager Agent now includes embedded support for running Application Management Profiles. The previous requirement to install a separate Server Management Agent has been removed.
- HP BSA Essentials Network: Where you can obtain the latest Client Automation Enterprise community content, including AMPs.

## Application Manager and Application Self-service Manager

- SSL/HTTPS communication is not supported.
- The default, installation directory path for Windows-based HP Client Automation (HPCA) agents—formerly HP Configuration Management (CM) agents—has been changed to `Program Files\Hewlett-Packard\HPCA`.
- Connect Deferral is a new feature. It allows a user to defer required actions on their systems. This feature adds a new class, **Connect Deferral Configuration** (**CDFCFG**) to the CLIENT Domain, as well as a new RADSKMAN setting, **cdf**.
- The **HPCA Registration and Agent Loading Facility** (**RALF**) is an agent component that is available for thin-client devices that are managed by an HPCA Core infrastructure. RALF auto-registers the device with the HPCA infrastructure, and manages the HPCA agent installation, which is initiated from the main console.
- There is one new HPCA agent sub-features:

— **PlusHP** which includes: *SMART Drive Alert Monitoring*, *HP Hardware Alert Monitoring*, and *HP Hardware BIOS configuration support*.

## 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.<br>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. |

## 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 |

## Agent: 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. |

## 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. |

## 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 |
| WORKAROUND: | During the upgrade, dispose of the dialog (by clicking **Ignore** or **OK**, depending on the dialog) to continue with the agent install. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

## 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. |

### 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. |

### 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. |

### 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. |

### 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. |
| 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. |

### 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 Usage Manager

- Add supports for posting data to a SQL database hosted by:
  - SQL Server 2008
  - Oracle 11g, Release 1 with the latest Oracle patch set
- **ODBC DSNs Require 32-bit Drivers**: Client Automation components running on 64-bit systems run in 32-bit emulation mode. Therefore, when using ODBC on 64-bit Windows platforms, you must create the DSN for the ODBC database using 32-bit drivers.

  On a Windows 64-bit machine, you can access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the DSNs required by our product.

## Batch Publisher

- The Batch Publisher was rebranded from Configuration Management to Client Automation.
- Batch Publisher supports only Linux and Windows operating systems.
- Object-based publishing is no longer supported.

## Configuration Analyzer

### Failed to import state files when database name contains "." character

| | |
|---|---|
| PROBLEM: | Failed to import state files when database name contains "." character |
| CAUSE: | The SQL Server expects the BCP command as [DatabaseName].[OwnerName].[TableName] & so on.<br>When the database name contains a period, the BCP interprets it as the Next parameter (the OwnerName) and this causes it to fail. |
| WORKAROUND: | Create a Database without any period character in its Name and HPCA Configuration Analyzer State file importing will work without any issues. |

### No security information is shown for registry

| | |
|---|---|
| PROBLEM: | No security information is shown for registry. |
| CAUSE: | The State Files that are imported by HPCA Configuration Analyzer are generated by the State File Generator. State file Generator does not populate the security information of registry every time.<br>If its is populated, it may be seen on the HPCA Configuration Analyzer State Details security properties, and if its not populated, blank screen shown in the State Details security properties. |
| WORKAROUND: | No workaround. |

## Configuration Baseline Auditor

No changes for this release.

## Configuration Server

- Added the following ADMIN.ZCONNECT class attributes: DRIVEMAP, ROLE, SUBNET, MODEL, MANUFACT, LDS, and LME.
- Added CLIENT classes: CDFCFG and NTFYSEC.
- Changed the following PRIMARY.SECURITY.ZSERVICE class variable lengths to 255: ZREPAIR, ZVERIFY, ZUPDATE, ZDELETE, and ZCREATE.
- Added the class attribute: PRIMARY.SYSTEM.ZMETHOD.ZSTOP001.
- Added a new export option command-line parameter for RadDBUtil, **`-substitute`**.

### **RESOLVED** When shutting down a Configuration Server on HP-UX, a core.ZLICUTIL file will show up

| | |
|---|---|
| PROBLEM: | When shutting down a Configuration Server that is running on an HP-UX server, the ZLICUTIL executable is launched and fails to execute, and might generate a CORE dump. |
| CAUSE: | During the shutdown, the process tries to obtain the LOCALE on which the platform is running. Often, this call returns an unexpected NULL value which is not recognizable to the process. This causes the ZLICUTIL executable to prematurely terminate. |
| WORKAROUND: | No work-around available for this release. |

### SSL: Configuration Server not able to find certificate in CJK directory (I18N path)

| | |
|---|---|
| PROBLEM: | When the Configuration Server is installed on an I18N path and the SSL Manager task is properly configured, the SSL Manager failed to startup with the error message in the Configuration Server log: Missing certificate file. |
| CAUSE: | When the Configuration Server starts, the SSL Manager is not able to read the certificate file in the I18N path. |
| WORKAROUND: | No work-around available for this release. |

### During database migration, custom data may not supersede information currently in the database

| | |
|---|---|
| PROBLEM: | During database migration, custom data may not supersede information currently in the database (CORE data). |
| WORKAROUND: | Review the output of the DBDIFF file to ensure anything that is not going to be imported (REPLACE=NO), but should be, is imported after the migration process completes. |

### 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.<br>Example:<br>if today you run from a script:<br>`raddbutil.exe export -output foo -walk 0 PRIMARY.POLICY.USER.RPS`<br>Which updates the ../log/raddbutil.log<br>If you change this cmd line in your custom scripts to:<br>`raddbutil.cmd export -output foo  -walk 0 PRIMARY.POLICY.USER.RPS`<br>The following being the content of raddbutil.cmd –<br>`@set logfile=..\log\raddbutil.log`<br>`@del /F /Q %logfile%.new`<br>`raddbutil.exe %1 -logfile %logfile%.new %2 %3 %4 %5 %6 %7 %7 %9 %10 %11`<br>`@type %logfile%.new >> %logfile%`<br>`@del /F /Q %logfile%.new` |

### **RESOLVED** RadDBUtil incorrectly deletes Classes referenced by dynamic connections

| | |
|---|---|
| PROBLEM: | When using RadDBUtil to do a delete with the walk option "delete -walk 1" and you are using dynamic connections, RadDBUtil will also delete the class's dynamic connections Connect To. |
| CAUSE: | The interpretation of ABC.&(XYZ) -> ABC.* during a "walk" option was intended to relate to EXPORT only, not DELETE.<br>ABC.&(XYZ) should map to ABC.* on EXPORT due to the uncertainty of what XYZ might be – and should have mapped to nothing on DELETE due to this same uncertainty. Instead it still maps to ABC.* and the DELETE, and removes more than intended. |
| WORKAROUND: | Obtain the latest version of RadDBUtil. |

## Distributed Configuration Server

- There are no new features in this release.

### **RESOLVED** DCS with SSL: cacert.pem error on slave side will cause unlock error, and thus a sync failure

| | |
|---|---|
| PROBLEM: | After running a DCS synchronization using SSL, dmabatch gives the error<br>`unlock Error: slave RCS(localhost:444) reason={bad certificate location "cacert.pem": no such file or directory`<br>and leaves the Configuration Server Database in hard-lock state, causing the synchronization to fail with RC 16. |
| CAUSE: | Bug in RC5 of HPCA DCS. |
| WORKAROUND: | **CAE Environment**: Copy …`\dcs\cacert.pem` to:<br>`C:\Program Files\Hewlett-Packard\CM\ConfigurationServer\DB`.<br>**Core/Satellite Environment**: Copy `C:\Program Files\Hewlett-Packard\HPCA\ApacheServer\conf\ssl.crt\ca-bundle.crt` to<br>`C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\HPCA\ConfigurationServer/DB\cacert.pem`<br>and to<br>`C:\Program Files\Hewlett-Packard\HPCA\dcs\cacert.pem`. |

### **RESOLVED** DCS Source installation read I18N CA-CS DB path as garbage

| | |
|---|---|
| PROBLEM: | When installing the DCS Source component, the dialog at which you select a Source HPCA-CS Database path shows the non-ASCII characters in database path as garbage. |
| CAUSE: | The setup program may be displaying double-byte characters as ASCII until a refresh occurs. |
| WORKAROUND: | Click Browse to re-select the directory; the characters will be correctly displayed. |

### **RESOLVED** DCS fails to load DBPATH with I18N characters

| | |
|---|---|
| PROBLEM: | After installing the DCS Source component, when trying to access HPCA-CS with an I18N DBPATH, (path containing double-byte characters) there is a warning message in the `httpd-distributedcs-3473.log` file and the DCS cannot execute.<br>`Warn: DCS: failed to load: bad DBPATH <C:/Program Files/Hewlett-Packard/CM/ConfigurationServeréŽ¯çŠ³æ«˜/DB>`<br>But in the `dcs.cfg` file, the DBPATH is<br>`C:/Program Files/Hewlett-Packard/CM/ConfigurationServeræƒ æ™®/DB` |
| CAUSE: | Double-byte characters are incorrectly being handled as ACSII characters. |
| WORKAROUND: | Use Notepad to open the `dcs.cfg` file, and then save it in UTF-8 format. This will result in the 3-character BOM being inserted at the front of the `dcs.cfg` file. |

## Enterprise Manager

- Job Management was updated to include **Distributed Task Management** (**DTM**) jobs. The target devices periodically synchronize themselves with the HPCA infrastructure and receive instructions to perform a particular action according to a specified schedule. You can configure and manage this schedule in the HPCA Enterprise Console. This is a more distributed (client-pull) method of job management.

DTM jobs are available to Windows agents only.

- Operating System Management (OSM) features formerly available in the HPCA Portal user interface are now available in the HPCA Enterprise Console (or the Enterprise Manager in a traditional component-based HPCA installation). You can now deploy and manage operating systems on individual client devices or groups of devices directly from the HPCA Enterprise Console.
- In addition to Vulnerability Management (introduced in HPCA version 7.20), HPCA now offers Compliance Management and Security Tools Management capabilities. See Security and Compliance Manager on page 69 for details.

In the following list of known issues, the <*InstallDir*> placeholder is used to represent the location where the Enterprise Manager is installed. This location is specified during the installation process.

For a Core and Satellite installation, the default installation location is:

`C:\Program Files\Hewlett-Packard`

For a traditional (classic) HPCA Enterprise installation, the default installation location is:

`C:\Program Files\HP\HP BTO Software`

The MySQL database instance embedded in the Enterprise Manager is an operational database that holds information about jobs and user role assignments.

The availability of this database is not critical to the core (lights out) 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 only be accessible via a special service account, to processes local to the Enterprise Manager – no direct network access is possible.

### ** RESOLVED ** EM 7.20: Vulnerability Management dashboard statistics display 0 values when data exists

| | |
|---|---|
| PROBLEM: | After an initial CAE install and priming of the OVAL vulnerabilities, the vulnerability statistics displayed on the Vulnerability Management homepage may show “Vulnerabilities Imported: 0”. |
| CAUSE: | The database table being used to populate the report has not yet been updated. |
| WORKAROUND: | Resolved in HPCA version 7.50. |

### ** RESOLVED ** EM 7.20: The Most Vulnerable Products dashboard pane takes too long to load

| | |
|---|---|
| PROBLEM: | The Most Vulnerable Products dashboard pane might take a long time to load or times out. |
| CAUSE: | The underlying query used for the Most Vulnerable Products pane takes a long time to complete when a large dataset exists. |
| WORKAROUND: | Resolved in HPCA version 7.50. |

## ** RESOLVED ** EM7.20: Reset button on Updates and Databases tab on the HP Live Network configuration page has little or no effect

| | |
|---|---|
| PROBLEM: | On the Live Network configuration page, the **Reset** button on the Databases and Updates tabs should reset the values on the form to their initial values when this editing session was initiated. Some of the values, however, are not reset. |
| CAUSE: | The **Reset** button on this page does not work for all fields. |
| WORKAROUND: | Resolved in HPCA version 7.50 |

## ** RESOLVED ** EM7.20: Directory Services – Cannot save after clicking the Reset button

| | |
|---|---|
| PROBLEM: | Clicking **Reset** while updating an existing directory service will result in a “Fields are not complete or contain invalid data” error when you attempt to save your changes. |
| CAUSE: | The form submission logic incorrectly believes that a field has changed when, in fact, no changes have been made due to the reset. This prevents form submission. |
| WORKAROUND: | Resolved in version 7.50. |

## ** RESOLVED ** EM 7.20: HP Live Network content acquisition reports successful completion, but log file shows connection errors

| | |
|---|---|
| PROBLEM: | An HP Live Network content update (acquisition) reports a successful completion, but the log file shows connection errors. |
| CAUSE: | The HP Live Network Connector may not exit with a proper error code when there are connection errors. HPCA then treats the content acquisition as a successful acquisition which did not have any new content to download. The most typical reasons for the connection error are incorrect proxy settings or HP Live Network credentials. |
| WORKAROUND: | Resolved in HPCA version 7.50. |

## ** RESOLVED ** EM 7.20: Directory Services configuration changes result in an empty password

| | |
|---|---|
| PROBLEM: | You can save LDAP directory configuration changes without re-entering the appropriate password. After the administrator clicks **Save**, the directory service is saved with a blank password. Symptoms include LDAP sources disappearing and leaf nodes not expanding properly. |
| CAUSE: | The blank password that is saved is invalid. The LDAP source will not provide any additional data. While the user interface might appear to have some of the data and respond to requests, this is only due to caching. Checking the status of the connection will show that it is invalid. |
| WORKAROUND: | Resolved in HPCA version 7.50 – an error message is displayed if you attempt to save without entering a password. |

## ** RESOLVED ** EM 7.20: Vulnerability Management reports may show inconsistent number of vulnerabilities

| | |
|---|---|
| PROBLEM: | When you drill down into an individual device report, the number of Vulnerabilities Found in the Device Details section does not always equal the number of vulnerabilities that are displayed in the Device Vulnerability Details table. |
| CAUSE: | Vulnerability Management reports that show bulletin information are filtered on Vendor = Microsoft. If the vendor is not Microsoft, the remedy for the vulnerability on the selected device will not be displayed. Thus, the counts may not always match. |
| WORKAROUND: | Resolved in HPCA version 7.50. |

## ** RESOLVED ** EM 7.20: Date format is not locale sensitive

| | |
|---|---|
| PROBLEM: | Both the Notify Wizard and Updates tab on the Live Network configuration page contain Start Date. This date is displayed in the USA format (MM/DD/YYYY) and the format does not change with the locale of the browser. |
| CAUSE: | Start Date is implemented using a standard Adobe Flex component. This is due to the lack of internationalization support in Flex 2, which was used in Enterprise Manager 7.20. |
| WORKAROUND: | Resolved in version 7.50. |

## ** RESOLVED ** Truncation of object names in navigation tree

| | |
|---|---|
| PROBLEM: | If you expand a navigation tree – such as the directory tree – the names of the expanded items that are not visible when the tree is expanded, and do not fit in the pane, are truncated to the current pane width. |
| CAUSE: | Adobe Flex code contains a defect that is fixed in Flex 2 Hot Fix 2 or Flex 3. |
| WORKAROUND: | Resolved in HPCA version 7.50. |

## ** RESOLVED ** Session timeout occasionally puts Enterprise Manager into unusable state

| | |
|---|---|
| PROBLEM: | This can happen if you perform an action in the Enterprise Manager console that causes a pop-up window to open just as your console session begins the process of timing out. |
| CAUSE: | A timing issue arises between the pop-up for the action and the pop-up for the session expired condition. |
| WORKAROUND: | Resolved in HPCA 7.50. |

## EM 7.50: CAE – 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. |

## EM 7.50: 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. |

## EM 7.50: 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.<br>1. Open *`ManagementPortal_InstallDir`*`/etc/rmp.cfg.`<br>2. Add or change the following parameter to indicate the job history in days to keep:<br>**`JOBHISTORYTTLDAYS 30`**<br>3. Save the file.<br>4. Restart HPCA Portal service.<br>The default location of the `rmp.cfg` file is:<br>Core server: `c:\Program Files\Hewlett-Packard\HPCA\ManagementPortal\etc`<br>HPCA Legacy: `c:\Program Files\Hewlett-Packard\CM\ManagementPortal\etc` |

## EM 7.50: 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. |

## EM 7.50: 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. |

## EM 7.50: 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. |

## EM 7.50: 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. |

## EM 7.50: 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:<br>`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:<br>1 Go to the HPCA installation directory, and locate the sub-directory named `LiveNetwork`.<br>2 Copy the `LiveNetwork` directory and all of its contents to the root path on your system (for example, `C:\LiveNetwork`)<br>3 Open the HPCA Console. Go to the **Configuration** tab. Expand **Infrastructure Management**, and select the **Live Network** settings section.<br>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`).<br>5 Click **Save**. |

## EM 7.50: 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. |

## EM 7.50: 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.

## EM 7.50: CVE definition is truncated when written to the database

PROBLEM:

The `vms-server.log` 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.

CAUSE:

The CVE description is larger that the supported 2000 characters.

WORKAROUND:

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:

- Look up details about the CVE from either NIST or MITRE.
- Update the data base directly with the missing CVE contents using a SQL update statement such as the following:

```
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'.
```

## EM 7.50: 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

## EM 7.50: 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. |

## EM 7.50: 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. |

## EM 7.20: 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.<br>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:<br>CAE: `<`*`InstallDir`*`>\VulnerabilityServer\logs\vms-server.log`<br>Core and Satellite: `<`*`InstallDir`*`>\HPCA\VulnerabilityServer\logs\vms-server.log`<br>Both: `<`*`LNc-InstallDir`*`>\lnc\log\live-network-connector.log` |

## EM 7.20: 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.<br>Alternative Workaround: Upgrade to Internet Explorer 7. |

## EM 7.20: 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. |

## EM 7.20: 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). |

## EM 7.20: The Firefox browser shows an actionscript error upon sign-out

| | |
|---|---|
| PROBLEM: | The Adobe Flash Player 9 plug-in in the Firefox browser reports the following error message after you sign out of the Enterprise Manager:<br>`Error #2044: Unhandled SecurityErrorEvent: text=Error #2047: Security sandbox`<br>`violation: LocalConnection.send: ... cannot access`<br>`http:// ... /em/flex/em.swf` |
| CAUSE: | This is a well known problem with the Adobe Flash Player plug-in. More information on this issue can be found at **https://bugs.adobe.com/jira/browse/FB-8927.** |
| WORKAROUND: | Refreshing the browser window makes this intermittent issue disappear. |

## EM7.20: Collapsing a container on Management → Directories page changes current object selection in navigation tree but not contents displayed in right pane

| | |
|---|---|
| PROBLEM: | In some cases, when you collapse a container node in the left navigation tree, that node appears to become the selected node. The right side content pane, however, is not updated. |
| CAUSE: | The navigation tree representation does not necessarily reflect the current node. |
| WORKAROUND: | Click the node that you want to make the current node in the content pane. |

## EM7.20: 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. |

## EM 7.20: 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:<br>`\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. |

## EM 7.20: 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. |

## EM 7.20: 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).<br>Verify your SQL Server port settings, and update the SQL Server port information in the following places:<br>Core and Satellite installation: Configuration > Infrastructure Management > Database Settings<br>Traditional installation: Configuration > Live Network > Databases tab<br>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.<br>The following pertains only to a traditional (component-based) HPCA installation:<br>On the Configuration > Live Network page, verify the following settings on the Databases tab:<br>The **Database Server** should be the hostname where the database resides. For example:<br>mydbserver.mycompany.com<br>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:<br>mydbserver.mycompany.com\HPCA<br>The **Database Name** field requires that you enter the specific database name in that instance.<br>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.<br>If SQL Server is using a dynamic port, be sure that the **Port** field in the Reporting Database Configuration section is blank. |

## EM 7.20: 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<br>`ERROR GraphElement : action threw exception: Connection to host timed out: <hostname>`<br>`ERROR GraphElement : action threw exception: Could not resolve host: <hostname>`<br>`ERROR GraphElement : action threw exception: Connection to client has been dropped`<br>`ERROR JobExecutorThread : exception in job executor thread. waiting 5000 milliseconds`<br>`ERROR DbPersistenceService : hibernate commit failed`<br>`ERROR Services : problem closing service 'persistence'`<br>`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. |

## EM 7.20: 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). |

## EM 7.20: 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:<br>`<install-dir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties`<br>Place this copy outside of the `<install-dir>` directory.<br>2. Uninstall the Enterprise Manager.<br>3. Install the Enterprise Manager.<br>4. Stop the “HP Client Automation Enterprise Manager” service by using the Services utility.<br>5. Restore the following file from the copy that you made in step 1:<br>`<install-dir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties`<br>6. Start the “HP Client Automation Enterprise Manager” service.<br>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. |

## After an upgrade, Tomcat installation of webapps/em or webapps/ope may be corrupted

| | |
|---|---|
| PROBLEM: | When you attempt to access Enterprise Manager, a 404 browser error is returned. Directories and files may be missing in the `em` and `ope` directories.<br>NOTE: This pertains only to a migration from HP Configuration Management version 5.11 to HPCA version 7.20. |
| CAUSE: | Tomcat does not always re-deploy the WAR files properly. |
| WORKAROUND: | There are two workarounds for this problem:<br>Workaround 1 — Before upgrading, stop the HP CM Enterprise Manager service.<br>Workaround 2 — If you have already upgraded, do the following:<br>1. Stop the HP Client Automation Enterprise Manager service.<br>2. Backup the `Console.properties` file located in the following directory:<br>`<`*`InstallDir`*`>/HP Openview/CM-EM/tomcat/webapps/em/WEB-INF`<br>3. Delete the `/em` and `/ope` directories from `<InstallDir>/HP Openview/CM-EM/tomcat/webapps`<br>4. Start the HP Client Automation Enterprise Manager service. Restarting the service will re-expand the application from the WAR file.<br>5. Restore the `Console.properties` file to the original directory<br>6. Restart the HP Client Automation Enterprise Manager service. This will cause the application re-read the `Console.properties` file. |

## 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:<br>The `Console.properties` file specifies the opeurl and vulnerability_management_server_url settings.<br>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 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.<br>For Internet Explorer, this setting is accessed in the Tools → Internet Options → Connections Tab → LAN Settings button. Select Bypass proxy server for local addresses.<br>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`<br>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` |

## 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:<br>Edit the following registry key:<br>`My Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings`<br>Add the following DWORD Value: `MaxConnectionsPerServer` with a Value of 8 (recommended).<br>For Firefox:<br>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). |

## Invalid context menu

| | |
|---|---|
| PROBLEM: | When using versions of the Adobe Flash Player prior to 9.0.47, if you right-click an image, an incorrect menu is displayed (options include zoom in and play). These options are not valid and should not be used. |
| CAUSE: | A bug with previous versions of Adobe Flash player. |
| WORKAROUND: | Upgrade to Adobe Flash Player version 9.0.47 or later. This will only partially fix this issue. After upgrading, the invalid context menu still appears if you right-click while a busy (clock) cursor is displayed. This has been reported as a defect and should be fixed by Adobe in a future release. |

## 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 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.<br>`+SOFTWARE/ZSERVICE < version = 1>`<br>`+SOFTWARE/ZSERVICE < version=<<in.version>> >`<br>`+SOFTWARE/ZSERVICE < version = 1> ; <<in.os>> == "XP"`<br>`Not supported syntax:`<br>`+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. |

## 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:<br>`group.processing.threads`<br>`group.processing.target.delay.ms`<br>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. |

## Firefox sometimes reports an error when nothing is wrong

| | |
|---|---|
| PROBLEM: | Occasionally, certain versions of the Firefox browser will report a Java Script error when you click the Reporting tab in the Enterprise Manager. |
| CAUSE: | Firefox-specific issue. |
| WORKAROUND: | The Enterprise Manager is functioning as designed. No workaround available. |

## 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. |

## 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. |

## 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.<br>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. |

## Communication to job process engine is not encrypted

| | |
|---|---|
| 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:<br>`http\://localhost\:8080/ope/resources,`<br>This is an unencrypted channel. |
| WORKAROUND: | Modify the `Console.properties` file, and change the `opeurl` property to: `https\://localhost\:8443/ope/resources.` |

## 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:<br>`<`*`InstallDir`*`>/nonOV/jre/b/lib/security/cm-ec.keystore`<br>`<`*`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.* |

## Keyboard navigation in the About window is broken in places

| | |
|---|---|
| PROBLEM: | In the About window, the **Close** button is not the default button. There is no way to use the **TAB** key to navigate to this button. |
| CAUSE: | The **Close** button is not set to be the default button. |
| WORKAROUND: | Click **Close** with the mouse. |

### Cannot tab to **X** button in pop-up window

| | |
|---|---|
| PROBLEM: | The **X** button to close a pop-up window cannot be accessed by using the keyboard. |
| CAUSE: | Problem with Adobe Flex versions 2.01 and 3. |
| WORKAROUND: | Press **ESC** when a pop-up window is active. To close the pop-up window, click the X with mouse. |

### 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. |

### 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. |

## Extensions for Windows Installer

There are no changes for this release.

## Inventory Manager

- **ODBC DSNs Require 32-bit Drivers**: Client Automation components running on 64-bit systems run in 32-bit emulation mode. Therefore, when using ODBC on 64-bit Windows platforms, you must create the DSN for the ODBC database using 32-bit drivers.

  On a Windows 64-bit machine, you can access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the DSNs required by our product.

## Knowledge Base Server

- Add support for posting data to a SQL Database hosted by:
  - SQL Server 2008
  - Oracle 11g, Release 1 with the latest Oracle patch set
- The product and guides were rebranded from CM KB Server to HP Client Automation KB Server for this release.

### 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. |

## Messaging Server

- **ODBC DSNs Require 32-bit Drivers**: Client Automation components running on 64-bit systems run in 32-bit emulation mode. Therefore, when using ODBC on 64-bit Windows platforms, you must create the DSN for the ODBC database using 32-bit drivers.

  On a Windows 64-bit machine, you can access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the DSNs required by our product.

- New tables or columns have been added to the SQL reporting databases to provide additional reporting capabilities. Refer to the *Messaging Server Migration Guide* for details.

### 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. |

## Multicast Server

There are no new features for this release.

## OS Manager for UNIX

- The Portal user interface has been deprecated for this release. OS Manager administrative tasks have been added to the Enterprise Manager and Core server Consoles.

### **RESOLVED** ESX 3.5 devices remain in _U_ state

| | |
|---|---|
| PROBLEM: | VMware ESX 3.5 devices remain in _U_ state |
| CAUSE: | VMware ESX 3.5 restricts functionality of the exposed Linux service OS console |
| WORKAROUND: | Resolved in version 7.50 |

### After migration to 7.2, incorrect or missing values for PORTAL_HOST and PORTAL_PORT in edmprof

| | |
|---|---|
| PROBLEM: | After migration of the HPCA Configuration Server and Database, check the PORTAL_HOST and PORTAL_PASS entries in the [MGR_ROM] section of the edmprof. |
| WORKAROUND: | When necessary, update the entries with the appropriate values for the Portal using a text editor. There is no need to restart the Configuration Server after saving the file. |

### SLES10 SP2 fails to mount for autoyast.xml file

| | |
|---|---|
| PROBLEM: | SLES10 SP2 fails to mount for autoyast.xml file |
| CAUSE: | OS Manager 7.20 does not support SLES10 SP2 |
| WORKAROUND: | none |

## OS Manager for Windows

- The Portal user interface has been deprecated for this release. OS Manager administrative tasks have been added to the Enterprise Manager and Core server Consoles.
- The USERTO and EVNTDEST attributes of the OS.BEHAVIOR class have been deprecated.
- If you want to capture a single image to deploy across both T5720 and T5730 thin client devices, the captured image must be built from a factory image for a T5730. This will ensure it contains the drivers needed for the T5730 (which are not in any of the T5720 factory images), and is backwards compatible with the T5720. Any T5730 factory image contains the utilities required to implement image expansion.
- If you want to capture an image on an XPE thin client device and deploy the image to an XPE thin client device with a larger flash drive, the image you capture must have been created using the T5720 SoftPaq build 323 (5.1.323 A 28 dated July 2006, which downloads sp33234.exe) or later.
- If you are using a T5545 Linux Thin Client you must run **`fsunlock`** before running the Image Preparation Wizard. To do this, start a new terminal window and type **`fsunlock`**.
- If you are using a T5135 Thin Client (which uses HP Thin Connect), you must expand the `/mnt` partition before installing the agent. To do this, you can use the Image Preparation Wizard media to boot the device and expand the partition. Note that this method requires an external CD-ROM.

   1. Use the Image Preparation Wizard media to boot the T5135 device.
   2. When prompted for the OS Manager server's IP address, press **Alt**+**F2** to start a new session.
   3. Type **`mount /dev/hda3 /mnt`**.
   4. Type **`cd /mnt`** to change the directory to `/mnt`.
   5. Type the following command to back up the partition: **`tar -cvf /work/mnt.tar`**.
   6. Type **`cd /`** to change to the root directory.
   7. Type **`umount /mnt`** to unmount the `/mnt` directory.
   8. Type **`fdisk /dev/had`** to repartition /dev/hda3.
   9. Respond to each prompt with the following values (in bold):

      a. Command (m for help): **d**

      b. Partition number (1-4): **3**

    c Command (m for help): **n**

    d Command action e extended p primary (1-4): **p**

    e Partition number (1-4): **3**

    f First cylinder (36-62, default 36): **Enter**

    g Last cylinder or +size or +sizeM or +sizeK (36-62, default 62): **Enter**

    h Command (m for help): **w**

10. Type **`mkfs.ext2 /dev/hda3`** to create a file system on `/dev/hda3`.
11. Type **`mount /dev/hda3 /mnt`**.
12. Type **`cd /mnt`** to change the directory to `/mnt`.
13. Type **`tar -xvf /work/mnt.tar`** to restore the partition.
14. Type **`cd /`** to change the directory to `/`.
15. Type **`umount /mnt`** to unmount the `/mnt` directory.
16. Remove the Image Preparation Wizard CD-ROM.
17. Reboot the device.

- Before running the Image Preparation Wizard on a T5135 Thin Client (which uses HP Thin Connect):
    1. Delete the `Computer Name` line in `/etc/configedit/config.ini`.
    2. Install the HPCA agent.
    3. From the HP Thin Connect console, click **Settings**, go to the **Management** tab and select the **Start Altiris** check box to ensure the agent starts after the device is restarted.
- The following functionality is not supported on thin clients:
    - Hardware Configuration Management
    - Defining Drive Layouts
    - Multicast
    - Modifying the hostname (getmachinename.tcl)
    - Install OS from cache partition
    - Install OS from CD or DVD
    - Sysprep
    - Image PIC compatibility

  It is important to be aware of this because the interface for these features has not been disabled. If you use these features, they will be ignored or produce unpredictable results on a thin client device.
- If you will be publishing .WIM files, you must install the Microsoft **Windows Automated Installation Kit** (**WAIK**) to the default location on the C:\ drive of the device that will be used to publish the operating system resources. WAIK is available from the Microsoft web site. It is not included as part of a standard Vista installation.
- OS Manager does not support agents that are connecting simultaneously with multiple NIC cards unless the OS Manager infrastructure can be reached through any available link.
- If you encounter extremely slow OS image downloads to your target devices, you can modify the Proxy Server configuration to allow you to tune downloads based on your environment. To enable tuning, add the following section to the Proxy Server's `httpd.rc` file.

*Do not change* the **buffering** value.
Enter the information exactly as shown; all parameters and string values are case sensitive.

```
Overrides Httpd {
  bufsize 16384
  buffering full
}
```

The default value for **bufsize** is 32768. Lowering it to 16384 may increase performance. Experiment with different values to optimize the throughput in your environment.

Using the Apache Proxy server (as opposed to the Legacy HPCA Proxy Server) will also result in faster downloads to target devices.

- **Notes**
  - When using `ImageDeploy.iso`, use of `netif` setting in `romsinfo.ini` is not supported under WinPE SOS.

## **RESOLVED** Publisher might show wrong file size in summary panel

| | |
|---|---|
| PROBLEM: | When publishing a `.wim` file, the size might display as "0" in the summary panel. |
| CAUSE: | Publisher fails to calculate total file size correctly in some cases. |
| WORKAROUND: | Fixed in version 7.50. |

## **RESOLVED** File copying from WNI image may fail on deployment

| | |
|---|---|
| PROBLEM: | Deploying a pre-Vista Windows operating system from a WNI image may fail during the step that copies Windows system files from the image to the system drive during setup. |
| CAUSE: | The allocated system drive is too small to fit all files that are copied from the WNI deployment image to that drive. The size of the system drive should be at least 3 GB or 2 times the size of the WNI image itself. If the WNI image size is too small, a system drive is created with insufficient space to copy the install files from the WNI image to the system drive. |
| WORKAROUND: | Fixed in version 7.50. |

## **RESOLVED** Assigning OS Policy via subnet location is not supported on WinCE thin clients

| | |
|---|---|
| PROBLEM: | Inability to use subnet location for policy resolution for OS deployments on WinCE thin clients. |
| CAUSE: | The subnet value in the SMINFO object is not properly captured by the HPCA agent. |
| WORKAROUND: | Resolved in version 7.50. |

## **RESOLVED** “Boot steering failed" message appears when WinPE SOS runs

| | |
|---|---|
| PROBLEM: | On internationalized platforms, such as Traditional Chinese, deploying Windows based images from the WinPE service OS may fail if the system initially booted into the Linux service OS.<br>This may happen if the Linux service OS is unable to deploy the OS service (for example, a .WIM image that must be deployed by WinPE). Any image deployment or hardware configuration element that references an internationalized OS service name or hardware configuration (LME) name which must be handled under the WinPE service OS requires that the system boot into the WinPE service OS first to identify and handle the internationalized OS or Hardware Configuration object name. |
| CAUSE: | The XML document that includes the Hardware Configuration Element (LME) and OS service names, provided with the CA infrastructure, is not encoded consistently when switching between the WinPE service OS and the Linux service OS. |
| WORKAROUND: | Resolved in version 7.50. |

## 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) |
| WORKAROUND: | Refer to the Thin Client Agent installation instructions in the *Application and Application Self-service Manager Guide*. |

## 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/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. |

## CAE75-I18N: can't get to desired 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. |

## 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. |
| 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.<br>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. |

## Prepwiz remote capture feature should be configurable

| | |
|---|---|
| PROBLEM: | Imagex/WinSetup capture requires downloading the SOS to capturing machine even if the ImageCapture.iso is being used. |
| CAUSE: | As a result of the Remote Capture capabilities introduced in 7.5 for ImageX/WinSetup images, booting the SOS from the local capture CD/DVD (ImageCapture.iso) is not available. |
| WORKAROUND: | None. |

## 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. |

## Localized message catalogs for Chinese, Japanese, and Korean not supported under LinuxSOS for HPCAS

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

## Fail to set keyboard mapping with fr in WinPE SOS

| | |
|---|---|
| PROBLEM: | For WinPE Service OS, setting keyboard is only supported with product versions which support "de" and "fr" completely; that is, provide "de_DE" and "fr_FR" message catalogs. The OS.BEHAVIOR instance attribute, KBDMAP is not supported. |
| WORKAROUND: | To switch keyboard and messages, the OS.BEHAVIOR attribute LANG needs to be used. 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.<br>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.<br>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. |

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

## 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 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. |
| WORKAROUND: | Manually delete or rename the existing OS image file in the upload folder. |

## RCS for ROM service created in 4.2 does not work in 7.20

| | |
|---|---|
| PROBLEM: | When the Portal is migrated from version 4.2 to version 7.20, the RCS for ROM service no longer works. |
| WORKAROUND: | Log in to the Portal as the romadmin. Delete the RCS for ROM service from the desktop. Go to Zone, Configuration, Configuration Servers, HPCA Database, and click the Add Desktop Shortcut icon. |

## Winpe.wim does not include VMware NIC driver

| | |
|---|---|
| PROBLEM: | `Winpe.WIM` does not include VMware drivers. |
| CAUSE: | `Winpe.WIM` provided in the CM OS Manager does not include network drivers used in VMware. |

## 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. |
| 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. |

## No Windows volumes detected when installing Vista from DVD in UDF format

| | |
|---|---|
| PROBLEM: | When using the ImageDeploy.iso, if you select the Install OS from CD/DVD option under WinPE, a `No Windows volumes detected` error might appear. |
| CAUSE: | The CD/DVD has UDF format. |
| WORKAROUND: | Re-create the CD/DVD without using UDF. |

## Migrating Infrastructure components from 4.2, OS Manager connect fails

| | |
|---|---|
| PROBLEM: | When migrating CM infrastructure components from 4.2 to 7.2, the 4.2 agent is unable to perform an OS Manager connect and it will fail. |
| CAUSE: | Migration/backward incompatibility between CM infrastructure 7.2 and CM agent 4.2 OSM client method. |
| WORKAROUND: | Migrate agent to version 7.2 and then perform an OS Manager connect. |

## 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. |

## 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 |

### 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:<br>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<br>2. Stop the Configuration Server service if it is running.<br>3. Open a command prompt and change the directory to <Configuration Server install directory>\bin.<br>4. Run the following command:<br>ZEDMAMS VERB=IMPORT_INSTANCE,FILE=os.xpi,XPR=os.xpr,TIME=OLD,PREVIEW=NO, DUPLICATES=MANAGE,CONTINUE=YES,REPLACE=YES |

## Hardware Configuration Management

No changes for this release.

# Patch Manager

HPCA Enterprise (Classic)

- **Patch Manager Administrator**:
  - The streamlined user interface is simpler to navigate and adds online help and an online guide.
  - Tasks are re-grouped into areas for: Configuration, Operations, and Status and Logs.
  - Configuration tasks are grouped into Environment Settings, Acquisition Settings, and Acquisition Jobs.
  - Online Help is available from the help button at the top-right of the Patch Manager Administrator pages. Online help opens a separate window that allows you to browse or search the help topics and online guide.
  - New tasks include the ability to view logs online.
- This release supports Patch Management on devices running Windows and Linux operating systems.
  - Support for RedHat versions have changed. Support for RedHat versions 2.1 and 3 is dropped and support for RedHat versions 5 and 5.3 are added.
  - Support for SuSE versions have changed. SuSE 8 support is dropped. SuSE 10 support is added for both SuSE Linux Enterprise Desktop (SLED) and SuSE Linux Enterprise Server (SLES).

  ⚠ HPCA Patch Management does not validate that Novell’s SuSE10 license or registration policy is met. It is the customer’s responsibility to adhere to Novell’s policy and have their SuSE10 machines registered with validated licenses.

- This release no longer supports Patch Management on devices running HP-UX or Solaris operating systems.

- This release adds the Patch Agent option for the Download Manager. This new capability allows for the transfer of content required to apply the designated patches to a managed device outside of the usual HPCA Agent connection process. The transfer process occurs passively as per the configured constraints. For more information refer to the topics in the *HPCA Patch Manager Installation and Configuration Guide*.
- **Reports and Dashboards**:
  - Dashboards for Patch Management are available from the Enterprise Manager, Dashboards tab. For details, refer to the *HPCA Enterprise Manager User Guide*.
  - Patch Management Reporting Server reports display quickly. Backend processing and table modifications in this release support quick rendering of reports for large enterprises.
  - Executive Summaries are new and offer four snapshots of patch compliance that allow you to drill down into detail reports.
  - Compliance Reports include new and modified reports. Three reports: Patch Status, Product Status, and Release Status, require version 7.50 of the Patch Agent in order to be populated. If you do not migrate your agents to version 7.50, the reports will show zero records.
  - For Patch Report details, refer to the "Assessment, Analysis and Reports" chapter of the *Patch Manager Installation and Configuration Guide* or Patch Manager Administrator online help.
- **ODBC DSNs Require 32-bit Drivers**: Client Automation components running on 64-bit systems run in 32-bit emulation mode. Therefore, when using ODBC on 64-bit Windows platforms, you must create the DSN for the ODBC database using 32-bit drivers.

  On a Windows 64-bit machine, you can access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the DSNs required by our product.

## **RESOLVED****CM 5.11:** Patches for some entitled bulletins on Red Hat Enterprise Linux 5 x86-64 systems fail to install

| | |
|---|---|
| PROBLEM: | On Red Hat Enterprise Linux 5 x86-64 systems, patches for some entitled bulletins fail to install. |
| CAUSE: | Some bulletins for Red Hat Enterprise Linux 5 x86-64 operating systems include Red Hat Package Manager (RPM) packages in both x86 and x86-64 architecture variants. For these bulletins, Patch Manager is installing only one of the architecture variants, which causes the verification to fail. |
| WORKAROUND: | Resolved in Version 7.20. |

## **RESOLVED** After migrating from Version 3.0.3 to 7.20, some Patch Reports show incorrect number of applicable products

| | |
|---|---|
| PROBLEM: | In the Reporting Server, the Patch Manager reports for "Compliance by Device" and "Simplified Compliance by Device" show an incorrect total in the applicable products column. However, when the number is clicked to show the products, the applicable products are listed correctly. |
| CAUSE: | This is a known issue after migrating from Patch Manager 3.0.3 to Patch Manager 7.20. |
| SOLUTION: | Resolved in HPCA 7.50. |

## Patch Agent Option: 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:<br>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 Agent Option: 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 Agent: 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:<br>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.<br>2. The fix information for `nvdkit` will be posted to the Agent Update Information page. |

## 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 Reports: 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. |

## Policy Server

No changes for this release.

## Portal

- The Portal user interface has been deprecated for this 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.

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.

- The *Portal Installation and Configuration Guide* (*Portal IC Guide*) was updated to remove all references to the Portal *user interface* and *tasks*. Topics currently in the guide include installation, OpenLDAP Directory Service and Portal Zone details, configuration options, and troubleshooting topics.
- The following Portal configuration parameter (`rmp.cfg`) was added to the Portal IC Guide.
  - WS_TOKEN_TTL – Portal Web Services session timeout parameter.

### Documentation Correction

- The *Managing the Portal Web Services Token* topic in the Troubleshooting chapter includes a reference to the “Core Console.” This is an error as the Core Console does not use the WS_TOKEN_TTL parameter to control its session timeout period.

  **Replace**: “During normal usage of the Enterprise Manager Console or Core Console the token is routinely refreshed.”

  **With**: “During normal usage of the Enterprise Manager Console the token is routinely refreshed.”

### Portal Migration: 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.<br>Or<br>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 Migration 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. |

### 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.<br>or<br>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 Server

- Table 1 lists all supported operating systems for the Proxy Server in this release.

### 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. |

### Proxy Server preload using SSL TCPS is not supported on AIX and Solaris operating systems

| | |
|---|---|
| PROBLEM: | SSL functionality is not supported on the AIX and Solaris operating systems. As a result, Proxy Server preloading using SSL TCPS will not work on these operating systems. |
| CAUSE: | N/A; SSL support on AIX and Solaris has never been supported. |
| WORKAROUND: | There is no work-around for this issue.<br>Proxy Server pre-loading using SSL TCPS is restricted to Windows and Linux operating systems. |

### Proxy server preloading using multicast does not work in UNIX/Linux

| | |
|---|---|
| PROBLEM: | Proxy server preloading using multicast does not work in UNIX/Linux.<br>The SUSE connect log contains the following error:<br>`Error opening control object [MULTCAST] in  [/opt/HP/CM/IntegrationServer/etc/rps/]`<br>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. |

## Reporting Server

- Added Compliance Management report packs.

### **RESOLVED** After migrating from Version 3.0.3 to 7.20, some Patch Reports show incorrect number of applicable products

| | |
|---|---|
| PROBLEM: | In the Reporting Server, the number of applicable products that are displayed on the "Compliance by Device" and "Simplified Compliance by Device" views are incorrect. However, when the number is clicked to show the products, the applicable products are listed correctly. |
| WORKAROUND: | This issue was resolved in version 7.50. |

## Security and Compliance Manager

In addition to Vulnerability Management (introduced in HPCA version 7.20), HPCA now offers Compliance Management and Security Tools Management capabilities. This feature set includes:

- Expansion of the HP Live Network subscription service to include regularly updated **Security Content Automation Protocol** (**SCAP**) data streams for client configuration, an SCAP-certified compliance scanner, and a security tools management scanner.
- Ability to scan client devices for compliance with configuration standards defined in SCAP format, such as the **Federal Desktop Core Configuration** (**FDCC**) benchmarks.
- Ability to scan client devices to determine:
  - Which anti-virus, anti-spy ware, and firewall tools are installed and enabled on each device
  - How recently the virus and spy ware definitions were updated on each device
  - How recently each device was checked for viruses and spy ware

- Introduction of the Compliance Management and Security Tools Management reports. These new reports enable you to review existing compliance content and the results of scans performed in your environment. The following types of reports are available:
  - Executive Summaries for quickly identifying high risk areas
  - SCAP Reports for viewing and assessing the available SCAP benchmarks and rules
  - Product Reports for viewing information about the specific anti-virus, anti-spy ware, and firewall products detected in your environment
  - Device Reports for viewing device compliance and security tools issues in detail
- Enhancements and updates to the HPCA Enterprise Console (the Enterprise Manager in a traditional component-based installation). This includes:
  - New Compliance Management dashboard
  - New Security Tools Management dashboard
- Enhanced configuration and operations support for the HP Live Network subscription service in an HPCA environment. This includes setting up access to the HP Live Network service, establishing when data should be pulled from HP Live Network, and establishing where this data should be placed for use within an HPCA deployment.
- New troubleshooting capabilities that enable you to test your HP Live Network configuration settings before you save them.

Some Enterprise Manager known issues also pertain to the Security and Compliance Manager. See Enterprise Manager on page 40 for details.

## Windows Terminal Server and Citrix Support

No changes for this release.

# 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.