# HP Client Automation Enterprise

# OS Manager

for the Windows® operating system

Software Version: 7.20

## System Administrator User Guide

Manufacturing Part Number: None

Document Release Date: September 2008

Software Release Date: July 2008

# Legal Notices

## Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notices



## Trademark Notices

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.

DHTML Calendar

# Documentation Updates

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

- Software Version number, which indicates the software version.
  - The number before the period identifies the major release number.
  - The first number after the period identifies the minor release number.
  - The second number after the period represents the minor-minor release number.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

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

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

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

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

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

Table 1 indicates changes made to this document.

**Table 1 Document changes**

| Chapter | Version | Changes |
|---|---|---|
| All | 5.10 | General edits.<br>Fixed outdated references. |
| All | 7.20 | General edits and rebranding.<br>Removed version number for WinPE.<br>Added cautions regarding Core and Satellite environments. |
| Chapter 1 | 5.10 | Reworked chapter. |
| Chapter 1 | 5.11<br>March 2008 | Added note on page20. |
| Chapter 1 | 7.20 | Added information about the HP Client Automation Mini Management Server to OS Manager Components on page 21. |

| Chapter | Version | Changes |
|---|---|---|
| Chapter 1 | 5.10 | Added note on page 25. |
| Chapter 1 | 7.20 | Changed the note under Machine 2 in Image Deployment Server Architecture on page 26. |
| Chapter 1 | 5.10 | Modified the steps in Using the HP Client Automation OS Manager on page 28 to account for situations where you may use `.WIM` files. |
| Chapter 1 | 5.10 | Added Provisioning Target Devices on page 28. |
| Chapter 1 | 7.20 | Updated version number in Product Media on page 29. |
| Chapter 1 | 5.10 | Added definition for Service Operating System (Service OS) to Terminology on page 32. |
| Chapter 2 | 5.10 | Changed from Target Requirements to Requirements. |
| Chapter 2 | 7.20 | Added information about thin clients in Target Devices on page 36. |
| Chapter 2 | 7.20 | Removed list of operating systems in Server on page 36. |
| Chapter 2 | 7.20 | Added Firewall Settings for Windows XPe Thin Client Devices on page 38. |
| Chapter 2 | 7.20 | Added Installing the Application Manager on Thin Clients on page 39. |
| Chapter 3 | 7.20 | Updated the Prerequisites on page 44. |
| Chapter 3 | 5.10 | Updated the Installation Checklist on page 45. |
| Chapter 3 | 5.10 | In Installing the OS Manager Server on page 46, added information about utilities necessary to capture images to be deployed by ImageX. |
| Chapter 3 | 7.20 | Updated name of log in the note on page 46. |
| Chapter 3 | 5.10 | In the Prerequisites on page 50 for the Boot Server, added information to a note about the types of editors to use to modify the Boot Server's configuration files. |
| Chapter 3 | 7.20 | Added Installing the Client Automation Mini Management Server on page 57. |
| Chapter 3 | 5.10 | Added Converting the Service OS to WinPE (optional) on page 58. |

| Chapter | Version | Changes |
|---|---|---|
| Chapter 4 | 5.11 March 2008 | Added information about capturing Windows Server 2008 operating systems. |
| Chapter 4 | 5.11 March 2008 | In Deployment Methods on page 62, removed Windows NT 4 x86 as a supported platform. Microsoft no longer supports this product. |
| Chapter 4 | 5.11 March 2008 | In Deployment Methods on page 62, updated Vista versions and added Windows Server 2008 versions supported. |
| Chapter 4 | 7.20 | Updated Deployment Methods on page 62. |
| Chapter 4 | 7.20 | In Capturing pre-Windows Vista Operating Systems for Legacy Deployment on page 64, modified the note in task 2. |
| Chapter 4 | 7.20 | In Capturing pre-Windows Vista Operating Systems for ImageX Deployment on page 66, modified the note in task 2. |
| Chapter 4 | 7.20 | Added a task Copy utilities to the HPCA OS Manager Server to Capturing Windows Vista Operating Systems for ImageX Deployment on page 67 and Capturing Windows Vista Operating Systems for Windows Setup Deployment on page 76. |
| Chapter 4 | 5.11 March 2008 | In Using the HP Client Automation OS Manager Image Preparation Wizard on page 81, combined the list of files uploaded for both ImageX and WinSetup. |
| Chapter 4 | 7.20 | Updated To use the HPCA OS Manager Image Preparation Wizard on page 82. |
| Chapter 4 | 7.20 | Added Preparing and Capturing Thin Client OS Images on page 88. |
| Chapter 5 | 5.11 March 2008 | In Prerequisites for publishing .WIM images of a Windows Vista OS on page 100, modified information about the /sources directory. |
| Chapter 5 | 5.10 | In Using the Admin Publisher on page 104, added information about support for publishing `.WIM` files. |
| Chapter 5 | 5.11 March 2008 | In Using the Admin Publisher on page 104, added a caution about the deployment method to be selected. |

| Chapter | Version | Changes |
|---|---|---|
| Chapter 5 | 7.20<br>August 7, 2008 | In Using the Admin Publisher on page 104, modified step 5. |
| Chapter 5 | 7.20 | In Using the Admin Publisher on page 104, modified step 8a. |
| Chapter 5 | 7.20<br>August 7, 2008 | In Using the Admin Publisher on page 104, modified step 11. |
| Chapter 6 | 7.20 | Added a note about thin client limitations on page 108. |
| Chapter 6 | 7.20 | Updated description for PMINITL on page 127. |
| Chapter 6 | 5.10 | Updated information in Adding Devices on page 147. |
| Chapter 6 | 7.20 | Added a note about the command line for Windows CE on page 152. |
| Chapter 7 | 7.20 | Updated graphics. |
| Chapter 10 | 5.10 | Updated prerequisites and added information about a new menu used to select the Service OS in Restoring Operating Systems on page 198. |
| Chapter 10 | 7.20<br>Sept. 2, 2008 | Updated first paragraph and added a note to Restoring Operating Systems on page 198. |
| Chapter 10 | 5.10 | Updated the requirements for Using HPCA Client Operations Profiles with OS Manager on page 203. |
| Chapter 12 | 5.10 | Added chapter Building a Custom WinPE Service OS on page 205. |
| Chapter 12 | 7.20 | Building a Custom WinPE Service OS on page 205 no longer has separate instructions for earlier versions. |
| Chapter 12 | 5.11 | Modified chapter Building a Custom WinPE Service OS on page 205 to have separate instructions for version 5.10 and 5.11. |
| Chapter 12 | 5.11<br>March 2008 | In the 5.11 section under Building a Custom WinPE Service OS on page 205, the filename for `winpe_i18n.wim` was changed to `winpe_cjk.wim`. |

| Chapter | Version | Changes |
|---|---|---|
| Chapter 12 | 5.11<br>March 2008 | In the section Changing the Locale on page 214, corrected the section in the sample default file to say [_SVC_LINUX_] from [SVC_LINUX]. |
| Chapter 13 | 7.20 | Updated Troubleshooting on page 217. |
| Chapter 13 | 5.10 | Updated description of osclone.log on page 219. |
| Chapter 13 | 5.10 | Added topic Locating the Payloads on page 219. |
| Appendix A | 7.20 | Updated AppEvents table. |

# 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 an active support contract. To find more information about support access levels, go to the following URL:

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

To register for an HP Passport ID, go to the following URL:
**http://h20229.www2.hp.com/passport-registration.html**

# Contents

# 1 Introduction

At the end of this chapter, you will:

- Understand the purpose and benefits of the HP Client Automation OS Manager.
- Know what operating systems are supported.
- Be familiar with the OS Manager components.
- Be familiar with key terminology.
- Have a high level understanding of the product architecture.
- Understand how target devices are provisioned.

The HP Client Automation OS Manager uses policy-driven, real-time, state-based management so you can configure and deploy operating systems (OSs). Use the OS Manager to install or replace operating systems on a device and maintain the device according to policy. The OS Manager ensures the installation of the appropriate operating system based on the targeted device's capabilities. For example, an image built for a computer with an ACPI BIOS will not be delivered to a computer that lacks an ACPI BIOS.

The OS Manager offers tools so that you can create images of operating systems that you have prepared on a reference machine or use the native installation media of the operating system. Policy determines the operating system that is most appropriate for a particular target device based on:

- An asset tag or other unique identifier that is embedded in the device's BIOS.
- The network segment to which the device is connected.
- The manufacturer of the device.
- The model of the device.
- The role of the device in your IT infrastructure.

Criteria are extensible; you can add to this list.

HP tests OS Manager to ensure compatibility with a wide range of HP devices and select devices from other manufacturers. Each version of the OS Manager is developed using tools that support technologies available at the time of release. In certain situations, adding support for new devices to earlier versions of the OS Manager is not feasible due to various factors, including introductions of new hardware technologies, availability of hardware device drivers and general product enhancements. HP makes a reasonable effort to support customers' existing environments, but customers may be required to upgrade OS Manager in order to be able to provision and manage new hardware devices.

# Using this Guide with Core and Satellite Servers

If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

# Product Overview

## Benefits of the OS Manager

The OS Manager:

- Is a fully integrated component of the HP Client Automation solutions, which reduces the learning curve for your administrators.
- Uses policy-based management to improve the speed and reliability of OS deployment.
- Maintains operating system configurations using desired-state management.
- Reduces IT costs by simplifying and streamlining the OS management process across multiple platforms.

## OS Manager Components

The OS Manager consists of the following components.

- **Boot Server** is a Windows-based PXE server and TFTP server.

Open Source PXE Server and TFTP Server are provided “as is” as defined by the Open Source Licensing model. These components are not maintained by HP; HP is not responsible for any defects related to them.

Open Source PXE Server and TFTP Server are provided for use in two cases:

- QA\testing in a pre-production environment
- Image capture on an isolated network

HP recommends that you work with your network specialists to use the most appropriate PXE and TFTP server, based on your network environment constraints.

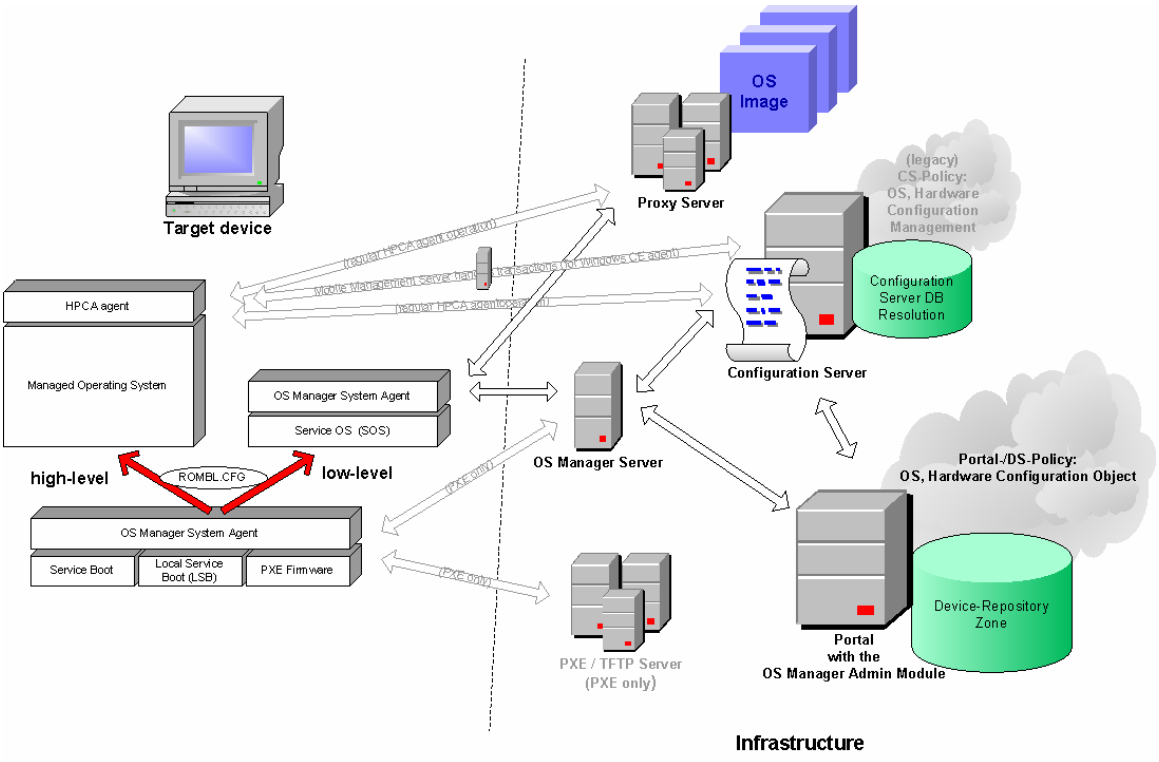
- **ImageDeploy.ISO** .initiates the HP Client Automation OS Manager System Agent if you encounter a non-PXE deployment or a disaster-recovery situation.
- **Local Service Boot (LSB)** is a typical service, stored in PRIMARY.OS.ZSERVICE, which is deployed by the HP Client Automation agent to the OS. It must be deployed to target devices that will use Local Service Boot for OS management.
- **HP Client Automation Application Manager** is the agent that runs in the operating system of the target device and is used to manage service packs, patches, hot fixes, applications, and other content. It also works with the HP Client Automation OS Manager Boot Loader and the HP Client Automation OS Manager System Agent to enable management of the operating system according to policy.
- **HP Client Automation Configuration Server** provides policy resolution services to determine the desired state of managed devices. The OS Manager runs a secondary resolution process against the HP Client Automation Portal to determine device-specific and external (directory service [DS]) policy. Refer to the *HP Client Automation Enterprise Configuration Server User Guide* for more information.
- **HP Client Automation Configuration Server Database** stores policy definition or links to an external policy store. The HPCA Configuration Server DB also contains OS packages for operating system images, supporting master boot record files and partition table files, which have been prepared and published with the HP Client Automation OS Manager Image Preparation Wizard.

- **HP Client Automation OS Manager Admin Module** is the OS Manager graphical user interface that is accessed through the HP Client Automation Portal.
- **HP Client Automation OS Manager Boot Loader** receives control when the managed device boots from the network via PXE. It then determines how to continue the boot process. It can either continue to boot to a currently in-state operating system that is located on the managed device's system drive or it can continue the boot procedure by loading the HP Client Automation OS Manager System Agent from the Boot Server's TFTP server.
- **HP Client Automation OS Manager Server** is an NVDKIT-based web server that communicates with the Configuration Server through TCP/IP. It mediates between the OS Manager and the Configuration Server to resolve policy for the correct operating systems for the managed device.
- **HP Client Automation OS Manager System Agent** is a low-level agent that runs in the **Service Operating System** (SOS) and which initiates policy resolution on the Configuration Server through the OS Manager Server, and determines which operating systems qualify for installation on the managed device.
- **HP Client Automation Mini Management Server** handles transactions between the agent and the HPCA Configuration Server when using Windows CE.
- **HP Client Automation Portal** stores information about the target devices in your environment. OS Manager-specific information is stored in the ROMS object in the target device's object. For general information on how to use the Portal, refer to the *HP Client Automation Enterprise Portal Installation and Configuration Guide*.
- **HP Client Automation Proxy Server** is an NVDKIT-based web server that serves OS deployment resources (primarily image files) to the OS Manager System Agent. You can place Proxy Servers strategically within your network infrastructure to optimize bandwidth utilization. Refer to the *HP Client Automation Enterprise Proxy Server Installation and Configuration Guide*.
- **PXE** is a network boot technology that initiates the OS Manager System Agent over the network.
- **ROMBL.CFG** is a configuration file in which the OS Manager Boot Loader stores state information. If this file exists on the target device, the device is considered under OS management and an HP Client Automation agent connect has occurred.

- **Service OS (SOS)** boots as an “in memory only” service OS without any dependency on persistent storage configuration or availability.

Figure 1 below illustrates the OS Manager components.

**Figure 1 OS Manager Components**




## Product Architecture

OS Manager comes with several tools to capture and prepare operating system images and then a group of Client Automation servers to deploy these images to target devices. Its architecture is divided into three areas: target devices, image preparation, and image deployment.

### Target Devices

Target devices are machines on which you want to apply operations or install, replace, or update an operating system.

## Image Preparation Architecture

HP provides two tools with which to capture the image of your operating system.

If you are using an existing .WIM (Windows Imaging Format) or are creating one using the System Information Manager (SIM) tool, you do not need to use the OS Manager's tools to capture the image.

- **HP Client Automation OS Manager Image Preparation Wizard**
  Use the HPCA OS Manager Image Preparation Wizard to prepare an image on the reference device. When you run the wizard, it creates an image that is sent to the OS Manager's `\upload` directory (by default *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload`). Then, use the HP Client Automation Administrator Publisher to promote the image to the Configuration Server DB.
- **HP Client Automation Windows Native Install Packager**
  Use the HP Client Automation Windows Native Install Packager to create an image of the installation media for an operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the Application Manager. The image is sent to the OS Manager's `\upload` directory (by default *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload`) and use the Publisher to promote the image to the Configuration Server DB.

  Do not use this tool if you want to create a .WIM image.

  See Preparing and Capturing OS Images on page 61 for additional information.

When you have an image file, use the Publisher to store the image in the Configuration Server DB.

**HP Client Automation Administrator Publisher**
Use the Publisher to store the image and its associated files in the Configuration Server DB. You can also use the Publisher to publish other files—such as override `Sysprep.inf` files or `unattend.txt` files—to the SYSPREP class in the Configuration Server DB. See Preparing and Capturing OS Images on page 61.

After publishing the image, prepare to deploy the image to your target devices.

## Image Deployment Server Architecture

The deployment architecture is comprised of a set of servers designed to manage and deploy operating systems to target devices based on a set of criteria. Typically, you need three server machines.

### Machine 1

- DHCP Server

  The target device uses a DHCP server to obtain an IP address. You can easily implement OS Manager in an existing DHCP-enabled network. There is no need to install additional DHCP servers.

### Machine 2

- OS Manager Server

  It is strongly recommended that you install the HPCA OS Manager Server on a machine separate from the Portal in order to obtain the best performance. It is always better to have a single server on a machine to avoid networking and performance issues.

- HP Client Automation Configuration Server
- HP Client Automation Proxy Server
- HP Client Automation Portal

  You can also install the Publisher on this machine.

See Installing and Configuring the Server Architecture on page 43.

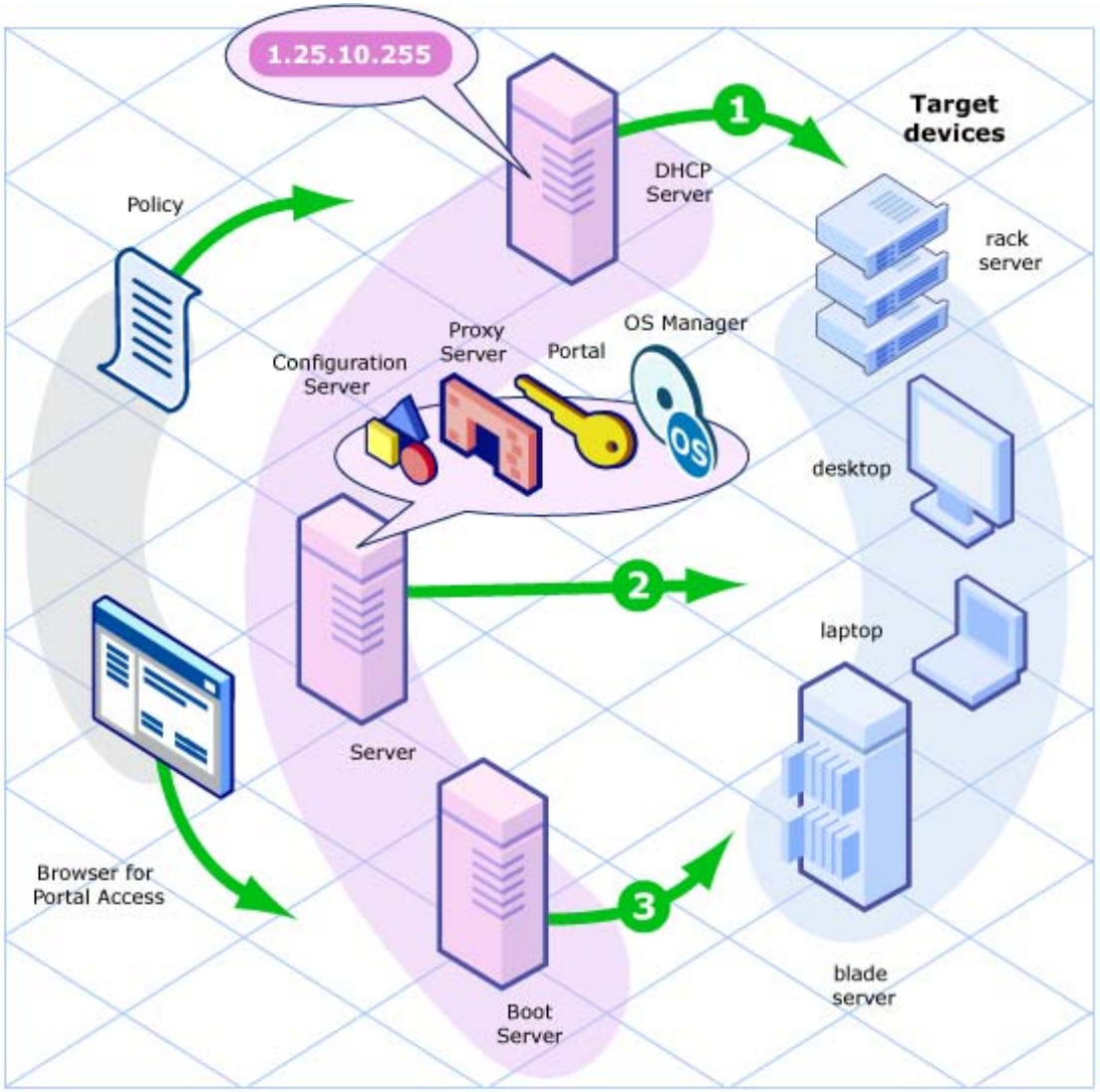
### Machine 3

- Boot Server (PXE/TFTP servers)

  Do not install the Boot Server on the same machine as your DHCP server. See About the Boot Server on page 50.

Figure 2 below illustrates the deployment architecture.

**Figure 2 Client Automation OS Manager deployment architecture**



## Using the HP Client Automation OS Manager

The following is a simple, high-level description of how you would use the OS Manager to deploy operating systems.

1. If you have an existing `.WIM` file or create one using Windows **System Image Manager** (SIM), skip to step 4.
2. If you need to create an image, determine the deployment method to be used and then use the appropriate tool to create the image. See Preparing and Capturing OS Images on page 61.
3. After you create the image, it is stored on the OS Manager Server.
4. Use the Publisher to publish the image files from the OS Manager Server to the Configuration Server DB.
5. Use the Portal to perform administrative tasks and define policy in preparation for deploying gold images to your target devices.
6. After deploying images to the target devices, use the Portal to review the state of your OS deployment.

## Provisioning Target Devices

The OS Manager can apply operations and deploy operating systems to target devices as determined by policy. To initiate the process, boot the target device:

1. from the network (PXE boot). See Implementing the HPCA OS Manager Server in your Environment on page 153 for details.
2. from a CD/DVD (ImageDeploy media). See Restoring Operating Systems on page 198 for details.
3. using Local Service Boot. You cannot use this for bare metal machines. See Implementing the HPCA OS Manager Server in your Environment on page 153 for details.

After the device boots, the OS Manager System Agent runs under the Service Operating System (SOS) that is specified by the OS Service or the **Hardware Configuration Element** (HWCE) to determine what actions to take on the target device. The target device may need:

- An operating system installed if no file system, boot partition, or master boot record is found.

- To be brought under management by the OS Manager if no `rombl.cfg` is found. See Bringing Machines under Management on page 137.
- Low level operations applied if there are Hardware Configuration Objects configured and resolved by policy. Hardware Configuration Objects contain HWCEs. HWCEs represent management functionalities. Refer to the *HP Client Automation Enterprise OS Manager Hardware Configuration Management Guide* for more information.

Depending on the needs of the target device, the service operating system may switch to a different SOS in order to support the operations that are taking place.

The switching of Service Operating Systems is called boot steering.

## Product Media

In order to install the product, you must use the OS Manager 7.20 media. Before you begin, you may want to create two additional CD/DVDs:

- Go to `iso\ImageCapture.iso` in order to create the media used to create images.
- Go to `iso\ImageDeploy.iso` in order to create the media used to restore an image.

# Document Overview

## Chapter Summary

This section includes a list and a brief description of the chapters in this guide.

### Chapter 2, System Requirements

This chapter describes requirements for your target devices.

## Chapter 3, Installing and Configuring the Server Architecture

This chapter describes how to install and configure the various components for operating system management.

## Chapter 4, Preparing and Capturing OS Images

This chapter describes how to prepare and capture operating system images for deployment to devices in your environment.

## Chapter 5, Publishing to the HP Client Automation Configuration Server Database

This chapter describes how to publish your image to the Configuration Server Database.

## Chapter 6, Operational Overview

This chapter provides information on how to use the OS Manager and Portal to prepare your operating system (OS) images for deployment to target devices.

## Chapter 7, Implementing the HPCA OS Manager Server in your Environment

This chapter describes implementing the OS Manager Server in your environment.

## Chapter 8, OS Manager Support for HP Blades

This chapter describes how to assign policy based on enclosures, racks, slots, and enclosure configurations.

## Chapter 9, Multicast and the OS Manager

This chapter describes how the OS Manager supports reliable delivery multicast so that you can concurrently rollout large numbers of OS images with improved performance.

### Chapter 10, Advanced Features

This chapter describes several advanced features that are available with the OS Manager.

### Chapter 11, Building a Custom WinPE Service OS

This chapter describes the HP script that allows you to customize your WinPE Service OS.

### Chapter 12, Double Byte Character Support

This chapter describes the changes that have been made to the OS Manager for internationalization.

### Chapter 13, Troubleshooting

This chapter provides information about the logs, various tests that you can run, and other troubleshooting information.

### Appendix A, AppEvents

This appendix describes the AppEvents stored in the ROM object.

### Appendix B, User Messages

This appendix lists the messages that a user may see.

### Appendix C, Storing Multiple Logs

This appendix describes how to store multiple logs per machine on the OS Manager Server.

## Related Documents

*HP Client Automation Enterprise OS Manager Hardware Configuration Management System Administrator Guide*

# Terminology

This section provides a description of generic and Client Automation-specific operating system management terms. Review these terms in order to better understand the concepts that are discussed in this guide.

### bare metal machine

A device that does not have a local OS installed.

### HP Client Automation agent

The software that runs on a target device and communicates with the Configuration Server.

### HP Client Automation OS connectt

An HPCA agent connect that is performed for the OS Manager. The dname parameter in the Run Once command is set to OS to specify that this connection is being performed for the OS Manager.

### device object

An object stored in the Portal that contains information about a target device.

### discovery

The process of a target device booting and communicating with the infrastructure to determine whether a ROM object exists.

### gold image

A snapshot of an installed OS, created with the HP Client Automation OS Manager Image Preparation Wizard.

### managed device

A device that is recognized and managed by the OS Manager.

### native installation

An installation in which an operating system is set up using the standard vendor-provided method. For example, for Windows, the setup program from the Windows distribution media is used to perform the installation. This type of installation can be completely unattended, using `unattend.txt`.

### OS state

The actual state of the OS, such as invalid, installed, or desired.

### reference machine

A workstation or server on which the OS image that is to be cloned is built.

### ROM object

An object—stored below the level of the device object—that contains information specific to the OS Manager.

### Service Operating System (Service OS)

A Service OS (SOS) is a pre-installation environment that is based on a lightweight operating system such as Linux or WinPE. This environment is used to apply operations to hardware on a target device as well as provision target devices.

### target device

A workstation or server on which you want to apply operations or install, replace, or update an OS.

### unmanaged OS

An unmanaged OS can be either:

- A target device that has been discovered by the OS Manager, but for which policy has not been assigned; or
- Policy has been assigned but you are not ready to overwrite the existing OS, so it is considered unmanaged.

_UNMANAGED_OS_ is also the name of the service in OS.ZSERVICE that is installed by the Application Manager on the target device.

# 2 System Requirements

At the end of this chapter, you will:

- Be familiar with the system requirements for the devices used in the OS Manager environment.

This chapter describes the requirements for the devices used in the OS Manager environment.

# Platform Support

For information about the supported platforms, see the release notes document that accompanies this release.

# Server

- At a minimum you will need a 3 GHz P4.
- A server with 1 GB of RAM and a minimum of 10 GB of free space for each image that you will publish.
- If you are publishing `.WIM` files, you must install Microsoft's **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 for download from Microsoft's web site.

  Be sure to review the system requirements for WAIK.

# HP Client Automation OS Manager Server

- Static IP address and port.
- Must have connectivity to the Configuration Server.

# Target Devices

The requirements for target devices are listed below.

- Target devices with existing operating systems that will be deployed using the legacy method must have the Application Manager already

installed. If you are using the ImageX or Windows Setup deployment methods, do not install the Application Manager.

- Target devices must meet the minimum hardware and BIOS requirements as published by Microsoft and the machine manufacturer for running the operating system that is to be deployed by the OS Manager.

A target device on which you plan to use WinPE for deployment must have a minimum of 512 MB RAM available. For additional requirements, refer to Microsoft's requirements for the Windows Vista operating system.

- HP thin client devices must have Windows XP Embedded, Windows CE, a Linux-based OS installed. Also see Firewall Settings for Windows XPe Thin Client Devices on page 38 and Installing the Application Manager on Thin Clients on page 39.
- If you are using VMware as the target device, change your target device's `.vmx` file to contain the following:

  **`ethernet0.virtualDev="e1000"`**

- If you want to report on, or make use of the device's make, manufacturer, and unique identifier for policy, the BIOS must support SMBIOS (for systems management) specification. If a target device lacks SMBIOS support, the only criterion available for specifying policy on that device will be the MAC address.
- An English, French, or German keyboard.
- A minimum of 128 MB of RAM.
- The machine can have one CPU or multiple CPUs. CPU must be an Intel 386 or higher, or AMD Athlon or Duron.
- If you are using a network (PXE) boot, you must:
  - Be able to boot from the Boot Server. To do this, make sure that the BIOS is set to boot from the network before the hard drive.
  - Have a **Network Interface Card** (NIC) that supports PXE, manufactured by Intel or 3Com.

    Note: Some older network cards are PXE capable but only support PXE with the addition of a network boot ROM. These cards must have the network boot ROM installed. Some older 3Com cards require a firmware upgrade to MBA 4.3 and PXE stack version 2.2.

— Be sure that the target devices have the same or a compatible **Hardware Abstraction Layer** (HAL) as the reference device in order to use Microsoft Sysprep. Devices with the same version of `HAL.DLL` share the same Hardware Abstraction Layer. For more information on determining a device's HAL, see

**http://support.microsoft.com/?kbid=237556**

If you cannot check the `HAL.DLL`, consider deploying the image on a target device in a lab environment to confirm success of the deployment.

- If you are using the ImageDeploy media and Local Service Boot, make sure that the BIOS is set to boot from the CD/DVD drive before the hard drive.
- Match the reference device's ACPI characteristics (that is, ACPI vs. non-ACPI, which is represented in the HAL) and boot drive interface.
- Be compatible with the *programmable interrupt controller* capabilities that are represented in the HAL that is captured on the reference machine.

  Note: An **Advanced Programmable Interrupt Controller** (APIC) HAL will not run on a device that does not have an APIC; however a **PIC** (standard on-board Programmable Interrupt Controller) HAL will run on a device that has an APIC. Newer HP/Compaq computers often come with an APIC.
- Support NTFS and FAT32 file systems.

# Firewall Settings for Windows XPe Thin Client Devices

## Sygate Firewall Settings

Windows XPE thin client devices ship with Sygate firewall pre-installed. Sygate must be configured to allow CA OS Manager to operate.

1. Log on to Windows XPE as Administrator.
2. Right-click the Sygate icon in system tray and select **Advanced Rules…**
3. On the General tab:
   - Add description **Allow CAE All**
   - Select **Allow this traffic**

4 On the Applications tab, use the browse button to add the following applications from `C:\Program Files\Hewlett-Packard\CM\Agent`:

   — Nvdkit

   — Radconct

   — Radpinit

   — Radexecd

   — Radstgrq

5 Make sure each item is selected (with a check mark next to each).

6 Click **OK** to save the new rule.

7 Click **OK** to exit.

Right-click the Enhanced Write Filter (EWF) icon in system tray and select commit. You are prompted to reboot. This will write your changes to the flash memory.

## Installing the Application Manager on Thin Clients

The Application Manager cannot be remotely deployed to thin client devices and must be installed manually using the installation programs included in the `\ThinClient` directory on the CM OS Manager media.

In addition to devices not always connected to the network, you will need to manually install the Application Manager to any Thin Client devices you want to manage.

### Linux-based thin clients

Installation of the Application Manager requires minimum free space of 3 MB on the `/mnt` file system. Certain thin client models and related images do not have enough space to install the Application Manager. See Running the agent from an NFS share on page 40.

#### To install the Application Manager on a Linux-based thin client

1 Login to the target thin client device as root.

2 Create a new directory called `/mnt/opt/OVCM`.

3 Copy the contents of `ThinClient.tar` (located on the product media in the `/ThinClient/Linux` directory) to `/mnt/opt/OVCM`.

Depending on your device model, you may have to extract the contents from `/tmp` or on another machine as some models do not have sufficient disk space to contain both the tar file and its exploded contents (requires approximately 7-8 MB free). After extracting the contents, delete `ThinClient.tar`.

4 Change the current directory to `/mnt/opt/OVCM` and run the installation by typing:

`./install -E -i HPCA_Configuration_Server`

Where *`HPCA_Configuration_Server`* is the hostname or IP address of the Configuration Server.

The Application Manager is installed.

These devices ship without the ability to contact and register with a DNS server. As such, you may not be able to ping this device. Also, the hosts file created on the factory image has 'localhost.localdomain' as its default hostname, and its (real) assigned hostname as an alias. As a result, the Application Manager registers the device as localhost.localdomain. You can switch the order in the hosts file to reflect the assigned hostname by placing it first in the list for the 127.0.0.1 entry

Management of these devices requires that the BIOS contain a valid serial number and machine UUID (setting asset tag is also recommended). Without these settings, OS deployment may not work properly.

### Running the agent from an NFS share

If you are using a model that has only 32MB flash memory, you will not be able to install the Application Manager locally. You will also not be able to use the Local Service Boot option to deploy an OS image and must therefore use PXE for that purpose.

### To run the Application Manager remotely from an NFS share:

1 Update the install script and modify the MEDIA_RAM_ROOT and INFRA_MEDIA_ROOT variables to point to the NFS directory.

2 Create the directory `/mnt/opt/OVCM` and place the install script into this location, and place the rest of the installation package (`thinclient.tar`) into the NFS directory.

3 Run install as described in step 4 above.

### To remove the Application Manager from Linux-based thin clients

Use the **uninstall** script to remove the Application Manager.

1 Login to the device as root.

2 Go to `/tmp/OVCM/IDMSYS`.

3 Type `./uninstall` and press **Enter**.

The Application Manager is removed.

## Windows XPe

### To install the Application Manager to Windows XPe

1 Access the product media from the Windows XPe Thin Client device.

2 On the product media, go to `SystemDrive:\ThinClient\XPE`.

3 Double-click **setup.exe**.

4 Follow the steps in the installation.

5 When prompted for the IP address and Port number, type the IP address and port number for your OS Manager Server.

The sgent is installed.

### To remove the Application Manager from Windows XPe

Use the installation program **setup.exe** to remove the Application Manager from Windows XPe.

1 Double-click **setup.exe.**

2 Select **Remove**.

3 Click **OK**.

The Application Manager is removed.

## Windows CE

### To install the Application Manager to Windows CE

1. Access the product media from the Windows CE thin client device.
2. On the product media, go to `SystemDrive:\ThinClient\WinCE`.
3. Double-click `radskman.X86.CAB`.
4. Type the IP address or hostname of the OS Manager Server and click **OK**.

The Application Manager is installed.

### To remove the Application Manager from Windows CE

- Use the Windows Control Panel applet **Add/Remove Programs** to remove the Application Manager from Windows CE.

# 3 Installing and Configuring the Server Architecture

At the end of this chapter, you will:

- Understand the prerequisites for installing and configuring the server architecture.
- Be able to install the HP Client Automation OS Manager Server.
- Be able to configure the HP Client Automation Portal.
- Be able to configure the HP Client Automation Proxy Server.
- Be able to install the Boot Server.

This chapter describes how to install and configure the various HP Client Automation components for operating system management.

It is helpful to have your license strings accessible.

If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

# Prerequisites

Before installing and configuring the HP Client Automation components, you must have the HP Client Automation Infrastructure for Windows set up that includes the following:

- HP Client Automation Configuration Server, version 7.20 or higher.

  To check the version of your Configuration Server, review the Configuration Server log file.

  During the installation, you must have selected the Client Automation OS Manager check box on the Select Products to be installed and supported by the Configuration Server.

- HP Client Automation Configuration Server Database, version 7.20 or higher

  To check the version of your Configuration Server DB, use the HP Client Automation Administrator Configuration Server Database Editor to view the PRIMARY.SYSTEM.DBVER Class. The DBVER attribute specifies the current version of your database.

- HP Client Automation Administrator, version 7.20 or higher.
- HP Client Automation Proxy Server, version 7.20 or higher.
- HP Client Automation Portal, version 7.20 or higher.
- Microsoft Internet Explorer with the security level set no higher than medium.

# Installation Checklist

For best results, HP recommends that you do the installation in the following order.

**Table 2 Installation Checklist**

- ❑ 1 Install the OS Manager Server.
- ❑ 2 (Optional) Enable communication between the OS Manager and the Configuration Server.
- ❑ 3 Install the Boot Server.
- ❑ 4 Configure the Portal.
- ❑ 5 Configure the Proxy Server.
- 6 (Optional) Install the Mini Management Server.
- ❑ 7 (Optional) Convert the OS Manager environment to use WinPE Service OS only (no Linux).

Check the HP support web site for product updates and release notes.

# About the OS Manager Server

The OS Manager Server handles requests for operating system images from the Configuration Server. It performs a low level exchange with the OS Manager System Agent and the OS Manager Boot Loader.

Every time a target device boots, the OS Manager Boot Loader connects with the OS Manager Server; which then accesses the Portal to verify that the device exists. In cases of policy changes or OS reinstallation, the OS Manager Boot Loader will load OS Manager System Agent, which will perform resolution and manage the operating system.

The OS Manager Server is capable of handling large numbers of target devices with modest requirements for disk space and memory. It is well suited to be co-resident with the Proxy Server.

## Installing the OS Manager Server

This section provides instructions for installing the OS Manager Server. Later, you must configure the Portal so that you can use the OS Manager administrative tasks. See Configuring the Portal on page 52.

### To install the OS Manager Server

If you have already installed an HP Client Automation Integration Server product such as the Proxy Server, some of the dialog boxes that are mentioned in this section may not appear during this installation; the information that was specified during that HPCA Integration Server installation (such as your license file) will be used.

1. From the OS Manager media, go to `\os_manager_server\win32` and double-click **setup.exe**.
2. Click **Next**.

   The End User License Agreement window opens.
3. Click **Accept**.

   The Installation Directory window opens.
4. Click **Next**.
5. Click **Browse** to navigate to your license file.

   The license file is installed in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\modules`.

   To check that your license string is valid, open *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\OSManagerServer\logs\httpd-osm-port.log` and search for “License is expired”. If you find this string, you must update your license file. See OS Manager Server Logs on page 218 for information about this log.
6. Click **Next**.

7 Type the User ID and Password for the Client Automation Portal. The default User ID is `romadmin` and the default Password is `secret`. This information is encrypted and stored in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\etc\roms.cfg`. If you want to change the User ID (PORTAL_UID) and Password (PORTAL_PASS), you must do it in `roms.cfg`. See Enabling Communication between the OS Manager and the Configuration Server on page 49 for encryption information.

8 If necessary, type the port for the OS Manager Server.

9 Click **Next**.

10 Specify the address and port for the Configuration Server. You may include the company name and domain, but it is not required.

11 Click **Next**.

12 Specify the address and port for the Proxy Server. You may include the company name and domain, but it is not required.

Do not type **`localhost`** or **`127.0.0.1`** in this field because the target device will be unable to locate the appropriate server.

The Proxy Server can be co-located with the Configuration Server. Refer to the *Client Automation Proxy Server Installation and Configuration Guide* for more information about installing this server and how to co-locate it with the Configuration Server.

13 Click **Next**.

14 Specify the address and port number for the Portal. You may include the company name and domain, but it is not required.

15 Click **Next**.

16 Type the name of the Portal Zone.

The Zone name that you enter *must* be the same name that you specified when you installed the Configuration Server. If you cannot recall this value, check the value of the PORTAL_ZONE setting in the MGR_ROM section of the `edmprof.dat` file in the Configuration Server's `bin` directory.

— Specify a maximum of 64 characters.

— Use only letters (a-z and A-Z), numerals (0-9), and the space character.

— Do not use special characters, such as an underscores, commas, and periods.

Refer to the *Client Automation Portal Installation and Configuration Guide* for information about zones.

17 Click **Next**.

18 Select an attribute to name the ROM object. If you do not make a selection, the default attribute, Computer Name, will be used. This name appears in the Portal.

If, during an OS Manager Server installation, you select one of the SMBIOS parameters for the ROM object display, these values may not be present or unique on all devices.

- If the value is not present, the common name will be used.
- If the value is not unique, multiple devices will be displayed with the same name.

19 Click **Next**.

The Summary window opens.

20 Click **Install** to begin the installation.

21 Click **Finish** when the installation is finished.

If you are installing the OS Manager Server on Microsoft Windows Server 2003, when you open the Portal you may be prompted to add it to the Trusted sites zone. Also, in order to ensure that the Portal works properly, set the security settings for your browser no higher than medium.

22 After the installation is complete, copy two utilities to the HPCA OS Manager Server in order to capture images for deployment using WinPE.

- Copy `bootsect.exe` from `C:\Program Files\Windows AIK\Tools\PETools\x86` to `C:\Program Files\Hewlett-Packard\CM\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`
- Copy `imagex.exe` from `C:\Program Files\Windows AIK\Tools\x86` to `C:\Program Files\Hewlett-Packard\CM\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`

  Windows AIK is available from the Microsoft web site. It is not included as part of a normal Vista installation.

## Enabling Communication between the OS Manager and the Configuration Server

You must perform the following steps to enable communication between the OS Manager Server and the Configuration Server *if you are using a password to access your Configuration Server*.

### If you are using a password to access your Configuration Server

1. Shut down the HPCA OS Manager service.
2. From a command prompt, switch to the Client Automation OS Manager Server installation directory (typically *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\OSManagerServer`).
3. Type **`nvdkit`** and press **ENTER**.
4. Type the following command:

   **`password encrypt`** *`your password`* **`aes`**

   *`your password`* represents your existing password for your Configuration Server DB. This is case sensitive.

   The encrypted password will resemble:

   `<AES256>kITMqDenvFUpdpBaYt8XBg==`
5. Copy the encrypted password from the nvdkit command line and paste it into *`SystemDrive:\Program`* `Files\Hewlett-Packard\CM\OSManagerServer\etc\roms.cfg` as the value for the ADMINPWD entry.

   The literal string `<AES256>` and the equal signs (==) must be included.
6. Restart the HPCA OS Manager service.

# About the Boot Server

The Boot Server is the Windows-based PXE (Pre-execution Environment) and **Trivial File Transfer Protocol** (TFTP) server for the OS Manager environment. Note that the TFTP daemon runs secure mode.

PXE uses DHCP broadcast, multicast, or UDP protocols and receives broadcasts. This means that if broadcast traffic is restricted between subnets, you must place PXE severs in each subnet, enable broadcasts (which may not be an option), or use a DHCP helper function to pass DHCP broadcast traffic. This situation is similar to that of standard DHCP servers and is probably well understood by your network administrator.

The PXE server is a low volume server. The TFTP server volume is slightly higher, but should only be transferring the OS Manager Boot Loader (less than 64 KB) on every target device boot and the Service OS *only* when a state change is required (such as, initial discovery, installation, or change of OS). This transfer will *not* occur for devices in desired state. Therefore, a few strategically placed PXE/TFTP servers should be able to support many clients. They should be accessible, however, on a relatively high-speed connection.

## Prerequisites

- Do *not* configure your DHCP server to preclude the use of the Boot Server.
- PXE Client version 2.2 or higher.
- Install the Boot Server on a machine separate from your DHCP server because the PXE server and the DHCP server listen on the same DHCP port by default.
- Do not install the Boot Server on a machine that has cygwin installed because this is not supported.
- If you have more than one PXE server in your environment, each must be on a separate segment and the PXE packets should not pass between the segments. You can use the Discover Boot Server utility to determine if there are PXE servers in your environment. See Using the Discover Boot Server Utility on page 228.
- A static IP address for the Boot Server.

If the OS Manager IP address or port is ever changed, you must update the Boot Server ISVR value and the ISVRPORT value in the Boot Server default file. The default file is typically located in *SystemDrive*:\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot\linux.cfg.

Do not use editors that automatically convert to Windows format, such as Notepad. Use Nano or WordPad to modify the Boot Server's configuration files.

- Remember that target devices must contain a PXE-compliant NIC card and be set to boot from the network. To determine whether a device contains a PXE-compliant NIC card; refer to the card's specifications.

To enable PXE in your network environment:

In some network environments (such as those containing Cisco), the client may fail to PXE boot and you may need to modify the network port configuration.

For the Cisco switch, use the following:

```
set port channel off
set spantree port fast enable
```

For all other vendors, consult their documentation.

# Installing the Boot Server

### To install the Boot Server

1. On the OS Manager media, go to \boot_server\win32 and double-click setup.exe.

   The Boot Server Install window opens.

2. Click **Next**.

3. Click **Next** to accept the default directory.

Do not install the Boot Server to a directory that contains spaces.

4. Type the IP address and port number for the OS Manager Server in the following format: *xxx.xxx.xxx.xxx*:*port*.

You can enter this information even if the OS Manager Server is not yet installed or running. The information is written to a configuration file.

5 Click **Next**.

6 Review the installation summary and click **Install**.

A window opens to indicate that the Boot Server has been successfully installed.

7 Click **Finish**.

If you want to check that the installation was successful:

- Press **Ctrl + Alt+ Delete**, go to Task Manager, and review the list of processes. Confirm that `PXE.exe` and `Inetd.exe` are running.

or

- Go to the Event Viewer and check the application events. You will see when the process starts. Entries for problems will appear soon after the event starts.

# Configuring the Portal

Make the following changes to configure the Portal to support the OS Manager.

### To update the modules

1 Stop the HPCA Portal service.

2 From the OS Manager media, copy the files in the `\os_administrator` folder to the `\ManagementPortal\modules` directory, the default location of which is *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\ManagementPortal\modules`.

3 Restart the HPCA Portal service.

### To update the edmprof.dat file

1 Open `edmprof.dat` in the Configuration Server's `bin` directory.

2 In the [MGR ROM] section

— Set PORTAL_HOST to the IP address for the Portal.

- Set PORTAL_PORT to the port for the Portal.
- The PORTAL_ZONE setting contains the value that you specified when you installed the Configuration Server.
- Set DISPLAYNAME to the same value as the DISPLAYNAME attribute in *SystemDrive:*\Program Files\Hewlett-Packard\CM\OSManagerServer\etc\roms.cfg.

  This ensures that the display name for the device is updated when the OS Manager Server interfaces with Portal. If you chose the default during the installation, set this to **compname**.
- PORTAL_UID contains the ID of a Portal user who can update a device or the ROM object.
- PORTAL_PASS contains the password for the Portal user who can update a device or the ROM object.

```
*--------------------------------------------------------------------*
* Manager CM OS Manager                                              *
*  PORTAL_HOST  = Host name or IP address for the CM Portal          *
*  PORTAL_PORT  = Port number for the CM Portal                      *
*  PORTAL_ZONE  = Zone name in the CM Portal                         *
*  DISPLAYNAME  = Display name used in the CM Portal for the device  *
*  PORTAL_UID   = ID of a CM Portal user who can update a device     *
*                 or the ROM object                                  *
*  PORTAL_PASS  = Password of a CM Portal user who can update        *
*                 a device or the ROM object                         *
*                                                                    *
*  PORTAL_ZONE and DISPLAYNAME parameters should match the ZONE and  *
*  DISPLAYNAME parameters in roms.cfg file                           *
*--------------------------------------------------------------------*
```

```
[MGR_ROM]
PORTAL_HOST = 192.168.1.9
PORTAL_PORT = 3471
PORTAL_ZONE = cn=Home,cn=radia
DISPLAYNAME = compname
PORTAL_UID = {AES256}ACuqUOk5jOzI23B243dvgw==
PORTAL_PASS = {AES256}3gMlspmbrGbqVXNPDx8tWg==
```

3. Save and close edmprof.dat.

## Adding a Directory Service

You must define a Configuration Server directory service in the Portal before you can use the OS Manager administrative tasks. You need to perform these steps only once.

### To add the directory service

1. Open your web browser and go to the Portal, `http://ipaddressORhostname:3471`.
2. Login as the Portal administrator (by default, the user ID is **`admin`** and the password is **`secret`**).

   For details on setting the user ID and password for the Configuration Server, see the *Client Automation Portal Installation and Configuration Guide*.
3. In the workspace, click the appropriate Zone.

   For detailed information about zones and directory services, refer to the *Client Automation Portal Installation and Configuration Guide*.
4. In the workspace, go to **Configuration** and click **Directory Services**.
5. From the Model Administration task group, click **Add Directory Service**.
6. From the Type list, select **ds-rcs**.
7. In the URL text box, change the value of `localhost` to the IP address of the Configuration Server that you want to use for OS Manager administration.
8. If necessary, change the Display Name. For example, Configuration Server DB.
9. Click **Submit**.

   The Configuration Server DB is available in Zone, Configuration, Configuration Servers.
10. Log out of the Portal.

## Assigning OS Manager Views to New Users

If you add a new user to the OS Manager, you may want to provide access to the OS Manager administrative tasks. (To create new users, refer to the

*Client Automation Portal Installation and Configuration Guide*.) After the OS Manager Views are assigned, the appropriate classes for the OS Manager will appear when the user logs in and connects to the Configuration Server.

1. Open your web browser and go to the Portal, `http://ipaddressORhostname:3471`.
2. Login as the Portal administrator (by default, the user ID is **`admin`** and the password is **`secret`**).
3. Click the appropriate Zone.
4. Click **Administrators and Operators**.
5. Click on the OS Manager user to whom you want to assign OS Manager Views.
6. In the Group of Tasks, click **Assign OS Manager Views**.
7. Click ✓ to confirm that you want to assign ROM Views to this user.

   OR

   Click ✗ to indicate that you do not want assign ROM Views to this user.

The Properties window opens, showing that the modification is complete.

## Configuring the Default Behaviors Instance

You must modify the default Run Once parameter string in the Default Behavior instance so that it contains the IP address for your Configuration Server. If you do not modify this parameter, your target device will not be able to run a successful CM OS connect. For more information on the BEHAVIORS Class, see Setting Behaviors on page 123.

### To configure the default Behaviors instance

1. Log on to the Portal as the HPCA OS Manager administrator.

   See Logging On on page 114 for more information.
2. In the workspace, click **Configuration**, **Configuration Servers**, and select the appropriate Configuration Server.
3. Click **Behavior**.

   The Behavior instances appear in the workspace.
4. Click **Defaults**.
5. In the OS Manager Administration task group, click **Modify Instance**.

6 In the RunOnce Parameter String change `IP=RCSSERVER` to reference the appropriate Configuration Server for your environment.

7 Click **Modify** to save the changes.

Now, the OS Manager Server is ready to use Portal.

# About the Proxy Server

The Proxy Server is a web server that is used to deploy the service containing the operating system image to the target devices.

We recommend that you pre-load images on the Proxy Server before deploying them to the target devices. Do not dynamically download your OS images because the target devices will experience timeouts indefinitely until the image is downloaded. Where appropriate, separate Proxy Servers may be used for applications and OS file serving.

Refer to the *Client Automation Proxy Server Installation and Configuration Guide* for more information about installing this server and how to co-locate it with the Configuration Server.

## Configuring the Proxy Server

The Configuration Server can be used to deploy operating system images. However, in order to do so, a Proxy Server must be co-located on the Configuration Server host machine, and the following changes must be made to the Proxy Server configuration file, `rps.cfg`, which is located (by default) in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc`.

1 Stop the HPCA Integration Server service.

2 Open *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\rps.cfg`.

3 Change the `-static-root` parameter (which is the source location) to the location of the Configuration Server DB (such as `C:/Program Files/Hewlett-Packard/CM/ConfigurationServer/DB`). Be sure to use forward slashes.

4 Change the `-static-type` parameter from **`agent`** to **`server`**.

5 Save the file.

6 Restart the HPCA Integration Server service.

These changes are shown in bold in the excerpt below.

```
rps.cfg example:  (top portion excluded)
rps::init {
    -stager         0
    -stager-port    3461
    -stager-trace   0
    -httpd          1
    -httpd-prefix   "/RESOURCE"
    -static-root  "C:/Program Files/Hewlett-Packard/
CM/ConfigurationServer/DB"
    -static-trace   0
    -static-type  server
```

# Installing the Client Automation Mini Management Server

You must install the HPCA Mini Management Server if you plan to use Windows CE images. This server handles transactions between the agent and the Configuration Server.

### To install the Mini Management Server

1 On the Infrastructure media, go to `extended_infrastructure\mini_management_server\win32` and double-click `setup.exe`.

The Client Automation Mini Management Server Install window opens.

2 Click **Next**.

The End User License Agreement window opens.

3 Click **Accept**.

4 Click **Next** to accept the default directory.

5 Type the IP address or name of the Client Automation Configuration Server and click **Next**.

6 Type the IP address or name of the Client Automation OS Manager Server and click **Next**.

7 Click **Install**.

8 Click **Finish** when the installation is complete. The server is installed with a service name HPCA Mini Management Server and the default port is 3470.

# Converting the Service OS to WinPE (optional)

When the OS Manager is installed, it is configured to use the Linux Service OS by default and only switches over to WinPE if required by a particular management operation. Under certain circumstances, you may prefer to run an environment using WinPE as the default Service OS, switching over to Linux only if necessary. The following steps describe how to convert an environment to use WinPE as the default Service OS.

Changing the default Service OS will affect newly discovered target devices in OS Manager 7.20 and higher only. Existing target devices will continue to operate using the Linux Service OS as the default.

## To convert the default Service OS to WinPE:

1 Modify the settings for PXE by opening the Boot Server's default file (typically located in *SystemDrive*:\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot\linux.cfg), and:

Do not use a text editor that automatically converts to Windows format, such as Notepad. Use Nano or WordPad to modify the Boot Server's configuration files.

— In the OS Manager section, change the DFTLSVOS to **_SVC_PEX86_**.

— Save and close the file.

2 Modify the setting for LSB by opening the Client Automation Admin CSDB Editor and going to PRIMARY, OS, Operating Systems (ZSERVICE), Local Service Boot and in the right pane scrolling to the Service OS List (ELGBLSOS) attribute.

— Double-click the attribute and change the setting to **_SVC_PEX86_**.

— Save, and close the Admin CSDB Editor.

3 Modify your deployment CD-ROM as instructed in Building a Custom WinPE Service OS on page 205.

# The Admin Publisher

The Admin Publisher is a component of the HP Client Automation Administrator. It is a prerequisite for configuring the server architecture, and can be used to publish the operating system image and its associated files, as well as other files (such as `Sysprep.inf` and `unattend.txt`), to the Configuration Server DB.

# 4 Preparing and Capturing OS Images

At the end of this chapter, you will:

- Be able to determine a deployment method.
- Be able to prepare and capture operating system images based on the deployment method.

In this chapter, you will learn how to prepare and capture operating system images for deployment to devices in your environment. After an image is captured, it is uploaded to the `\upload` directory on the OS Manager Server. Next, you must use the Admin Publisher to store the image in the Configuration Server DB and later you can use the OS Manager Admin Module in the Portal to deploy the operating systems to qualifying target devices.

If you are using an existing `.WIM` image or are creating one using Microsoft WAIK, you do not need to prepare or capture the image and can skip to the next chapter.

# Deployment Methods

Table 3 below provides information about the three methods (Legacy, Microsoft ImageX, and Microsoft Windows Setup) that can be used to deploy an image.

**Table 3 Deployment methods**

| Method | Service OS Type* | Image format | Resulting Files** | Supported Platforms |
|---|---|---|---|---|
| Legacy | Linux | sector-based image | `ImageName.IMG`<br>`ImageName.MBR`<br>`ImageName.EDM`<br>`ImageName.PAR`<br>For WinXPe or Windows CE, the files are:<br>`ImageName.IBR`<br>`ImageName.EDM`<br>For Linux, the files are:<br>`ImageName.DD`<br>`ImageName.EDM` | Windows 2000 Workstation, Server, and Advanced Server x86<br>Windows XP x86 or AMD64/EM64<br>Windows 2003 Server and Advanced Server x86 or AMD64/EM64<br>Windows XP Embedded<br>Windows CE<br>Debian Linux<br>HP Thin Connect |

| Method | Service OS Type* | Image format | Resulting Files** | Supported Platforms |
|---|---|---|---|---|
| Microsoft ImageX | WinPE | .WIM file-based format | `ImageName.WIM`<br>`ImageName.EDM` | Windows XP SP2 (or later) Professional x86 or AMD64/EM64T<br>Windows Vista Enterprise, Business and Ultimate Edition x86 or AMD64/EM64T<br>Windows Server 2008 Standard and Business edition x86 or AMD64/EM64T<br>Windows 2003 Server SP1 and Advanced Server x86 or AMD64/EM64 |
| Microsoft Windows Setup | WinPE | .WIM file-based format | `ImageName.WIM`<br>`ImageName.EDM` | Windows Vista Enterprise, Business and Ultimate Edition x86<br>Windows Server 2008 Standard and Business edition x86 |

*When deploying using a Service OS, you must have the compatible drivers for target device in the SOS. If you are using WinPE and the drivers are not available, see Adding Drivers to the WinPE Service OS on page 208. If you are using a Linux SOS, HP will provide periodic updates of the Linux SOS.

**Resulting files are stored in the `\upload` directory on the OS Manager Server.

For more information about the ImageX and Windows Setup deployment methods, refer to Microsoft's documentation.

The OS image preparation and capture steps will vary based on the operating system and deployment method. The instructions are detailed in the following sections of this chapter.

- Capturing pre-Windows Vista Operating Systems for Legacy Deployment, below
- Capturing pre-Windows Vista Operating Systems for ImageX Deployment, on page 66
- Capturing Windows Vista Operating Systems for ImageX Deployment, on page 67
- Capturing Windows Server 2008 for ImageX Deployment, on page 67
- Capturing pre-Windows Vista Operating Systems for Windows Setup Deployment, on page 70
- Capturing Windows Vista Operating Systems for Windows Setup Deployment, on page 76
- Capturing Windows Server 2008 for Windows Setup Deployment, on page 77
- Preparing and Capturing Thin Client OS Images on page 88
  - Windows XPe OS images on page 88
  - Windows CE OS images on page 92
  - Linux-based OS images on page 94

## Capturing pre-Windows Vista Operating Systems for Legacy Deployment

### Task 1 Prepare the Reference Machine

1 Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

Store the OS on the **C:** drive because it is the only drive that will be captured.

2 Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image. The following Microsoft KB article contains information for including OEM drivers for Windows OS installations:

**http://support.microsoft.com/default.aspx?scid=kb;en-us;314479**

3 Install the HP Client Automation Application Manager 7.20 for Windows with the OS Manager feature from the HPCA agent media. The Application Manager is required so that when the OS image is deployed, the device can connect to the OS Manager Server. If you need to update the Application Manager, you must use agent self-maintenance.

4 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.

5 Keep the image file size as small as possible. The ideal configuration is a partition just large enough to fit the operating system, plus additional space for the HPCA agent.

HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 140.

The following to helps minimize the size of the image file.

a Create free space.
HP recommends that after you have created the smallest partition with the least amount of free disk space as possible, set the ExtendOemPartition = 1 in the [Unattended] section of `Sysprep.inf`, to allow for the small image to be installed on a target device with a much larger drive. When the ExtendOemPartition is set to true, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The Application Manager can then use the free space on the volume for application installations.

b Disable hibernation if you are using a laptop.

c If necessary, remove the recovery partition.

d Disable the paging file. The page file will be enabled automatically when mini-setup is run after the deployment.

e Turn off System Restore.

f Turn off Indexing Service and Disk Compression.

g Turn off On Resume Password Protect.

### Task 2 Pre-requisites

- Download Microsoft Sysprep to distribute Microsoft operating systems using cloned images.

Review Microsoft's documentation for information about how to use Sysprep, how to create a `Sysprep.inf`, as well as the available parameters.

- Set up Microsoft's Sysprep
- Create a `Sysprep.inf`

See Using Microsoft Sysprep on page 50 for details.

### Task 3 Run the HP Client Automation OS Manager Image Preparation Wizard

See Using the HP Client Automation OS Manager Image Preparation Wizard on page 81.

## Capturing pre-Windows Vista Operating Systems for ImageX Deployment

### Task 1 Prepare the Reference Machine

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

   Store the OS on the C: drive because only the C: drive will be captured.

   Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

2. Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.

3. Keep the file system as small as possible which will minimize the size of the `.WIM` file.

   HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 140.

   a. Delete unnecessary files and directories from the files system.

b Turn off System Restore.

### Task 2 Pre-requisites

- Download Microsoft's Sysprep to distribute Microsoft operating systems using cloned images.

Review Microsoft's documentation for information about how to use Sysprep, how to create a `Sysprep.inf`, as well as the available parameters.

- Set up Microsoft's Sysprep
- Create a `Sysprep.inf`

See Using Microsoft Sysprep on page 50 for details.

### Task 3 Run the HP Client Automation OS Manager Image Preparation Wizard

See Using the HP Client Automation OS Manager Image Preparation Wizard on page 81.

## Capturing Windows Vista Operating Systems for ImageX Deployment

### Task 1 Copy utilities to the HPCA OS Manager Server

To capture images for deployment by ImageX copy the following utilities to the HPCA OS Manager Server.

2 Copy `bootsect.exe` from `C:\Program Files\Windows AIK\Tools\PETools\x86` to `C:\Program Files\Hewlett-Packard\CM\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`

4 Copy `imagex.exe` from `C:\Program Files\Windows AIK\Tools\x86` to `C:\Program Files\Hewlett-Packard\CM\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`

Windows AIK is available from the Microsoft web site. It is not included as part of a normal Vista installation.

### Task 2 Prepare the Reference Machine

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

   Store the OS on the C: drive because only the C: drive will be captured.

   Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

2. Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.

3. Turn off User Access Control.

4. Keep the file system as small as possible which will minimize the size of the `.WIM` file.

   HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 140.

   a. Delete unnecessary files and directories from the files system.

   b. Turn off System Restore.

### Task 3 Prepare unattend.xml

- Copy the sample unattend.`xml` from `samples\unattend\vista\x86` from the Image Capture media to `C:\windows\system32\sysprep`. You may need to modify this file for your environment.

### Task 4 Run the HP Client Automation OS Manager Image Preparation Wizard

See Using the HP Client Automation OS Manager Image Preparation Wizard on page 81.

# Capturing Windows Server 2008 for ImageX Deployment

## Task 1 Prepare the Reference Machine

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

   Store the OS on the C: drive because only the C: drive will be captured.

   Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

2. Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.

3. Turn off User Access Control.

4. Keep the file system as small as possible which will minimize the size of the `.WIM` file.

   HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 140.

   a. Delete unnecessary files and directories from the files system.

   b. Turn off System Restore.

## Task 2 Prepare unattend.xml

- Copy the sample unattend.`xml` from `samples\unattend\w2k8\x86` from the Image Capture media to `C:\windows\system32\sysprep`. You may need to modify this file for your environment.

## Task 3 Run the HP Client Automation OS Manager Image Preparation Wizard

See Using the HP Client Automation OS Manager Image Preparation Wizard on page 81.

## Capturing pre-Windows Vista Operating Systems for Windows Setup Deployment

This case is the only one in which you will use the HPCA Windows Native Install Packager to prepare an image. The image is of the installation media for a pre-Windows Vista operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the Application Manager source. The image is sent to the OS Manager's `\upload` directory and then you will use the Admin Publisher to publish the image to the Configuration Server DB.

When the image is deployed to a target device, the target device reboots and the Windows Native Install setup continues with the text mode setup phase, followed by the GUI phase. These two phases are controlled by `unattend.txt`, and allow for a completely unattended setup.

### **Task 2** Prepare the Reference Machine

The image of the original installation media created on the reference machine is deployed to target devices. Before using the HPCA Windows Native Install Packager to create the image, ensure that you have the OS Manager media and that the reference machine meets the following requirements:

1. Connectivity to a OS Manager Server.
2. A target drive, recommended being on an extended partition, that:
   - Will be used as if the target drive is currently formatted and empty (has no data). If the target drive is not formatted or it is formatted and contains data, the user will be prompted to format the drive.
   - A user can pre-format the drive with FAT32 if they format the drive and ensure that there is no data on the drive.

     Note that FAT32 cannot be expanded after deployed. NTFS can be expanded and is the default.
   - Is at least 1.5 GB. If the target drive is larger, it will take more processing time when the drive is imaged or the image may be larger than necessary depending on how the "Optimize Compression of Unused Disk Space" check box is set in the HPCA OS Manager Image Preparation Wizard.

     All data on the target drive will be lost.

3 A separate drive (to increase speed), such as the `C:` drive, with the HPCA Windows Native Install Packager software already installed. See Install the HPCA Windows Native Install Packager on page 72.

4 You must also have access to the following items; specify their location when using the HPCA Windows Native Install Packager:

— The setup files for the Application Manager.

— The `i386` directory from your operating system media.
You can slipstream any necessary service packs into this directory. See the `readme.txt` file associated with each service pack for more information about how to do this.

Windows setup will not let you run the setup for an older version of Windows. For example:

- If your device is running Windows XP, you cannot use the `i386` directory for Windows 2000.
- If your device is running Windows 2003, you cannot use the `i386` directory for Windows 2000 or Windows XP.

— `Unattend.txt`
You can create the file manually or use Windows Setup Manager on your Windows media. Sample files are available on the Image Capture media in `\samples`.

## Task 4 Create Unattend.txt

`Unattend.txt` automates the installation of the OS so that no user input is necessary. The `unattend.txt` file *must* match the release of Windows specified in the `i386` directory. These files may vary slightly depending on the version of Windows being installed.

The `Unattend.txt` file should not be larger than 800 KB.

The following are some tips about creating the `unattend.txt` file to be stored with the image:

- The settings in the file should be as generic as possible so that the file can be used with any device in your environment.
- Include the statements **`AutoLogon=YES`** and **`AutoLogonCount=1`** in the [GuiUnattended] section of this file.

  You must use the [GuiUnattended] section, rather than `$OEM$\cmdlines.txt`, because the Application Manager setup uses

Windows installer to install the Application Manager on the target device and `$OEM$\cmdlines.txt` cannot run the Windows Installer. The `AutoLogon` and `AutoLogonCount` statements ensure that the Application Manager is installed during the first user logon after the operating system is installed.

- Include the statement **`extendoempartition=1`** in the [Unattended] section of this file. This causes Windows to extend the file system and partition to include any unused space that follows the partition. If the target partition is too small, it is possible that the copy phase of the installation will work (the phase run on the reference machine), but when the image is deployed the text mode phase will fail or install the OS on some other partition.

  If you use a large target partition, the process that zeroes unused space on the file runs for a long time.

- You can also create separate `unattend.txt` files for any necessary customizations. You can use the Admin Publisher to publish these files to the SYSPREP class in the Configuration Server DB and then you can connect them to the appropriate OS image. Use the Connect Sysprep File task in the OS Manager Administration task group. When the image is deployed, the customized unattend.txt will be merged with the original file.

See Using the Admin Publisher on page 104 for information about the Admin Publisher. When publishing `Unattend.txt` files, follow the instructions as if you were publishing a `Sysprep.inf` file.

### Task 5 Install the HPCA Windows Native Install Packager

1. On the Image Capture media, go to `\windows_native_install` and double-click **setup.exe**.
2. Click **Next**.

   The End User License Agreement window opens.
3. Review the terms and click **Accept**.
4. Select the directory to install the product in and then click **Next**.

   The Summary window opens.
5. Click **Install**.

When the installation is done, click **Finish**.

### **Task 6** Run the HPCA Windows Native Install Packager

#### To run the HPCA Windows Native Install Packager

1 Double-click the HPCA Windows Native Install Packager icon on the desktop.

You must complete the information in each of the three areas on the Configure Options window– Client Automation, Windows Setup, and Package.

a The Client Automation area contains options used to set up options related to Client Automation products.

b The Windows Setup area gathers information needed to perform the OS installation.

c The Package area gathers information needed by HPCA about the package that you are creating.

If you click **Next** before completing the required fields on each of these windows, you will receive a message prompting you to complete the fields.

2 In the Client Automation Client Source Directory field, enter the path for the Application Manager.

3 Select the check boxes for the Client Automation products that you want installed.

4 Select the Run first connect after install check box to perform an HPCA OS connect after the OS is installed. If this is not selected, the HPCA OS connect will not occur automatically after the OS is installed.

5 In the Optional Packager Command Line Arguments box, type parameters used by the WNI application. The options can be placed all on one line or on several lines. Specify the options in the keyword-value format, such as

```
-trace_level 9
```

The keyword must always begin with a dash (-).

Usually you will use the Optional Packager Command Line Arguments text box only when directed by Technical Support.

There are many parameters that can be used to create logs. The following example describes how to create a file called `C:\temp\nvdwni.log`.

- `-trace_level 99`
- `-trace_dir c:\temp`

If you want to create a log with a different name, you can use the following:

- `-trace_file filename.log`

6 Click **Next**.

7 In the **unattend.txt File** box, browse to the appropriate `unattend.txt` file.

Select a generic `unattend.txt` file to be stored in the image. This file should contain options that are applicable for all devices that the image may be applied to. Later, you can attach a separate unattend.txt file to the image to make any necessary customizations.

The `Unattend.txt` file must match the release of Windows specified in the i386 directory. These files may vary slightly depending on the version of Windows being installed.

8 In the i386 Directory text box, select the Windows source distribution directory provided by Microsoft on its distribution media. You can use the Microsoft slipstream process to incorporate service packs and other fixes. See the `readme.txt` file that is associated with the service pack for more information about how to do this.

Be sure to copy the i386 from the Windows CD-ROM to another location. If you use the CD-ROM, Windows setup assumes you will have the CD-ROM loaded on the target device and will not copy all of the necessary files.

9 In the Target drive drop-down list, select the drive where the native install package will be created. We recommend that this drive is on an extended partition.

All existing data found on this drive will be lost.

10 In the Extra Command Line Parameters text box, type any parameters that you want to pass to the Windows Setup program when it is run. See the Microsoft web site for more information about the parameters.

11 Click **Next**.

12 In the Image Name text box, type the name of the package that will be stored in the `\upload` directory on the OS Manager Server. This name has a maximum length of eight characters and should be composed of alphanumeric characters only.

13 In the Image Description text box, type a description of the image (up to 255 characters).

14 In the Client Automation OS Manager Server text box, specify the IP address or host name for the OS Manager Server where the image should be uploaded.

15 In the Client Automation OS Manager Port text box, specify the port for the OS Manager Server.

16 Select the Optimize Compression of Unused Disk Space check box to null all unused disk space on the target drive before imaging it. This reduces the size of the image but causes the HPCA OS Manager Image Preparation Wizard to run longer.

17 Click **Next**.

18 Review the Summary and then click **Create**.

After you click **Create on a Windows 2000 machine**, Windows Setup may prompt you to reboot the system. Click **Cancel** to avoid the reboot. The reboot is not necessary; however nothing will be harmed if the reboot does happen.

Windows Setup runs and then returns to the HPCA Windows Native Install Packager.

19 When the HPCA Windows Native Install Packager is done, a message prompts you to reboot using the Linux CD-ROM. This refers to the Image Capture media.

Remember the boot order must be set to boot from the CD-ROM first.

20 Insert the Image Capture media, and then click **OK**.

21 Click **Finish**.

22 Reboot the device and the image is uploaded to your OS Manager Server's `\upload` directory.

23 When a message appears that the OS Image has been successfully sent to the OS Manager Server, you can remove the media from the drive and reboot your device.

## Capturing Windows Vista Operating Systems for Windows Setup Deployment

### Task 1 Copy utilities to the HPCA OS Manager Server

To capture images for deployment by ImageX copy the following utilities to the HPCA OS Manager Server.

1 Copy `bootsect.exe` from `C:\Program Files\Windows AIK\Tools\PETools\x86` to `C:\Program Files\Hewlett-Packard\CM\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`

2 Copy `imagex.exe` from `C:\Program Files\Windows AIK\Tools\x86` to `C:\Program Files\Hewlett-Packard\CM\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`

Windows AIK is available from the Microsoft web site. It is not included as part of a normal Vista installation.

### Task 2 Prepare the Reference Machine

1 Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

Store the OS on the C: drive because only the C: drive will be captured.

Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

2 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.

3 Turn off User Access Control.

4 Keep the file system as small as possible which will minimize the size of the `.WIM` file.

HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 140.

a Delete unnecessary files and directories from the files system.

b Turn off System Restore.

5 If you are going to run the HPCA OS Manager Image Preparation Wizard from the Image Capture media, set the boot order to CD-ROM first. If you are going to run the HPCA Image Preparation Wizard from another location, set the boot order to network first.

### Task 3 Run the HP Client Automation OS Manager Image Preparation Wizard

See Using the HP Client Automation OS Manager Image Preparation Wizard on page 81.

## Capturing Windows Server 2008 for Windows Setup Deployment

### Task 1 Prepare the Reference Machine

1 Install the operating system from the original product media. The reference machine must be capable of running the operating system you are installing. Make sure the reference machine is using DHCP.

Store the OS on the C: drive because only the C: drive will be captured.

Customize the OS as necessary. This may include installing a set of basic or required applications. Be sure to include the latest service packs for the OS and applications and all required drivers for the devices to which you will deploy the image.

2 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.

3 Turn off User Access Control.

4 Keep the file system as small as possible which will minimize the size of the `.WIM` file.

HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see Adding Partitions on page 140.

a Delete unnecessary files and directories from the files system.

b Turn off System Restore.

5 If you are going to run the HPCA OS Manager Image Preparation Wizard from the Image Capture media, set the boot order to CD-ROM first. If you are going to run the HPCA OS Manager Image Preparation Wizard from another location, set the boot order to network first.

**Task 4** Run the HP Client Automation OS Manager Image Preparation Wizard

See Using the HP Client Automation OS Manager Image Preparation Wizard on page 81.

# Using Microsoft Sysprep

In the last step of gold image creation, the HP Client Automation OS Manager Image Preparation Wizard runs Microsoft Sysprep in order to strip out all of the security identifiers in the gold image and reset the image.

After the operating system image is delivered to the target device, the Microsoft Mini-Wizard will run automatically when the target device is started. After using the answers provided by `Sysprep.inf`, the Microsoft Mini-Wizard deletes the Sysprep directory on the target device.

## To set up Sysprep

1 Go to `DEPLOY.CAB` in the `SUPPORT\TOOLS` folder of the Microsoft operating system installation media. See Microsoft's documentation for details.

2 Extract the Microsoft Sysprep files from the `Deploy.cab` file using the appropriate operating system media. Copy these files to `C:\SysPrep` on the reference machine and make sure the directory and files are not set to read-only.

Be sure that you are using the latest Sysprep version. If you use an older version, you may receive an error.

If you do not have the appropriate version of Sysprep, you can download it from the Microsoft web site.

Even if you have administrator rights, make sure that you have the appropriate user rights set to run Sysprep. Refer to the article *#270032 "User Rights Required to Run the Sysprep.exe Program"* on the Microsoft web site. If you do not have the appropriate user rights, when Sysprep runs, you will receive the following error:

```
You must be an administrator to run this
application.
```

The HPCA OS Manager Image Preparation Wizard will exit and after you set up the appropriate user rights you will need to run the wizard again.

3 Be sure that the reference machine is part of a WORKGROUP and not a domain in order to use the Microsoft Sysprep.

4 Create a `Sysprep.inf` and save it to `C:\Sysprep`.

### To create Sysprep.inf

You can create `Sysprep.inf` manually or use the Microsoft Setup Manager (`Setupmgr.exe`). The Setup Manager can be found in the `Deploy.cab` file in the `SUPPORT\TOOLS` folder of a Microsoft OS distribution media. See Microsoft's documentation for more information.

Microsoft does not support creation of a mass storage section using the Sysprep utility for Windows 2000. If you use this option with Windows 2000, you may see issues with the capture or deployment of an image.

Sample `Sysprep.inf` files are available on the Image Capture media in `\samples\sysprep\`.

The `Sysprep.inf` file should not be greater than 800 KB in size.

Below are a few tips to consider when creating the `Sysprep.inf` file:

- Adjust the TimeZone value for your enterprise.
- Set up the AdminPassword.
- Make sure to include a product key so that the user will not need to enter this at the target device.

- In order to have an unattended installation, you must include UnattendMode = FullUnattended in the [Unattended] section.
- Set ExtendOemPartition to 1, so that Microsoft Sysprep will extend the OS partition into any available non-partitioned space that physically follows on the disk.
- If JoinDomain is present in `Sysprep.inf`, then `Sysprep.inf` has to have the Admin User ID and Password of an account in the domain that has the rights to join the computer to the domain. Note that JoinDomain is case sensitive.

## How Sysprep.inf files are prioritized

The `Sysprep.inf` file can be delivered with the operating system image or it can be delivered as a package that is connected to the operating system image (known as an override Sysprep file). If the `Sysprep.inf` file is published separately, it will be merged with the `Sysprep.inf` file in the image's NTFS into a single, combined `Sysprep.inf`.

`Sysprep.inf` files are prioritized in the following order, from lowest to highest:

1. Sysprep embedded in the image (lowest priority). If there is no separately published `Sysprep.inf` (override Sysprep), just the `Sysprep.inf in` the image will be used.
2. Override Sysprep (a Sysprep file that is separate from the gold image. See Connecting a Sysprep File on page 145 for details).

   Only one override `Sysprep.inf` will be resolved.

3. Sysprep attached to policy criteria (highest priority).

   - To attach a Sysprep file to policy, you must publish the Sysprep file to the Configuration Server DBand then use the Admin CSDB Editor to manually connect the Sysprep instance to the appropriate Policy instance.
   - Even if you override the Sysprep.inf, the ComputerName (COMPNAME) and JoinDomain (COMPDOMN) are still updated by the OS Manager based on the Computer Name and Domain stored in the Portal device repository.

# Using the HP Client Automation OS Manager Image Preparation Wizard

The HPCA OS Manager Image Preparation Wizard performs the following tasks:

1. Creates an object that contains information (including hardware and OS information capabilities) about the reference machine.
2. Runs Microsoft Sysprep on supported operating systems.
3. Restarts the reference machine into the Service OS (booted from the appropriate media). The Service OS runs to collect the image and its associated files.
4. Creates and copies files to *SystemDrive*:\Program Files\ *SystemDrive:**Program* Files\Hewlett-Packard\CM\OSManagerServer\upload on the OS Manager Server.

   If you choose to create a legacy image, the files uploaded are:

   - ImageName.IMG
     This file contains the gold image. This is a compressed, sector-by-sector copy of the boot partition from the hard drive system that may be very large. The file contains an embedded file system that will be accessible when the image is installed.
   - ImageName.MBR
     This file contains the master boot record file from the reference machine.
   - ImageName.PAR
     The file contains the partition table file from the reference machine.
   - ImageName.EDM
     This file contains the object containing inventory information.

   If you chose to create an image using ImageX or using Windows setup, the files uploaded are:

   - ImageName.WIM

     This file contains a set of files and file system information from the reference machine.
   - ImageName.EDM

     This file contains the object containing inventory information.

### To use the HPCA OS Manager Image Preparation Wizard

Before continuing, set the reference machine to boot from the CD-ROM drive. You must do this because the ImageCapture media is bootable. When you run the ImageCapture media, it reboots the device in order to upload the image.

1 Insert the ImageCapture media into the reference machine. See Product Media on page 29 if you need more information about where to get this media.

2 Go to `\image_preparation_wizard` and double-click `prepwiz.exe`.

If you are using a legacy operating system and the agent is not installed, you will see the following message.

```
This computer does not have the Application Manager
installed. You may not be able to manage the target
computers with the OS Manager product.
```

If you want the device to be managed, you must install the agent before running the Image Preparation Wizard.

- If you are capturing an image to be deployed using the Legacy method, the Image Preparation Wizard verifies that the `C:\Sysprep` folder exists and that Application Manager is installed before continuing.
- If you are capturing an image to be deployed using ImageX or Windows Setup, the Image Preparation Wizard will locate Sysprep in `C:\Windows\system32\sysprep` for Windows Vista or `C:\sysprep` for pre-Windows Vista operating systems.

Note that when you plan to deploy a .Windows Vista WIM file using ImageX or Windows Setup, the agent will be injected into the image during the deployment process. When using the Admin Publisher, you will be given an option to select the location of the agent. This is advantageous because you can package the agent independently and can update the agent as needed by publishing a new version to the Configuration Server DB. After you do this, all new .WIM deployments will automatically use the latest agent.

3 Click **Next**.

The End User License Agreement window opens.

4 Click **Accept**.

5 The deployment methods that may appear are:

- **Legacy** captures a raw disk image of the partition (.IMG format).
- **ImageX** captures an image in .WIM format that will be deployed using WinPE and the ImageX utility.
- **Windows Setup** captures an image in .WIM format that will be deployed using WinPE and Windows Setup.

If a deployment method is not supported for the OS, it will not appear.

6. Type the IP address or host name and port for the OS Manager Server. This must be specified in the following format: *xxx.xxx.xxx.xxx*:*port*. The OS Manager Server port reserved for OS imaging is 3469.
7. Click **Next**.
8. Type a name for the image file. This is the image name that will be stored in the `/upload` directory on the OS Manager Server.
9. Click **Next**.

   If you chose the Legacy deployment method, the Span Disk Image window opens.
10. Type the amount of the total uncompressed disk space (in MB) to use for each image file. Type **`0`** (zero) if you do not want to create a spanned image.

    Use spanned images to break the image file into smaller segments. Each segment of a spanned image is restricted to 4 GB. This is helpful so that you can comply with the restriction of whole images needing to be less than 4 GB so that they can be stored in the Configuration Server. If you choose not to use the spanned image option (by typing 0) your images must be less than 4 GB.
11. Click **Next**.

    If appropriate, the Additional Sysprep Options window opens.
12. The text box is pre-filled with a command that clears all the SIDs to prepare the machine for capture.

    If you want, you can type additional options to pass to Sysprep using a space as the delimiter.

    This is an advanced option. Be cautions when entering additional options as the command you enter will not be validated.

    Review Microsoft's documentation for information about additional Sysprep options

13 Click **Next**.

14 Type a description for the image file and click **Next**.

The Select the Windows Edition window may open.

15 Select the Windows edition that you are capturing and click **Next**.

The Options window may open.

If you do not have the Application Manager installed, you will not see the **Perform client connect after OS install** check box. However, please remember that it is important to have this agent installed if you are using the Legacy method to capture an image.

16 Select the appropriate options.

The options appear depending on the operating system that you are capturing.

— **Build Mass Storage Section in Sysprep.inf**.
Select this check box to build a list of the Mass Storage drivers in the [SysprepMassStorage] section of the `Sysprep.inf` for Windows XP and above.

Microsoft does not support creation of a mass storage section using the Sysprep utility for Windows 2000. If you use this option with Windows 2000, you may see issues with the capture or deployment of an image.

The list of Mass Storage Drivers is installed in the registry. This takes about 15-20 minutes, but provides fundamental mass storage device drivers to ensure success of image deployment across machine models and manufacturers.

If there are any errors in these entries, subsequent Sysprep execution can fail.

— **Optimize compression of unused disk space**
Select this check box to optimize compression of unused disk space.

This adds zeroes up to the end of the system drive partition. Note that this may take some time depending on the size of the hard drive.

This increases the compressibility of the captured image, reducing its size. Smaller image files require less disk space to store and less bandwidth to move across the network.

— **Resize partition before OS upload**
Select this check box to resize the partition to make it as small as possible. If you do not select this check box, make sure that your partition is sized appropriately.

— **Perform client connect after OS install**
Select this check box to connect to the OS Manager Server after the OS is installed. If this is not selected, the HPCA OS connect will not occur after the OS is installed.

This option will not appear if you are using a method where you do not have the agent installed (e.g., if you are using the Legacy method and did not install the Application Manager client or if you are capturing a Windows Vista image because the agent is installed during the deployment and a connect is run by default).

17 Click **Next**.

The Summary window opens.

18 Click **Start**.

19 Click **Finish**.

If you are working with an APIC device, the Make image compatible with PIC window opens. Note that Windows Vista operating systems can only be captured from and deployed to APIC compatible devices.

20 If necessary, select the **Make image compatible with machine with PIC** check box.

Microsoft does not recommend this. Be sure to see their web site for more information before making this selection.

21 Click **Next**.

If you selected the check box in the figure above, the Select Windows CD window opens.

22 Browse to the Windows CD-ROM and click **Next**.

23 Click **Finish** to run Sysprep.

The Image Preparation Wizard will start Sysprep; this can take 15-20 minutes to complete. Sysprep will reboot the device when complete. You may need to click **OK** to restart the device.

- If you are using Windows 2000, Sysprep may take some time to run even if you do not see any activity on the screen.
- If you are using the audit mode (previously known as factory mode), the machine will reboot to the operating system with networking enabled. After your customizations are completed, you must put the Image Capture CD/DVD into the machine and then go to a command prompt and run
  **`sysprep.exe -reseal -reboot`**

After Sysprep restarts, the image must be uploaded to the server.

- If the boot order is set to boot from CD-ROM first and the Image Capture media is loaded, the device will boot to the CD-ROM.
- If your device does not have a CD-ROM, you must have a PXE environment and the device must be set to boot from the network first. Then, during the network boot you can press **F8** on your keyboard to capture the image using PXE. A menu appears and you must select Remote Boot (Image Upload).

If the device does not boot to the CD (boots to operating system instead) you will need to restart the preparation process.

Then, the device will connect to the network, and store the image on the OS Manager Server.

- The upload of the image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a bottleneck. Transfer speeds will be approximately 30-400 Kbps but may vary depending on processor speeds and your network environment.
- You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

The Image Preparation Wizard connects to the network and stores the image on the OS Manager Server in the `/upload` directory.

When the upload process is complete, you will see the following message:

```
**** OS image was successfully sent to the HPCA OS Manager
Server.
```

24 Reboot the reference machine and readjust your boot settings if necessary to return to the original operating system.

Next, you will want to publish your image to the Configuration Server DB. See Chapter 5, Publishing to the HP Client Automation Configuration Server Database.

# Preparing and Capturing Thin Client OS Images

The following sections explain how to prepare and capture supported Thin Client operating system images:



## Windows XPe OS images

You can capture an image on an XPe thin client device and subsequently deploy the captured image to an XPe thin client device with a larger flash drive. This is subject to certain restrictions as specified in the release notes document.

### Task 1 Prerequisites for an XPe thin client image capture

- Product media
- XPe Embedded Toolkit CD-ROM
- Image Preparation CD-ROM

### Task 2 Prepare the XPe Reference Machine

1. Log into Windows XPe as Administrator.
2. From the XPe Embedded Toolkit, copy `etprep.exe` to C:\Windows.
3. From the XPe Embedded Toolkit, copy `fbreseal.exe` to `C:\Windows\fba`.
4. Install the Application Manager.

### Task 3 Install the Application Manager on Windows XPe

1. Access the product media from the Windows XPe Thin Client device.
2. On the product media, go to *`SystemDrive`*`:\ThinClient\XPE`.
3. Double-click `setup.exe`.
4. Follow the steps in the installation.

5 When prompted for the IP address and Port number, type the IP address and port number for your OS Manager Server.

The Application Manager is installed.

### Task 4 Run the HP Client Automation OS Manager Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.

2 Restarts the reference machine into the service operating system (booted from the Image Preparation CD you created). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.

3 Creates and copies the following files to *SystemDrive*:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload on the OS Manager Server.

— ImageName.IBR
This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Windows XPe images can be deployed to target machines with flash drives of equal or greater size. The file contains an embedded file system that will be accessible when the image is installed.

— ImageName.EDM
This file contains the object containing inventory information.

While these files are transferred, network speed will be less than optimal as the operating system image is compressed during transfer.

A comprehensive log (*machineID-all*.log) is also available in *SystemDrive*:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload after the image is deployed.

#### To use the Image Preparation Wizard

1 Insert the ImageCapture media into the reference machine. Thin client devices require a USB CD-ROM drive. See Product Media on page 29 if you need more information about where to get this media.

2 Click **Browse** to open the \image_preparation_wizard\win32\ directory.

3 Double-click **prepwiz.exe**. The Image Preparation Wizard verifies that `etprep.exe` and `fbreseal.exe` are available before continuing.

   The Welcome window opens.

4 Click **Next**.

   The End User Licensing Agreement window opens.

5 Click **Accept**.

6 Type the IP address or host name and port for the OS Manager server. This must be specified in the following format: *`xxx.xxx.xxx.xxx:port`*. The OS Manager server port reserved for OS imaging is 3469.

   If the Image Preparation Wizard cannot connect to the OS Manager server, a message opens and you must:

   — Click **Yes** to continue anyway.

   — Click **No** to modify the host name or IP address.

   — Click **Cancel** to exit the Image Preparation Wizard.

7 Click **Next**.

   The Image Name window opens.

8 Type a name for the image file. This is the image name that will be stored in the `/upload` directory on the OS Manager server.

9 Click **Next**.

   A window opens so you can enter a description for the image.

10 Type a description for the image file.

11 Click **Next.**

   The Options window opens.

12 Select the appropriate options.

   **Perform client connect after OS install.**
   Select this check box to connect to the OS Manager server after the OS is installed to verify the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.

13 Accept the defaults and click **Next**.

   The Summary window opens.

14 Click **Start**.

Click **Finish.**

The wizard prepares the image.

15 Click **OK**.

The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

If the device does not boot to the CD (boots to Windows XPe instead) you will need to restart the process.

The upload of the image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a bottleneck. Transfer speeds will be approximately 30-400 Kbps but may vary depending upon processor speeds and your network environment.

You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

16 OS Image Preparation Wizard connects to the network, and stores the image on the OS Manager server in the `/upload` directory.

When the upload process is complete, you will see the following messages

```
OS image was successfully sent to the OS Manager Server

**** If you had inserted a CD remove it now and reboot
```

17 Reboot the reference machine and readjust your boot settings if necessary to return to the original operating system.'

Next, you will want to publish your image to the Configuration Server DB. See Chapter 5, Publishing to the HP Client Automation Configuration Server Database.

## Windows CE OS images

### Task 1 Preqrequisites for a CE thin client image capture

- Product media
- Image Preparation CD-ROM

### Task 2 Install the Application Manager on the CE Reference Machine

1. Access the product media from the Windows CE thin client device.
2. On the product media, go to *SystemDrive*:\ThinClient\WinCE
3. Double-click **radskman.X86.CAB**.
4. Type the IP address or hostname of the OS Manager server and click **OK**.

   The Application Manager is installed.

### Task 3 Run the HP Client Automation OS Manager Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
2. Restarts the reference machine into the service operating system (booted from the ImageCapture media). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.
3. Creates and copies the following files to *SystemDrive*:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload on the OS Manager Server.

   — ImageName.IBR
   This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Windows CE images can be deployed to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.

   — ImageName.EDM
   This file contains the object containing inventory information.

While these files are being transferred, network speed will be less than optimal as the operating system image is compressed during transfer.

A comprehensive log (*machineID-all*.log) is also available in *SystemDrive*:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload after the image is deployed.

### To use the Image Preparation Wizard

1. Insert the ImageCapture media into the reference machine. Thin client devices require a USB CD-ROM drive. See Product Media on page 29 if you need more information about where to get this media.
2. Click **Browse** to open the \image_preparation_wizard\WinCE\ directory.
3. Double-click **prepwiz.exe**.
4. Type the IP address or host name and port for the OS Manager server. This must be specified in the following format: *xxx.xxx.xxx.xxx*:*port*.

   If the Image Preparation Wizard cannot connect to the OS Manager server, a message opens and you must:

   - Click **Yes** to continue anyway.
   - Click **No** to modify the host name or IP address.
   - Click **Cancel** to exit the Image Preparation Wizard.
5. Click **OK**.

   The wizard prepares the image.

   The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

   If the device does not boot to the CD (boots to Windows CE instead) you will need to restart the process.

The upload of the image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a bottleneck. Transfer speeds will be approximately 30-400 Kbps but may vary depending upon processor speeds and your network environment.

You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

6 The Image Preparation Wizard connects to the network, and stores the image on the OS Manager server in the `/upload` directory.

When the upload process is complete, you will see the following messages

```
OS image was successfully sent to the OVCM OS Manager Server
**** If you had inserted a CD remove it now and reboot
```

7 Reboot the reference machine and readjust your boot settings if necessary to return to the original operating system.

Next, you will want to publish your image to the Configuration Server DB. See Chapter 5, Publishing to the HP Client Automation Configuration Server Database.

## Linux-based OS images

### Task 1 Prerequisites for a Linux-based thin client image capture

- Product media
- Image Preparation CD-ROM

### Task 2 Install the Application Manager on the Linux-based Reference Machine

For additional thin client device information see Installing the Application Manager on Thin Clients on page 39 or the readme file included with `ThinClient.tar`.

1 Login to the target thin client device.

2 Create a new directory called `/mnt/opt/OVCM`.

3 Copy the contents of `ThinClient.tar` (located on the product media in the `/ThinClient/Linux` directory) to `/mnt/opt/OVCM`.

Depending on your device model, you may have to extract the contents from `/tmp` or on another machine as some models do not have sufficient disk space to contain both the tar file and its exploded contents (requires approximately 7-8 MB free). After extracting the contents, delete the `ThinClient.tar`.

4 Change the current directory to `/mnt/opt/OVCM` and run the installation by typing:

`./install –E –i HPCA_Configuration_Server`

Where *`HPCA_Configuration_Server`* is the hostname or IP address of the Configuration Server.

The Application Manager is installed.

### **Task 3** Run the HP Client Automation OS Manager Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.

2 Restarts the reference machine into the service operating system (booted from the Image Prep CD you created). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.

3 Creates and copies the following files to *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload` on the OS Manager Server.

— `ImageName.DD`
This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Linux-based images can be deployed only to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.

— `ImageName.EDM`
This file contains the object containing inventory information.

While these files are transferred, network speed will be less than optimal as the operating system image is compressed during transfer.

A comprehensive log (*machineID-all*.log) is also available in *SystemDrive*:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload after the image is deployed.

### To use the Image Preparation Wizard

1. Insert the ImageCapture media into the reference machine. Thin client devices require a USB CD-ROM drive. See Product Media on page 29 if you need more information about where to get this media.

   On certain Linux thin client models, the CD-ROM may be mounted by default with the noexec option, which prevents execution from the CD-ROM. This will result in a permissions error or otherwise failed execution when trying to run the Image Preparation Wizard. Re-mounting the CD-ROM without the noexec option will resolve this issue.

2. On the Image Preparation CD, go to /image_preparation_wizard/linux and run ./prepwiz.

   The Welcome window opens.

3. Click **Next**.

   The End User Licensing Agreement window opens.

4. Click **Accept**.

5. Type the IP address or host name and port for the OS Manager server. This must be specified in the following format: *xxx.xxx.xxx.xxx*:*port*.

   If the Image Preparation Wizard cannot connect to the OS Manager server, a message opens and you must:

   - Click **Yes** to continue anyway.
   - Click **No** to modify the host name or IP address.
   - Click **Cancel** to exit the Image Preparation Wizard.

6. Click **Next**.

   The Image Name window opens.

7. Type a name for the image file. This is the image name that will be stored in the /upload directory on the OS Manager server.

8 Click **Next**.

A window opens so you can enter a description for the image.

9 Type a description for the image file.

10 Click **Next.**

The Options window opens.

11 Select the appropriate options.

**Perform client connect after OS install.**
Select this check box to connect to the OS Manager server after the OS is installed to verify the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.

12 Accept the defaults and click **Next**.

The Summary window opens.

13 Click **Start**.

14 Click **Finish.**
The wizard prepares the image.

15 Click **OK**.

The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit F10 during the reboot process and change the boot order in the configuration settings).

If the device does not boot to the CD (boots to Linux instead) you will need to restart the process.

The upload of the image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a bottleneck. Transfer speeds will be approximately 30-400 Kbps but may vary depending upon processor speeds and your network environment.

You may want to create copies of the files stored in the `\upload` directory so that you can retrieve them if necessary.

16 The Image Preparation Wizard connects to the network, and stores the image on the OS Manager server in the `/UPLOAD` directory.

When the upload process is complete, you will see the following messages:

```
OS image was successfully sent to the OS Manager Server
**** If you had inserted a CD remove it now and reboot.
```

17 Reboot the reference machine and readjust your boot settings if necessary to return to the original operating system.

Next, you will want to publish your image to the Configuration Server DB. See Chapter 5, Publishing to the HP Client Automation Configuration Server Database.

# 5 Publishing to the HP Client Automation Configuration Server Database

At the end of this chapter, you will:

- Be able to use the Publisher to publish your operating system image to the Configuration Server DB.

After you have created your image, you must use the Admin Publisher to publish it to the Configuration Server DB.

Publishing is an administrative task that should be done in a non-production lab environment.

For more information about the Admin Publisher, see the *HP Client Automation Enterprise Administrator User Guide*.

# Prerequisites for publishing .WIM images of a Windows Vista OS or Windows Server 2008

If you are publishing a `.WIM` image of a Windows Vista operating system you must:

- Copy the `\agent` folder from the agent media to the device where you are publishing the image. This folder is only required the first time you publish a `.WIM` file or if you want to publish an updated agent package. The agent will be published as a separate package which ensures that all future deployments of your `.WIM` files will automatically receive the latest agent available.

Do not make any modifications to the default installation path in install.ini.

- If you are deploying using Windows Setup, you must be able to access the `\sources` folder from the Windows Vista or Windows Server 2008 media (used to obtain or create the .WIM file) on the device where you are publishing the image.
- Install WAIK.
  - If you are using the x86 platform, WAIK must be installed under `C:\Program Files\Windows AIK\`
  - If you are using the x64 platform, WAIK must be installed under `C:\Program Files (x86)\Windows AIK`.
- If you are using an existing *`filename`*`.wim` or created one using the System Information Manager (SIM) tool, copy the file to the device where you are publishing the image.

- If you prepared and captured a `.WIM` file using the Image Preparation Wizard, copy *`filename`*`.wim` and *`filename`*`.edm` from the OS Manager Server's `\upload` directory to the device where you are publishing the image.
- Copy `substitutes` and `unattend.xml` to the same directory as *`filename`*.wim. Samples of these files are available on the Image Capture media in`\samples`. If you choose to use the samples, modify information as needed such as the setting the time zone and entering the product key. See the instructions below for more information.

  Note that all of these files must have the same prefix. For example, `filename.wim`, `filename.subs`, and `filename.xml`.

Confirm that all files and folders in the directory are not set to read-only. If they are set to read-only, the image may not deploy.

## About the .subs and .xml files

*`Filename`*`.subs` and *`filename`*`.xml` are used to customize information. During deployment of the operating system, *`filename`*`.subs` and *`filename`*`.xml` will be combined to create `unattend.xml` which provides information during all phases of the Windows setup on the target device.

*`Filename`*`.xml` is an answer file that contains standard information as well as placeholders for information that will be included from *`filename`*`.subs`. If you choose, you can use the *`filename`*`.xml` provided and use Microsoft's Windows System Image Manager (SIM) tool to make additions to this file. If you do so, you must open the corresponding `.WIM` file before opening *`filename`*`.xml`.

You must specify your Windows Vista installation product key in this file.

*Do not delete any XML values from this file!* If you modify this file incorrectly, you may cause your installation to fail.

If you see errors in the Messages section in the SIM tool similar to "…The value $$SUBSTR$$ is invalid…" you can ignore them. When you save the file you may also see a message similar to "There are validation errors in the answer file. Do you want to continue?" Click **Yes** to continue.

*Filename*.subs is the substitutes file that lists each XML item to be modified in *filename*.xml and what its value should be modified to. The lines in the substitutes file are called XPATHs.

Information entered in the *filename*.subs file takes precedence over information in the *filename*.xml file.

## Example of Substitution

If you want to see how substitution works, you can review the following example which will show how the JoinDomain attribute gets set from anything in the *filename*.xml to VistaTeam in the unattend.xml.

Code that appears within < > should appear all on one line in the xml file.

2 Review the XML element for JoinDomain which has been extracted from a *sample*.xml file.

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
          <component name="Microsoft-Windows-Shell-Setup"
          processorArchitecture="x86"
          publicKeyToken="31bf3856ad364e35" language="neutral"
          versionScope="nonSxS"
          xmlns:wcm="http://schemas.microsoft.com/WMIConfig/20
          02/State"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-
          instance">
            <Identification>
                <JoinDomain>anything</JoinDomain>
            </Identification>
        </component>
    </settings>
          <cpi:offlineImage
          cpi:source="wim://hpfcovcm/c$/vista_inst/vista.wim#W
          indows Vista ULTIMATE" xmlns:cpi="urn:schemas-
          microsoft-com:cpi"/>
</unattend>
```

2 Modify the following XPATH element in the *sample*.subs. Note that this XPATH element appears on a single line in the *sample*.subs file.

```
//un:settings[@pass='specialize']//un:component[@name='Microso
ft-Windows-Shell-
Setup'][@processorArchitecture='x86']/un:Identification/un:JoinDomain,VistaTeam
```

3 During deployment of the operating system, the *filename*.subs and filename.xml files will be combined to create unattend.xml that provides information during all phases of the Windows setup. In this example, the JoinDomain attribute will be set to VistaTeam. Below you can see an example of the customized XML element.

```
<?xml version="1.0" encoding="utf-8"?>

<unattend xmlns="urn:schemas-microsoft-com:unattend">

   <settings pass="specialize">

    <component name="Microsoft-Windows-Shell-Setup"
   processorArchitecture="x86"
   publicKeyToken="31bf3856ad364e35" language="neutral"
   versionScope="nonSxS"
   xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/Stat
   e" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

      <Identification>

      <JoinDomain>VistaTeam</JoinDomain>

      </Identification>

   </component>

   </settings>

<cpi:offlineImage
cpi:source="wim://hpfcovcm/c$/vista_inst/vista.wim#Windows
Vista ULTIMATE" xmlns:cpi="urn:schemas-microsoft-com:cpi"/>

</unattend>
```

## Preparing filename.xml

Use the SIM tool to modify the product key and any other information that you must modify for your environment.

# Using the Admin Publisher

## To use the Admin Publisher

1. Go to **Start→All Programs→HP Client Automation Administrator→Publisher→Client Automation Admin Publisher**.

   The Logon screen opens.

2. In the User ID text box, type your HPCA Administrator user ID (by default **`rad_mast`**).

3. In the Publishing Options windows select **OS Image** from the drop-down list.

4. Click **OK**.

5. Use the Select window to find and select the file you want to publish (typically stored in the `\upload` directory on the OS Manager Server). Only supported file types appear in the window.

   If you select a `Sysprep.inf` file or a `unattended.txt` file, a field appears where you must type the instance name. When you click **Next**, you will skip directly to the final step because you will not be creating a service for these files. Sysprep and unattended text files are published to the SYSPREP class in the OS domain of the Configuration Server DB. Use the Portal to view your published instances and then connect them to the appropriate OSs.

   If you are publishing the agent to be used with a `.WIM` file, you must have copied the `\agent` folder from the agent media to this device. Then, be sure to select the appropriate `.msi` file.

6. Use the information in the Description box to verify that you have selected the correct file before you continue. You can also add information to the description if you choose.

7. Click **Next**.

   If you chose to publish a .WIM file, the WIM Deployment Configuration window opens. If you are publishing an .IMG file, you can skip to the next step.

a From the Deployment method drop-down list box, select the appropriate method. See Deployment Methods on page 62 for more information.

If you created your .WIM file using the Image Preparation Wizard, select the same deployment method here as you did when you created the .WIM file.

If you are using an existing `.WIM` (Windows Imaging Format) or are creating one using the System Information Manager (SIM) tool, you must use the Microsoft Setup method.

b If you chose Microsoft Setup, from the Sources directory text box, browse to the sources directory from the Windows Vista installation media.

c In the Client media location, browse to the correct path for the agent media. It may take a few moments for the path to appear.

If you have already published this, you can select **Use an existing package published previously** and then select the appropriate package.

8 Click **Next**.

9 Use the Package Information section to enter the package information. Note that the Limit package to systems with section is not available when publishing OS images.

10 Click **Next**.

11 On the Configure window, select **Create new**.

If you are publishing the agent, select **No Service**.

12 Enter the appropriate information in the rest of the fields.

13 In the Assignment type group box, select whether the service is mandatory or optional. By default, Mandatory is selected, which will distribute this service to all available subscribers.

Optional services are only available if you are using the Application Self-service Manager. Refer to the *HP Client Automation Enterprise Application Manager and Application Self-service Manager Installation and Configuration Guide* for more information about mandatory versus optional services.

14 Click **Next**.

15 Review the Summary section to verify the package and service information you provided during the previous steps. When you are satisfied, click **Publish**.

16 Click **Finish** to exit the Admin Publisher.

Use the Portal to view your service, which is now ready for distribution to your enterprise.

Remember, Sysprep files are published to the SYSPREP class in the OS domain of the Configuration Server DB. Use the Portal to view your published Sysprep files.

# 6 Operational Overview

At the end of this chapter, you will:

- Understand how a target device is discovered.
- Understand how to bring a device to its desired state.
- Understand the policy classes used for OS management.
- Understand how to determine policy assignments.
- Understand how to handle ambiguities in policy resolution.
- Use the OS Manager Admin Module to prepare and deploy operating systems to target devices.

This chapter provides information on how to use the OS Manager and Portal to prepare your operating system images for deployment to the appropriate target devices. The OS Manager allows for OS installations on bare metal devices, migration of existing OSs, and disaster recovery of devices.

Hardware Configuration Management, Defining Drive Layouts, Multicast, getmachinename.tcl, Downloading Resources, Sysprep, and image PIC compatibility are not supported on thin clients. 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 simply be ignored on a thin client device.

# About Discovery

When a target device boots, it communicates with the OS Manager Server to determine whether a ROM object exists. This process is called **discovery**. If a ROM object does not exist, one will be created the first time the target device communicates with the OS Manager Server. After a ROM object is established in the Portal, the OS Manager Server and the target device can communicate. Use the Portal to view the ROM object, which is stored below the target device in the Devices container. See About the OS Manager Administration Classes on page 114.

If a ROM object *does* exist, what happens depends on several factors, such as whether the device has an OS installed or how policy is defined. The following table provides several scenarios and the expected results.

In order to implement any changes to your operating system based on policy, a HPCA OS connect must run before the target device reboots.

**Table 4 Expected Results on target device**

| If the target device... | then... |
|---|---|
| is a bare metal machine and no policy is assigned | nothing will happen until policy is assigned.<br>Note: The default behavior is to prompt the user for workstation or role. However, if no policy is assigned, no OS can be installed. The user will be informed of this and instructed to press **Enter**. The device shuts down. |

| If the target device... | then... |
|---|---|
| is a bare metal machine and policy is assigned | the appropriate OS is installed, a ROM object is created and the device is considered to be under Client Automation management. |
| has an OS that was not installed by the OS Manager and no policy is assigned | the OS Manager discovers the device but considers it *unmanaged* and a ROM object is created; however, the installed OS remains on the machine. |
| has an OS that was not installed by the OS Manager, has the HPCA OS Manager User Agent installed, and policy is defined | after the next HPCA OS connect a ROM object will be created.<br>The behavior settings will determine how and when the installation will take place (e.g., whether the resolved OS is installed or not, whether a user is prompted or not). |
| has a corrupted partition table and `PMDISCRV=_CONFIRM_` | the target device shuts down so that the administrator can recover data from the target device. |
| has a corrupted partition table and `PMDISCRV=_AUTO_` | the appropriate OS is re-installed. |

After devices are under Client Automation management, the OS will be changed if a device is not in the desired state. A device may not be in the desired state if:

- There is a change in policy.
  When policy is modified, the current OS on a device may no longer be applicable. In other words, the list of OS services returned as a result of policy resolution does not include the currently installed OS. This will trigger installation of an OS so that the device's OS is in the desired state.

  *You typically use policy to manage your OSs*.

  An example of this occurs during an upgrade where the desired OS changes from Windows 2000 to Windows XP.
- It does not have a local OS (bare metal).
- There is administrator intervention.
  In some cases, you may wish to install an OS regardless of what is currently on the device e.g., when a device has a corrupted local hard drive which can no longer successfully boot the local OS.

# About Policy

The OS Manager uses the following classes in the POLICY Domain.

- Machine manufacturers (MANUFACT)
- Machine models (MODEL)
- Machine roles (ROLE)
- Machine subnets (SUBNET)

These classes are resolved in the following order: ROLE, MANUFACTURER, MODEL, and SUBNET. *This order is subject to change*. See Determining Policy Assignments below for important information about implementing policy,

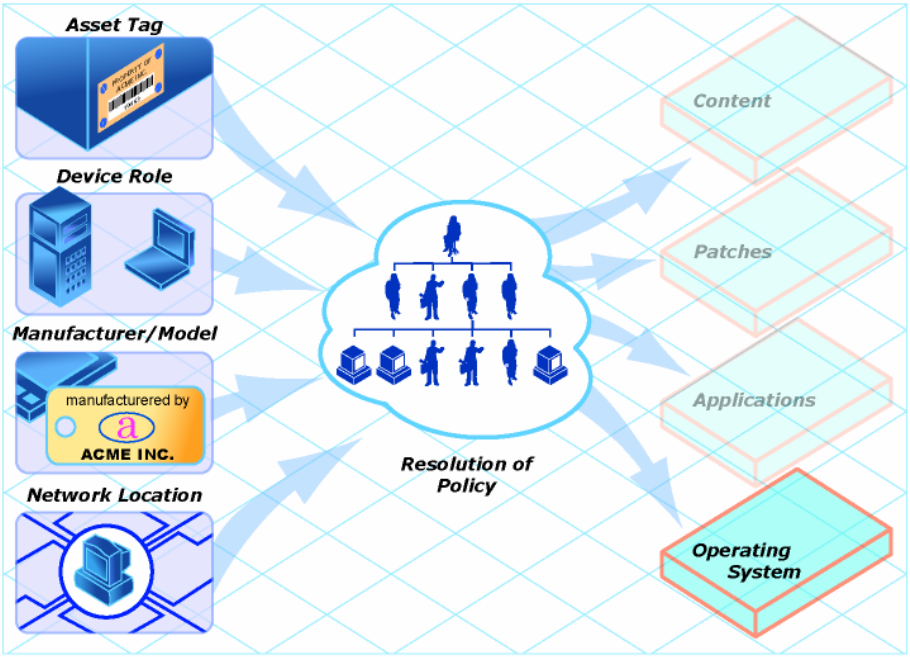
Manufacturer, model, and subnet are based on attributes related to a device. Role is *not* based on a device's attributes. It is simply a grouping of devices, similar to how you might assign policy based on departments. You can set policy based on a device's assigned role—such as server or workstation.

Role is the only criterion that you can use to allow a user to determine the OS that is installed on the device. Note that to allow a user to select an OS, you must set the system behaviors accordingly (see Setting Behaviors on page 123). After a role is selected by the user, only you, the administrator, can reset it to a different value, or to empty, so that the user may select the role again.

## Determining Policy Assignments

We recommend that you select a single criterion for policy.

**Figure 3 Resolution of Policy**




In order to determine which criterion to use, look at your overall environment. In general, you will probably most often assign policy by subnet or role.

- If your environment is divided by subnets, you may choose to use the SUBNET criterion. For example, server farms are typically defined by subnets.
- If your environment is a build center, it may make sense to use the ROLE criterion so that users can select what OS should be installed.
- If your environment is standardized by hardware, then you may choose to use the MANUFACTURER or MODEL criterion. For example, one vendor makes all the laptops in your environment and a different vendor makes all of the workstations in your environment, you may decide to use the manufacturer class. These criteria will probably be used less often than the others because it may be unusual to use a certain model or manufacturer throughout your environment.

In general, you should use policy to determine the OS to be installed. Occasionally, you may want to assign a specific OS directly to a device. This can be useful for testing purposes; however it should be considered the exception to the rule. This is not recommended. Remember—policy rules.

If you have followed the recommendation to use one criterion to determine policy, your OSs will deploy as expected.

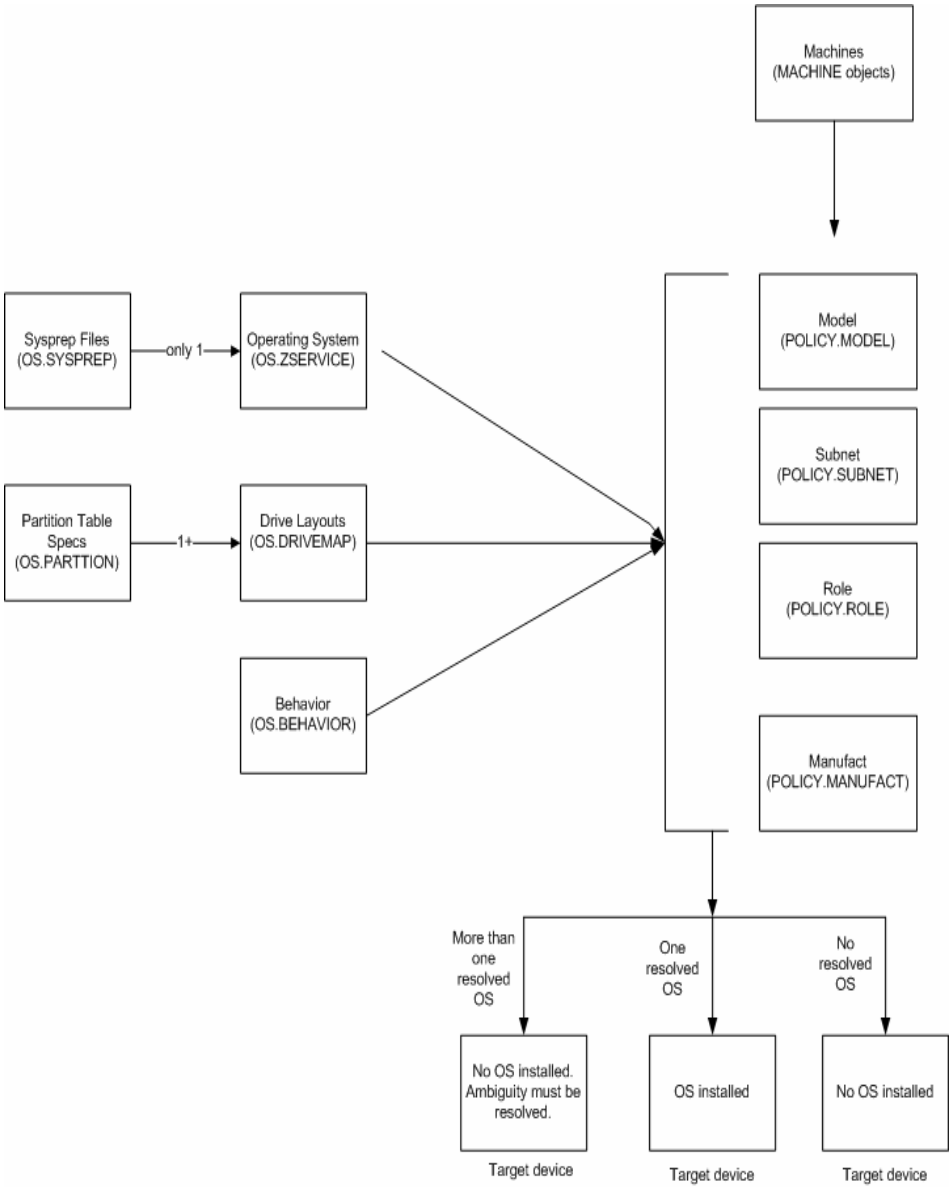
## Ambiguities in Policy Resolution

At times, you may find that more than one OS has been resolved for a device. We call this an **ambiguity**. You may need to use the behavior settings to arbitrate the ambiguity if more than one criterion was used to determine policy. See Setting Behaviors on page 123 for more information about determining who is responsible for selecting the appropriate OS.

In some situations, you may intend to cause an ambiguity. An example of this would be if you have a test lab that is on its own subnet, yet you want users to have the option to rebuild the devices frequently, choosing from one of three OSs. You would assign policy by subnet and role, but you would also have to set the behavior to prompt the user to select the role.

Below is an overview of how the classes relate in order to determine what OS is installed on a target device.

**Figure 4 Class relationships**



# Performing OS Manager Administrative Tasks in the Portal

Use the HPCA OS Manager Administration tasks in the Portal to prepare your OSs and initiate deployment. Remember, you must be familiar with the Portal to complete these tasks.

## Logging On

### To log on to the Portal as a HPCA OS Manager administrator

1. Open your web browser.
2. In the Address bar, type **`http://IP_AddressForCMPortal:3471.`**
3. In the User Name box, type **`ROMADMIN`** to log in as the OS Manager administrator.
4. In the Password box, type a password. The password is case-sensitive.

   The pre-defined password is *secret*.

   Be sure to change your password before moving the Portal with the OS Manager administrative tasks into your production environment.
5. Click **Login** or press **Enter**.

## About the OS Manager Administration Classes

### To access the OS Manager Administration classes

1. Go to Desktop, Zone: *`ZoneName`*, Configuration, Configuration Servers and select the appropriate HPCA Configuration Server service for the OS Manager.
2. In the workspace, the following icons appear.
   - Behaviors
     Lists the settings for how the OS Manager behaves. You can assign different system behaviors to different target devices. See Setting Behaviors on page 123.

— Drive Layouts
Lists the types of partitions that you can add or copy, and allows you to configure new partitions. See Defining Drive Layouts on page 138.

— HW Config

Stores objects that contain the information about how a target device's hardware must be configured in order for it to be ready for operating system installation. Refer to the *HP Client Automation Enterprise OS Manager Hardware Configuration Management System Administrator Guide*.

— HW Config Element

Stores the objects that contain information about the resources required for a Hardware Configuration Management operation, the sequencing of operations, and how the operation is to be carried out. Refer to the *HP Client Automation Enterprise OS Manager Hardware Configuration Management System Administrator Guide*.

— Machine Manufacturers
Used to set policy based on the device's manufacturer.

— Machine Models
Used to set policy based on the device's model.

— Machine Roles
Used to set policy based on the device's role.

— Machine Subnets
Used to set policy based on the device's subnet.

— Operating Systems
Stores the OS services to be deployed to your target devices.

— Sysprep Files
Lists the Sysprep files and unattend.txt files stored in your database. See Connecting a Sysprep File on page 145.

## Using the HPCA OS Manager Administration tasks

Use the HPCA OS Manager Administration task group to manage the various criteria as well as define policy structures.

Before you begin using the individual tasks, it is recommended that you review some typical scenarios and the procedures that you might follow when preparing to deploy OSs to your target devices. The table below provides sample scenarios and a summary of the tasks that you can use in each of

these situations. See the referenced descriptions listed with the individual tasks to learn how to use the OS Manager Admin Module to complete the tasks.

To use the scenarios below, you must be logged into the Portal as a HPCA OS Manager administrator.

**Table 5 Administrative Procedures**

| If you want to... | Then... |
|---|---|
| Install an OS on a bare metal machine<br>Note: This does not apply to Local Service Boot implementations. | 1 Create any necessary policy instances, such as subnet or role. See Creating an Instance on page 129.<br>2 Connect the policy instances to the OS service. See Connecting Operating Systems on page 130.<br>3 If you do not want to use the default behavior (the Undefined instance in the Behavior class), you can modify the behaviors. See Setting Behaviors on page 123.<br>4 Boot the target device. When the device boots up, the appropriate OS (according to policy) is installed and a ROM object is created. |
| Bring an unmanaged machine with an installed OS under Client Automation management and install the appropriate OS as per policy.<br>Reminder: The target device must have the Application Manager with the HPCA OS Manager feature installed. | 1 Boot the target devices so that discovery occurs. Note that the OS State is set to Desired and the Current OS and Selected OS are Unmanaged.<br>2 If necessary, use the Filter Machines task to determine which devices are unmanaged. See Filtering Machines on page 132.<br>3 If necessary, create policy instances, such as department, machine, model, or subnet. See Creating an Instance on page 129.<br>4 Connect the policy instances to the OS service. See Connecting Operating Systems on page 130.<br>5 Run an HPCA OS connect (via Notifying Target Devices) and select the Bringing Machines under Management task which initiates a reboot of the device and starts the migration process. |
| Force a re-installation of the current OS without retaining any existing data. | 1 Use the Force OS Install task. See Forcing an OS Installation on page 134.<br>2 Reboot the target device.<br>3 Run an HPCA OS connect. |

| If you want to... | Then... |
|---|---|
| Force the installation of a valid OS that you choose without retaining any existing data. | 1 Assign policy so that the new OS that you want to install is the *only* OS connected to policy.<br>2 Use the Force OS Install task. See Forcing an OS Installation on page 134.<br>3 Run an HPCA OS connect.<br>4 Reboot the target device. |
| Initiate the installation of a different OS. | 1 Set the Select OS (PMACKOVW) behavior to _NEVER_ to give the administrator control over policy. See Setting Behaviors on page 123.<br>2 Assign policy so that the new OS that you want to install is the *only* OS connected to policy.<br>3 Use the Re-evaluate/install OS task to re-evaluate the state of the OS and install a new one based on policy. See Re-evaluating the Operating System on page 133.<br>4 Run another HPCA OS connect and the device will reboot and install the new OS. Note that if you do not set the Behavior to NEVER the user will be prompted to confirm whether they want to reinstall the OS. |
| Allow the user to decide which OS to install. | 1 Verify that your policy will result in more than one OS available for the target devices.<br>2 Set the Select OS (PMSLCTOS) behavior in the Undefined behavior to _LOCAL_. See Setting Behaviors on page 123.<br>3 Use the Re-evaluate/install OS task to re-evaluate the state of the OS and install a new one based on policy. See Re-evaluating the Operating System on page 133.<br>4 Run an HPCA OS connect. |
| View a list of devices that have more than one resolved OS and then select the OS to be installed. | • Use the Select OS for pending machines task. See Selecting an Operating System on page 131. |

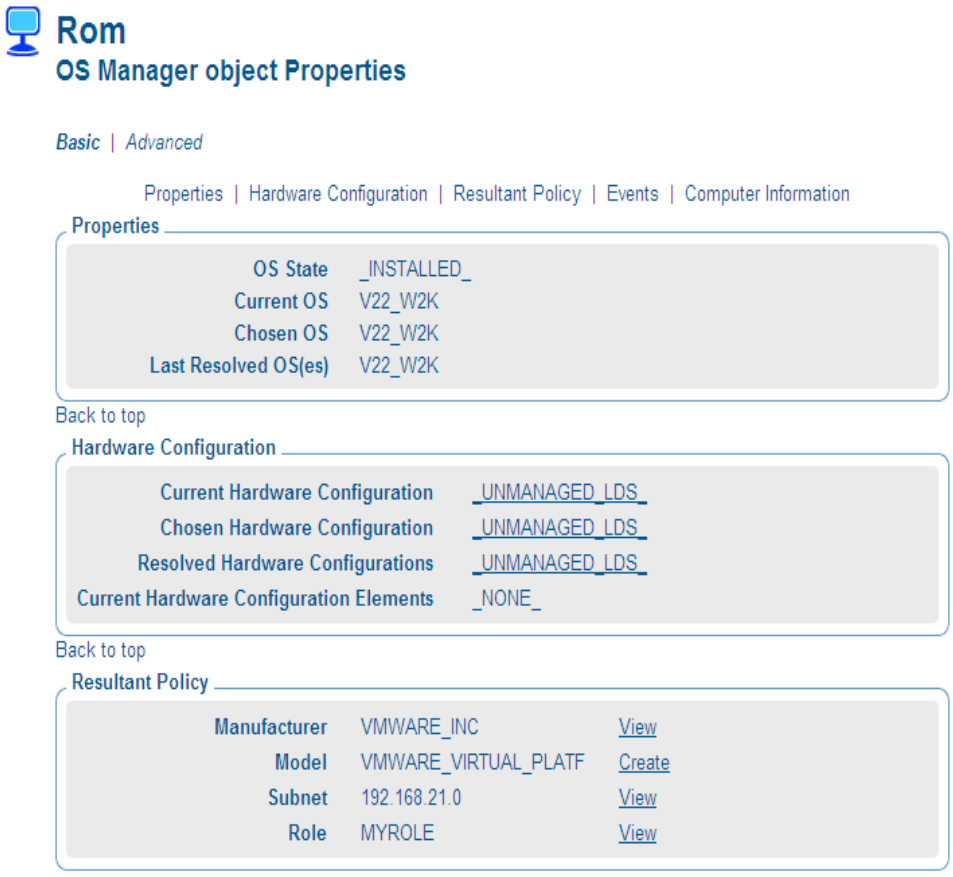
| If you want to... | Then... |
|---|---|
| The following are additional options that can be used in many scenarios | |
| Use an override Sysprep file. | • Connect a Sysprep instance to the operating system instance. See Connecting a Sysprep File on page 145. When the OS is deployed to the target device, the override Sysprep file will be merged with the Sysprep file that is embedded in the OS. |
| Add partitions. | 1 Use the Drive Layouts Class to specify the type of partition. See Defining Drive Layouts on page 138.<br>2 Add a partition. See Adding Partitions on page 140. All existing data will be lost.<br>3 Assign the appropriate drive layouts to your target devices. See Connecting Drive Layouts on page 140. |
| Create a replace, cache, or merge type partition. | 1 Use the Drive Layouts class to specify the type of partition. See Defining Drive Layouts on page 138.<br>2 Assign the appropriate drive layouts to your target devices. See Connecting Drive Layouts on page 143. |

## Viewing the ROM Object

Earlier you learned that the ROM object is created in the Portal when a device is discovered by the OS Manager Server. For more information review the topic About Discovery on page 108. In order to perform many of the tasks to prepare an OS for deployment, you must have a ROM object.

To view a ROM object, select the appropriate Zone from the desktop and click on Devices. Then select the managed device you want to view and click the ROM object. The Properties window opens.

**Figure 5 ROM Object Properties window**




This window is separated into several sections: The Properties section displays the OS Manager-specific attributes for the device.

**Table 6 ROM Object Attributes - Properties**

| Field | Description |
|---|---|
| OS State | Indicates the state of the OS on the target device.<br>• _INVALID_ –OS Manager will install a valid, managed OS.<br>• _DESIRED_ – The device is already managed and has a valid OS.<br>• _INCONSISTENT_ – The machine is managed, but the OS must be repaired.<br>• _INSTALLED_ – A temporary state after the gold image has been installed and before a connection with the OS Manager Server. After the HPCA OS connect, the correct OS will be installed and the OS state will change to _DESIRED_.<br>Default: _INVALID_ |
| Current OS | Indicates the OS that is successfully installed on the device. This represents the ZSERVICE instance in the OS class.<br>Default: _NONE_ |
| Chosen OS | Indicates the OS to be installed on this device.<br>Default: _NONE_ |
| Last Resolved OSs | Indicates the OSs resolved for this device.<br>Default: _NONE_ |

- The Hardware Configuration section displays information about the current hardware configuration, including the Hardware Configuration Elements that have been successfully applied. Refer to the *HP Client Automation Enterprise OS Manager Hardware Configuration Management Guide* for more information.
- The Resultant Policy section displays policy for the device. If policy does not already exist, you can click **Create** to create a policy instance. If policy does exist, you can click **View** to see the existing policy assignments.

**Table 7 ROM object Attributes – Resultant Policy**

| Field | Description |
|---|---|
| Manufacturer | Manufacturer reported by SMBIOS. |

| Field | Description |
|---|---|
| Model | Model reported by SMBIOS. |
| Subnet | Current subnet. |
| Role | Specifies the role selected for this device by the local user or the administrator (depending on the PMROLE setting in the BEHAVIOR class of the OS domain).<br>Default: _NONE_ |

The Events section displays the last five events that have been reported.

The Computer Information section displays all of the MACHINE attributes that contain values. These values are stored in the Configuration Server.

**Table 8 ROM Object Attributes - Computer Information**

| Field | Description |
|---|---|
| Computer Name | Computer Name.<br>If the ROM object exists and there is a successful HPCA OS connect, this attribute will be updated with the computer's current information. |
| Display Name | The friendly name for the ROM object. |
| DNS Host Name | The host name of the machine. |
| Enclosure Manufacturer | Manufacturer of the enclosure. |
| Enclosure Serial Number | Serial number for the enclosure. |
| Enclosure Type | Type of the enclosure. |
| IP Address | The target device's IP address. |
| ACPI BIOS? | Indicates whether the device has ACPI BIOS.<br>• Y – indicates the device is ACPI-compliant.<br>• N – indicates the device is not ACPI-compliant. |
| APIC | Indicates whether the device has an Advanced Programmable Interrupt Controller. |
| Mass Storage Interface | Indicates the mass storage interface - IDE or SCSI. |
| Boot drive disk space (MB) | Disk space on the boot drive in MB. |

| Field | Description |
|---|---|
| Number of CPUs | Number of CPUs in the target device. |
| CPU Speed (MHz) | CPU speed in MHz. |
| Current IP Address | Current IP address. |
| MAC Address | MAC address is a unique identifier derived from the NIC card. |
| Memory (MB) | Computer's total memory. |
| Subnet | The current subnet. |
| Sys Locator Enclosure Name | (Compaq-specific) EnclosureName field from the SMBIOS Locator structure. For HP-Compaq blades, this might be the user-defined enclosure name. |
| Sys Locn Enclosure Sys Bay | (Compaq-specific) EnclosureSystemBay field from the SMBIOS Locator structure. For Compaq blades, the relative location of this blade is in the enclosure. |
| Baseboard Location in Chassis | LocationInChassis field from the SMBIOS BaseBoardInformation structure.<br>Note: For Dell and IBM blades, this stores the relative location of this blade inside the enclosure. Also for Dell and IBM blades, the enclosure name might be found in the SerialNumber field of the SMBIOS SystemEnclosure structure; it will be in SMINFO under the name SNENCLOS. The format of all of those four raw information fields is entirely manufacturer/model specific. |
| Manufacturer Derived from SMBIOS | Manufacturer reported by SMBIOS. |
| Model Derived from SMBIOS | Model reported by SMBIOS. |
| Current Subnet Mask | Current subnet mask. |
| Device Architecture | The processor architecture (CPU). |
| Baseboard Serial Number | The serial number for the baseboard. |

| Field | Description |
|---|---|
| Enclosure Asset Tag | The asset tag for the enclosure. |
| SMBIOS Enclosure S/N | System Enclosure Serial Number from the SMBIOS. |
| Number of Processors | The number of processors in the device. |
| Processor Family | The processor family. |
| Processor Type | The type of processor. |
| SMBIOS Manufacturer | Manufacturer. |
| SMBIOS Product | System Product (model number) from the SMBIOS. |
| SMBIOS System S/N | System Serial Number. |
| SMBIOS Machine Unique UID | Machine Unique ID from the SMBIOS. |

## Setting Behaviors

You can assign system behaviors to your target devices based on policy. If you do not assign a behavior to policy, the Undefined Behavior (_NULL_) instance is the default.

For example, you may want to configure some managed devices to require that the user acknowledge that this OS is about to change, while others may not require user acknowledgement.

You must be very careful if you are using more than one Behavior instance, because these instances determine the behavior of the system. You may have unintended consequences if this is not performed properly. For example, if you set the wrong policy, you may inadvertently allow users to make policy changes, or an unattended device may become stuck at a prompt.

It is highly recommended that you connect one Behavior instance to one Policy instance only.

One potential way to prevent errors would be to connect Behavior instances to mutually exclusive instances of different policies.

### To set the behaviors

1. Use the navigation aid to select the appropriate Configuration Server.
2. In the workspace, click **Behavior**.
3. Create a new instance.

   or

   Click an instance in the workspace and then click **Modify** to make changes to an existing instance.

If you do not know how to create or modify instances, refer to the *Client Automation Portal Installation and Configuration Guide* or follow the steps in Creating an Instance on page 129 or Modifying Instances on page 138.

Table 9 describes the attributes for the Behavior class.

**Table 9 Attributes of the BEHAVIOR class**

| Field | Attribute in CM Configuration Server Database | Description |
|---|---|---|
| Instance | BHVRINST | Instance Name |
| Select ROLE | PMROLE | Indicate whether the user is allowed to select a machine role.<br>• _LOCAL_<br>displays a user interface so a user at the target device can select a role for the device. The list of available roles, determined from the instances in the POLICY.ROLE class in the Configuration Server DB, is displayed.<br>• _CENTRAL_<br>does not display the user interface. The administrator can assign a role, if necessary.<br>A role selection remains in effect until you (the administrator) void or overrule the selection.<br>Default: _LOCAL_ |

| Field | Attribute in CM Configuration Server Database | Description |
|---|---|---|
| Select OS | PMSLCTOS | Indicates whether the user or administrator is responsible for action if policy resolves more than one OS for the target device.<br>• _LOCAL_<br>displays a choice of OSs so the user can make a selection.<br>Note: If a device prompts the user to make a selection even though it already contains a managed OS, it will also give the user the option to use the existing OS. For example, this would occur if a device is managed, but the ROM object was deleted from the Configuration Server DB. This option allows the user to preserve the existing data and applications.<br>• _CENTRAL_<br>delays installation until the administrator specifies the Chosen OS. (SLCTDOS).<br>An OS selection remains in effect until you (the administrator) void or overrule the selection or policy changes.<br>Default: _LOCAL_ |
| OS Overwrite Prompt | PMACKOVW | Indicates whether to prompt the user before overwriting or modifying the OS. If the prompt is displayed, it will ask the user to select “install,” “use,” or in some cases (where you have a valid OS with minor changes), “refresh.”<br>• “Install” creates a ROM object and installs the OS on the device.<br>• “Use” creates a ROM object, does not install the OS and considers the device to be unmanaged.<br>• “Refresh” reinstalls the existing OS, but includes updates to the OS made using the OS Manager Admin Module.<br>Use one of the following to set PMACKOVW.<br>• _ALWAYS_ (Default)<br>Prompts the user only if there is a valid |

| Field | Attribute in CM Configuration Server Database | Description |
|---|---|---|
| | | file system (including a valid Master Boot Record) on the machine.<br>• _NEVER_<br>Does not prompt the user, but installs the OS.<br>— Caution: NEVER is designed for use in bare metal machines or kiosk situations. Use this option with caution, as the user will not be prompted before the OS is overwritten.<br>• _VALID_<br>Prompts the user only if the current installation is valid. If there is a valid OS on the device where an OS is to be installed, the user will be prompted to overwrite the OS. If there is no valid OS, the user will not be prompted and the OS will be installed without user intervention. |
| Timeout for user response (seconds) | USERTO | Specifies how long a message displays to the user before continuing.<br>• Set USERTO = -1<br>to wait indefinitely for input by the user.<br>• Set USERTO = *number of seconds*<br>to wait the specified length of time before continuing. |
| Download:<br># bytes/sec (opt K/M/G) | BANDWITH | The bandwidth throttle used by each target device. For example, 1000K.<br>• If this attribute is left empty, the download process will run at the maximum speed of the network interface.<br>• You can specify bandwidth throttle in Kbs (K), MB/sec (M), or GB/sec (G). The default definition is in bytes/sec. The default value is blank (no bandwidth limitation). |
| RunOnce parameter string | RUNPARAM | You must modify this parameter to specify the IP address for your Configuration Server. If you |

| Field | Attribute in CM Configuration Server Database | Description |
|---|---|---|
| | | do not modify this parameter, your target device will not be able to successfully run an HPCA OS connect.<br>Specifies the parameters that are appended to the radskman command line. This command line will run after the OS has been installed, and will install the target device's applications. For additional parameters, refer to the *HP Client Automation Enterprise Application Manager and Application Self-service Manager Installation and Configuration Guide* and the HP support web site.<br>• For the IP parameter value, enter your CM Configuration Server IP address or DNS name.<br>• The cop=y parameter must included to meet the requirement that COP must be enabled to use the OS Manager. |
| Action on existing OS upon Machine Discovery | PMINITL | Specifies whether an OS should be installed over an existing file system on a recently discovered, but unmanaged device.<br>The PMINITL attribute is referenced only if there is no `rombl.cfg` on the device. If there is a `rombl.cfg`, this indicates that the device is already under management and PMINITL will not be referenced at all.<br>• _LOCAL_<br>Prompts the user.<br>• _KEEP_<br>Does not prompt the user and keeps the current OS if the device has a valid operating system. If the device does not have a valid operating system and there is a resolved OS, it will be installed.<br>• _REINSTALL_ (default)<br>Does not prompt the user and reinstalls the operating system, regardless of what exists. |

| Field | Attribute in CM Configuration Server Database | Description |
|---|---|---|
| Ack Timout ROLE/OS (seconds) | ACKTMOUT | Specifies how long ACKTMOUT waits before assigning the default AUTOROLE.<br>• Set ACKTMOUT = 0 to disable the timeout.<br>• Set ACKTMOUT = *number of seconds* to wait the specified length of time before continuing. |
| Default value for ROLE | AUTOROLE | The ROLE that is assigned if a timeout occurs. |
| Disaster Recovery | PMDISRCV | Specifies the action to be taken when the master boot record is found to be damaged.<br>If PMDISRCV _CONFIRM_, the target device shuts down so that the administrator can recover data from the target device.<br>If PMDISRCV = _AUTO_, the appropriate OS is re-installed. |
| Keybd Language Support | KBDMAP | Sets the keyboard mappings:<br>• **en** (default) loads English keyboard mappings<br>• **fr** loads French keyboard mappings<br>• **de** loads German keyboard mappings |
| ROMA Parameters | ROMAPARM | This field has several uses. Typically, you should use this only if instructed by Technical Support.<br>Also used in conjunction with the TESTMODE flag. |
| Send AppEvent To | EVNTDEST | Indicates where to send the AppEvent objects. Options are:<br>• OPS – For future use.<br>• RIM – This option sends the AppEvent to the Inventory Manager.<br>• RMP – This option sends the AppEvent to the Portal. |

| Field | Attribute in CM Configuration Server Database | Description |
|---|---|---|
| System Language | LANG | Specifies the language to be supported.<br>• en_US = English<br>• zh_CN = Simplified Chinese<br>• ja_JP = Japanese<br>• ko_KR = Korean |

4 When you are done making changes, click **Modify**.

The Defaults for the Behavior Properties window opens again.

## Creating an Instance

The following is an example of how to create a subnet instance. Use these steps to create an instance in any class over which you have the appropriate authority.

Note that if you want to create an instance for a machine manufacturer or machine model, you should use the manufacturer or model information that is stored in the ROM object that was created when the device was discovered.

The reason for this is that the instance name must correspond with the data derived from SMBIOS. For example, Hewlett-Packard would be HEWLETT_PA. You cannot use spaces and are restricted to ten characters.

Also, remember that you can create policy instances directly from the MACHINE instance, as described in Viewing the ROM Object on page 118.

### To create a subnet instance

1 Use the navigation aid to select the appropriate Configuration Server.

2 In the workspace, select the appropriate class, such as Machine Subnets.

3 In the OS Administration task group, click **Create Instance**.

4 In the Instance box, type the name of the instance that represents the subnet. Remember that when specifying the subnet, you must use underscores ( _ ), not periods ( . ).

5 In the Friendly name box, type a friendly name.

6 Click **Create**.

The Subnet Properties window opens.

## Assigning Roles

Use the Assign Role task to assign the appropriate role to the target device. HP includes the following sample roles – SERVER and WORKSTATION.

### To assign roles

1 Use the navigation aid to go to the appropriate device.

2 In the workspace, click **ROM**.

3 In the OS Manager Administration task group, click **Assign Role**.

4 Select a role from the list of Available Roles.

5 Click **Submit**.

The Properties window opens.

## Removing Roles

Use the Remove Role task to remove the assigned role from the target device.

### To remove a role

1 Use the navigation aid to go to the appropriate ROM object.

2 In the OS Manager Administration task group, click **Remove Role**.

3 Click ✓ to confirm that you want to remove the role.

or

Click ✗ to indicate that you do not want to remove the role.

## Connecting Operating Systems

Use the Connect Operating Systems task to assign the appropriate OSs to your target devices based on policy such as machine type, manufacturer, model, role or subnet.

### To connect operating systems

1. Use the navigation aid to go to the appropriate POLICY instance, such as a SUBNET instance.
2. In the OS Manager Administration task group, click **Connect Operating Systems**.
3. From the Available list, select the OSs that you want to assign to the POLICY instance and then click  to add your selections to the Selected list.
4. Click **Next**.

   The Summary window opens.
5. Click **Commit**.

   The Properties window for the selected POLICY instance opens.

## Disconnecting Operating Systems

Use the Disconnect Operating Systems task to remove assignments between OSs and the target devices based on the selected criteria.

### To disconnect operating systems

1. Use the navigation aid to go to the appropriate POLICY instance.
2. In the OS Manager Administration task group, click **Disconnect Operating Systems**.
3. From the Available list, select the images that you want to disconnect.
4. Click  .
5. Click **Next**.

   The Summary window opens.
6. Click **Commit**.

   The Properties window for the selected POLICY instance opens.

## Selecting an Operating System

Use the Select OS task to assign the appropriate OS to the selected target device. This task may be useful if:

- a device has more than one resolved OS (for example, if the MACHINE attribute Last Resolved OS(es) (RSLVDOS) = WIN2K WINXP).
- the user was offered a list of OSs to choose from, and selected the wrong one. To resolve this situation, you (the administrator) must set the current OS to NONE. Then, you can use the Re-evaluate/install OS task to allow the user to select the appropriate OS. Of course, you can also change the behavior settings so that the user no longer receives a list of options, and the OS of your choice is installed.

Note that:

- The Chosen OS (SLCTDOS) must be in a pending state (_SLCTOS_PENDING_).
- This task does not initiate the installation of the OS; it simply allows you to select the OS that you want to install.

### To use the Select OS task

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices** and select the appropriate device.
3. Click the ROM object.
4. In the OS Manager Administration task group, click **Select OS**.
5. Select the operating system that you want to install from the list.
6. Click **Submit**. The Chosen OS (SLCTDOS) attribute contains the name of the OS that you selected. You may use this task in conjunction with the Force OS Install task to force the installation of the selected OS.

## Filtering Machines

Use the Filter Machines task to query for devices with an invalid OS state, unmanaged devices with no resolved OS, or devices that have more than one eligible OS.

### To use the Filter Machines task

1. Use the navigation aid to go to the appropriate zone.
2. Click **Devices**.
3. In the OS Manager Administration task group, click **Filter Machines**.
4. Select the type of query that you want to perform.

- Select **Invalid OS** state to find devices whose current OS is invalid. The OS State (OSSTATE) is set to _INVALID_.
- Select **Unmanaged OS** to find devices with an OS installed, but which the OS Manager does not manage. An unmanaged device is a device whose Current OS (CURROS) is set to _UNMANAGED_OS_.
- Select **Pending OS selection** to find devices that have no OS currently installed, but also have more than one eligible OS and are waiting for you (the administrator) to make a selection. A device is pending OS selection if the Chosen OS (SLCTDOS) is _SLCTOS_PENDING.
- Select **No resolved OS** to find devices that have no resolved OSs; in other words, no policy has been assigned to the device. A device has no resolved OS if Last Resolved OS(es) (RSLVDOS) is empty.
- Select **Pending Hardware Configuration Selection** to find devices that have no hardware configuration currently applied, but also have more than one eligible hardware configuration and are waiting for you (the administrator) to make a selection. A device is pending OS selection if the Chosen LDS (SLCTDLDS) is SLCTLDS_PENDING.

## Re-evaluating the Operating System

Use the Re-evaluate/install OS task to change the currently installed operating system (Chosen OS) to a different operating system. The list of potential operating systems is stored in the Last Resolved OSs field in the ROM object. See Viewing the ROM Object on page 118. Depending on your behavior settings, the user will be prompted to select an operating system or you (the administrator) will use the Select OS for Pending Machines task to make the selection.

Use of this task requires that the target device is already under management and has the ability to perform an HPCA OS connect. After selecting this task, you must perform an HPCA OS connect in order to initiate the policy change.

When the HPCA OS connect occurs, the data capture exit point is executed so that any user data or settings can be captured. The device then reboots and resolution continues as normal. If the behavior is set to prompt the user, he will select the appropriate OS from the list displayed. The new OS is installed and the data restore exit point will be executed so that any user data or settings can be restored. See Addressing Requirements for Capturing, Recovering, and Migrating Data on page 201.

If you want to completely re-evaluate the existing installation, and the Select Role attribute in the Behavior Properties is set to LOCAL, you may consider setting the Role assigned to the device to NONE so that the user is prompted for a role on the next reboot. See Assigning Roles on page 130 for information about how to set the role for a device.

### To use the re-evaluate/install OS task

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices** and select the appropriate device.
3. Click the ROM object.
4. In the OS Manager Administration task group, click **Re-evaluate/install OS**.
5. Click ✓ to continue.

   or

   Click ✗ to cancel this procedure.
6. If you click ✓, Chosen OS (SLCTDOS) is set to NONE and Current OS (CURROS) is set to NONE until the new OS is installed.

## Forcing an OS Installation

Use the Force OS Install task to force the installation of the resolved OS over any previously existing operating system.

Use this task only in situations where you have no other choice, such as if something unrecoverable happened to a drive.

Data capture/restore exit points will *not* be executed. All data and settings will be lost. See Addressing Requirements for Capturing, Recovering, and Migrating Data on page 201.

Typically, you should modify policy to change a device's OS.

Note that if a cached partition exists, the image will be obtained from the partition. See Defining Drive Layouts on page 138.

### To force an OS installation

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices** and select the appropriate device.
3. Click the ROM object.
4. In the OS Manager Administration task group, click **Force OS Install**.
5. Click ✔ to continue.

   or

   Click ✘ to cancel this procedure.
6. If you click ✔, the OS State (OSSTATE) is set to INVALID, which is a last resort option. The OS will be re-installed on the next boot. If the next boot happens before the next HPCA OS connect data/restore capture, backups and so on will not be executed.

## Selecting the OS for Pending Machines

Use the Select OS for Pending Machines task to return a list of devices that have more than one resolved OS and then select the OS to be installed.

### To return a list of devices in pending state

1. Use the navigation aid to go to the appropriate Zone.
2. Click **Devices**.
3. In the OS Manager Administration task group, click **Select OS for Pending Machines**.

   A list of devices opens. A device is in pending state if Chosen OS (SLCTDOS) is set to _SLCTOS_PENDING_.
4. From the Available list, select the devices whose OSs you want to set, and then click ⏩ to add your selections to the Selected list.
5. Click **Next**.

   A list of the resolved OSs opens. Note that if you select multiple devices, this list is limited to the OSs that are eligible for all of the selected devices.

   For example, if you have two devices:

   — Device A's eligible OSs are Win2K and WinXP, and

— Device B's eligible OS is Win2K.

The list in this window will only contain Win2k.

6 From the Resolved Operating Systems list, select the OS that you want to specify for the selected devices.

7 If you want to “wake” the target devices, select the Issue Wake on LAN check box.

8 Click **Next**.

The Summary window opens.

9 Click **Submit**. The Chosen OS (SLCTDOS) is set according to your selection.

## Selecting HW Configuration for Pending Machines

Use the Select HW Configuration for Pending Machines task to return a list of devices that have more than one resolved hardware configuration and then select the hardware configuration to be applied.

### To return a list of devices in pending state

1 Use the navigation aid to go to the appropriate Zone.

2 Click **Devices**.

3 In the OS Manager Administration task group, click **Select Hardware Configuration for Pending Machines**.

A list of devices opens. A device is in pending state if Chosen LDS (SLCTDLDS) is set to _SLCTLDS_PENDING_.

4 From the Available list, select the devices whose hardware configurations you want to set and click  to add your selections to the Selected list.

5 Click **Next**.

A list of the resolved hardware configurations opens. Note that if you select multiple devices, this list is limited to the hardware configurations that are eligible for all of the selected devices.

6 From the Resolved Hardware Configurations list, select the hardware configuration that you want to specify for the selected devices.

7 If you want to “wake” the target devices, select the Issue Wake on LAN check box.

8 Click **Next**.

The Summary window opens.

9 Click **Submit**. The Chosen LDS (SLCTLDS) is set according to your selection.

## Bringing Machines under Management

If there is an existing OS on a device when it is discovered, the Current OS will be set to indicate that the device is unmanaged (_UNMANAGED_OS_). You must assign policy and then use the Bring Machines Under Management task. Note that the Current OS will be set to _NONE_ until another HPCA OS connect occurs and the resolved OS is installed.

A typical scenario would be to filter the machine to find all of the unmanaged machines, assign policy, and then use the Bring Machines Under Management task to remove the unmanaged OS and install the new, resolved, OS. If you have not set policy, no change will occur. Note that the data capture/restore exit points will be executed so that any user data or settings can be captured and restored. See Addressing Requirements for Capturing, Recovering, and Migrating Data on page 201

This task should not be used as the way to change OSs on a daily basis. Typically, you should modify policy to change a device's OS.

### To bring machines under management

1 Use the navigation aid to go to the Devices.

2 In the OS Manager Administration task group, click **Bring machines under management**.

3 From the Browse devices area, select the devices to be brought under management. Click  to add the device to the Device area.

4 In the Device area, select the check box.

5 Click **Next**.

The Summary window opens.

6 Click **Submit**.

The workspace displays a list of the devices that are under management. The next time the target devices boot, they will follow the typical boot process and the appropriate OS will be installed. Until the devices boot, the value of Current OS remains set to _NONE_.

## Removing Instances

Use the Remove task to remove the selected object.

### To remove an object

1 Use the navigation aid to go to the appropriate instance, such as a Manufacturer instance.

7 In the CM OS Manager Administration task group, click **Remove**.

8 Click ✓ to confirm that you want to remove the instance.

or

Click ✗ to indicate that you do not want to remove the instance.

## Modifying Instances

Use the Modify Instance task to change the selected object.

### To modify an object

1 Use the navigation aid to go to the appropriate instance.

9 In the OS Manager Administration task group, click **Modify Instance**.

10 Make any necessary changes.

11 Click **Modify Instance**.

The Properties window for the selected instance opens.

## Defining Drive Layouts

The OS Manager Server supports the ability to:

- Create one or more data partitions in addition to the boot partition.

  or

- Create a copy of your new OS image and its supporting files on a hidden partition to be used for recovery.

Use the Drive Layouts class to specify the type of partition. Partitioning is supported for the boot drive only.

We strongly recommend that you connect a Drive Layout instance to only one Operating System or Policy instance to prevent conflicting definitions. Doing otherwise may cause unpredictable results.

It is possible that multiple Drive Layout instances may be resolved for an installation. Only the first resolved instance will be used. Any other instances will be ignored.

### To specify a drive layout

1. Use the navigation aid to go to the appropriate Configuration Server.
2. Click **Drive Layouts**.
3. In the OS Manager Administration task group, click **Create Instance**.
4. In the Instance name box, type the name of the instance.
5. In the Friendly name box, type a friendly name.
6. In the Type drop-down list, select the type of partition you want to create.

**Table 10 Types of Partitions**

| Type | Description |
|---|---|
| Add | Creates one or more extended partitions at the end of the hard disk. |
| Replace (default) | Replaces the current mappings on the target device with the partition that is defined with the OS image being installed. If there are no DRIVEMAP instances connected to the OS being installed, this is the default method.<br>Important: If you use Replace, *all existing data will be lost.* |

| Type | Description |
|---|---|
| Cache | Creates a hidden back-up partition at the end of the target drive. The size of the partition will be dynamically determined by the size of the OS installation image. All files necessary to reinstall the OS will be saved (in compressed form) in this partition. Note that during the reinstallation, the name and size of the image are confirmed.<br>Important: If you use the Cache type, *all existing data will be lost.*<br>See Restoring Operating Systems on page 198 for information about restoring this image. |
| Merge | Use for migration purposes. Replaces or updates an OS on a machine where existing data needs to be preserved. Merge will overlay only the existing boot partition and will not touch data on any other partitions.<br>• If the boot partition to be installed is larger than the space already defined for the partition, the installation will fail. The starting point of the existing partition will be used and the boot partition will be placed at the beginning of the drive segment defined in the partition.<br>• If the target drive does not contain existing partitions, the boot partition definition will be used to partition the target drive. |

7 Click **Create**.

The Drive Layout Properties window opens.

## Adding Partitions

You can create a new layout that contains a boot partition and one or more logical data partitions at the end of the hard disk in a single, extended partition. These partitions are in addition to the OS boot partition. Partitions are added from the “back” of the disk to the “front.”

All existing data will be lost.

There is a limit of four *physical* partitions on a hard drive and only one partition may be an extended partition (which may contain any number of logical drives).

Also, if you start with a single physical drive such as:

| PARTITION | LOGICAL DRIVE |
|---|---|
| Primary | C |
| Extended | D |
| | E |
| | F |

and then add a second hard drive, the drive letter mappings are reassigned so that the primary partitions are in alphabetical sequence. See the example below.

### Drive 1

| PARTITION | LOGICAL DRIVE |
|---|---|
| Primary | C |
| Extended | E |
| | F |
| | G |

### Drive 2

| | |
|---|---|
| Primary | D |
| Extended | H |
| | I |
| | J |

The partition will be added after the boot partition. Make sure you allow enough space for the OS. Note that if the total requested space would exceed the capacity of the drive where the OS is being installed, the installation will fail.

### To add partitions

1 Use the navigation aid to go to the appropriate Zone.

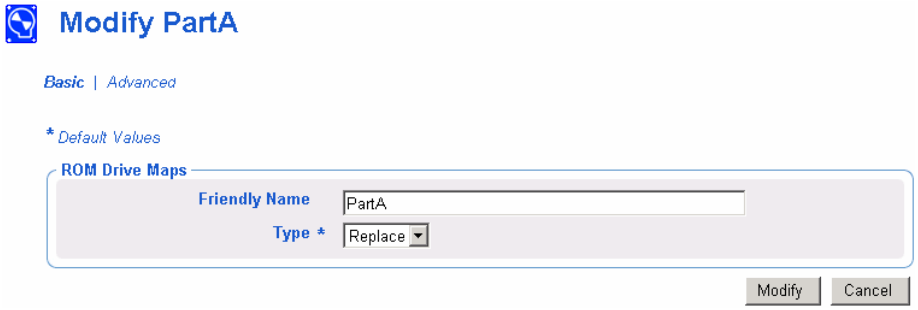
2 Click **Drive Layouts**.

3 Select the appropriate drive layout instance.

4 Make sure the type is set to Add.

Remember, *all existing data will be lost*.

5 If you need to modify the partition type, use the Modify Instance task; otherwise, skip to step 8.




6 From the Type drop-down list, select **Add**. See Table 10 on page 139.

7 When you are done making changes, click **Modify**.

8 In the OS Manager Administration task group, click **Add Partition**.

9 Specify the options in the Properties area. Note that an instance is created in the OS.PARTTION Class for each partition that you add.

**Table 11 PARTTION Class Attributes**

| Field | Attribute in the Database | Description |
|---|---|---|
| Partition Identifier | PARINFO | Identifies the name of the partition. |
| Units | UNITS | Indicates whether the partition size is being specified as a percentage or in megabytes. |
| Partition Size in pct or MB | SIZE | Specifies the partition size specified as a percentage of the hard drive or in MB.<br>These values equal the total hard drive space. |
| Type | PARTYPE | Indicates the type of partition: NTFS, FAT32, EXT2, EXT3, or QNTFS. EXT2 and EXT3 are not supported under the WinPE Service OS.<br>Note that QNTFS performs a quick format without zeroing out the partition. |

| Field | Attribute in the Database | Description |
|---|---|---|
| Reformat drive | FORMAT | Specifies whether to format the drive. |

10 Click **Modify** when you are done defining the partition information.

11 In the Partition Information area, you can use the Modify or Delete hyperlinks to make changes to the defined partition. If you make changes to the partition, you will be returned to this window when you are done.

## Connecting Drive Layouts

Use the Connect Drive Layout task to assign the appropriate drive layouts to your target devices based on policy such as machine manufacturer, model, role, or subnet.

### To connect drive layouts

1 Use the navigation aid to go to the appropriate POLICY instance, such as a SUBNET instance.

2 In the OS Manager Administration task group, click **Connect Drive Layout**.

3 From the Available Drive Layouts list, select the appropriate drive layouts, and then click Submit.

Remember that you can add partitions *or* merge, replace, or cache partitions. You cannot do both.

The Properties window opens.

## Disconnecting Drive Layouts

Use the Disconnect Drive Layouts task to remove assignments between drive layouts and the target devices based on the selected criteria.

### To disconnect drive layouts

1 Use the navigation aid to go to the appropriate POLICY instance.

2 In the OS Manager Administration task group, click **Disconnect Drive Layout**.

3 When prompted, click ✓ to accept to continue.

or

Click ✗ to cancel this procedure.

The Properties window for the selected POLICY instance opens.

## Connecting Behaviors

Use the Connect Behavior task to assign the appropriate behaviors to your target devices based on policy. Connect only one behavior instance per policy instance.

A behavior instance defines system behaviors that can be assigned to targets based on policy.

### To connect behaviors

1 Use the navigation aid to go to the appropriate POLICY instance, such as a SUBNET instance.

2 In the OS Manager Administration task group, click **Connect Behavior**.

3 From the Available OS Behaviors list, select the appropriate behavior.

4 Click **Submit**.

The Properties window opens.

## Disconnecting Behaviors

Use the Disconnect Behaviors task to remove the behavior assignment.

### To disconnect behaviors

1 Use the navigation aid to go to the appropriate POLICY instance.

2 In the OS Manager Administration task group, click **Disconnect Behavior**.

3 When asked if you are sure that you want to disconnect the behavior, click ✓ to continue.

or

Click ✗ to cancel this procedure.

The Properties window for the selected POLICY instance opens.

## Connecting a Sysprep File

Use the Connect Sysprep File task to assign a `Sysprep.inf` that is separate from the gold image to allow the same image to be set up differently on target devices. The override `Sysprep.inf` will be merged with the embedded `Sysprep.inf`. Therefore, the values in the override `Sysprep.inf` will take priority; however any values not specified in the override file will remain as is in the original file.

Each Sysprep can only be connected to one OS service. At this time OS services cannot share Sysprep instances.

The `Sysprep.inf` file should not be greater than 800 KB in size.

### To create an override Sysprep.inf

1. Modify `Sysprep.inf` to contain the appropriate information.
2. Use the Publisher to publish the new `Sysprep.inf` file to the OS domain, Sysprep Files (SYSPREP) class.

   In the Publisher, from the Type of Data to Publish drop-down list, you must select **OS Image**. Then, you can select the appropriate `Sysprep.inf` file that you want to use. See Using the Admin Publisher on page 104.
3. Use the Connect Sysprep File in the OS Manager Administration task group to connect the Sysprep file to the appropriate OS. You can only attach one Sysprep file to an OS. If the OS does not have this connection, the embedded `Sysprep.inf` file will be used.

   Currently, the COMPNAME and DOMAIN from the ROM object will be used in `Sysprep.inf`, whether `Sysprep.inf` was embedded in the image or published separately.

Consider running a manual test of `Sysprep.inf` to verify the accuracy of the file prior to using the Image Preparation Wizard. Remember that if you run Sysprep and have extendoempartition = 1, the partition will be extended after Sysprep runs.

If you want to deliver the same OS with varying setup behaviors, you can create multiple OS services. Each OS service can contain the same OS image, yet each may have a different `Sysprep.inf` attached to it.

### To connect a Sysprep file to an OS instance

1. Use the navigation aid to go to the appropriate OS instance.
2. In the OS Manager Administration task group, click **Connect Sysprep File**.
3. From the Available OS Sysprep list, select the appropriate Sysprep file.
4. Click **Submit**.

   The Properties window opens.

## Disconnecting a Sysprep File

Use the Disconnect Sysprep File task to remove an assignment between OSs and a Sysprep file. If you disconnect the override Sysprep file, the next time that the OS is installed, the Sysprep file that is embedded in the OS image will be used.

### To disconnect a Sysprep file

1. Use the navigation aid to go to the appropriate operating system instance.
2. In the OS Manager Administration task group, click **Disconnect Sysprep File**.
3. When asked if you are sure that you want to disconnect the Sysprep file, click ✓ to continue.

   or

   Click ✗ to cancel this procedure.

   The Properties window for the selected OS opens.

## Adding Devices

This task is available for bare metal machines in a PXE environment.

Use the Add Device task to create a device object in the Portal.

The Add Device task is most useful when provisioning servers. For example, if you want to install Windows 2003 Server on a machine, you may not want to have the machine discovered so that you have some control over identifying parameters. Therefore, you can add the device in the Portal and assign a unique computer name. When the device boots for the first time, it will be provisioned with the information that you specified.

This task is useful for a small number of devices. If you have many devices and want to specify their identifying parameters (via an algorithm or mapping), you would use the exit point called `getmachinename.tcl`, located on the OS Manager Server, to configure devices dynamically. This exit point can interact with existing servers, such as Web servers or SQL servers. Refer to the engineering note, *Assigning unique Machine Names with OS Management* for more information about this exit point.

### To add a device

1. Use the navigation aid to select the appropriate Zone.
   a. In the workspace, click **Groups**.
   b. Select a group and from the OS Manager Administration task group, click **Add Device**.
2. (Required) In the MAC Address field, type the MAC address for the device.
3. In the following fields, you can specify the following:
   a. In the Computer Name field, type the host or fully qualified host name.
   b. In the SMBIOS System S/N field, type the SMBIOS System Serial Number for the device.
   c. In the Common Name field, type a unique name.
4. (Optional) In the Sysprep Data field, type the Sysprep data that you want to inject in the following format:
   `section/key=value,section/key=value,section/key=value,...`

You cannot use blanks except as part of a value. You cannot use a forward slash (/), equal sign (=), or comma (,) in the section, key or value.

5 From the Default Service OS drop-down list box, select the default service OS to use the first time this machine is booted as part of the OS Manager. Note that this works only if the device is booting via the network.

6 (For advanced users) In the Policies text box, you can specify policies using the format of DOMAIN.CLASS.INSTANCE, such as OS.ZSERVICE.XPSP2I66. However it is recommended that you use the HPCA OS Manager administration tasks such as Connect Operating Systems task (see Connecting Operating Systems on page 130) and Connect Hardware Configurations (refer to the *HP Client Automation Enterprise OS Manager Hardware Configuration Management Guide* for more information).

7 Click **Submit**.

## Modifying Devices

Use the Modify Device task to modify Sysprep data that you manually added to a device using the Add Device task.

### To modify a device

1 Use the navigation aid to select the appropriate Zone.

2 In the workspace, click **Devices**.

3 Select the device that you want to modify and then select its ROM object.

If you want to see the Sysprep Data that was added to the device, click **Advanced** in the workspace. Scroll to the Advanced section and you will see a Sysprep Data field that shows the current settings.

3 From the OS Manager Administration task group, click **Modify Device**.

4 Make the necessary changes and click **Submit**.

## Downloading Resources

Use the Download Resources task to save the resource files for OS services or Sysprep files to a directory on the OS Manager Server. Then, you can burn a CD-ROM or DVD-ROM with this data. Do not span your resources over

multiple CD-ROMs or DVD-ROMs. Typically, this is meant for use with DVDs to store multiple images.

You must use Client Operations Profiles (COP) to specify where OS Manager Server should retrieve the image. See Using HPCA Client Operations Profiles with OS Manager on page 203.

Your CD-ROM must be in Joliet format.

### To download resources to a target directory

1. Use the navigation aid to go to the appropriate class — Operating Systems or Sysprep Files.
2. In the OS Manager Administration task group, click **Download Resources**.
3. From the Available list, select the operating system services that you want to download.
4. Click **Next**.
5. If you changed the port number for the Proxy Server, type the new port number in the **Please specify the port number of your Proxy Server on localhost** text box.
6. Type the name of the directory on your OS Manager Server to which you want to download your resources. If the directory does not exist, you must create it.

   If your browser is not running on the OS Manager Server, specify a UNC path to the target directory.
7. Click **Next**.

   The Summary window opens.
8. Click **Submit**.

   The workspace returns to the class you were viewing.

   Use Windows Explorer to see that the files have been downloaded to the target directory that you specified.

Be sure that your CD writer software does not change the case of the directories or files that you are copying. If it does, then be sure to change it back to match the file structure that was created using this task.

9 Copy the entire `RESOURCE` directory to the CD-ROM or DVD-ROM.

Now that you have the `RESOURCE` directory stored appropriately, use Client Operations Profiles to specify where the OS Manager Server should retrieve the image. See Using HPCA Client Operations Profiles with OS Manager on page 203.

### Retrieving the OS image from a CD-ROM

If you used the Download Resources task, the following is an example of how to use a CD-ROM or a DVD-ROM to install an OS to a target device.

Refer to *Configuring Client Operations Profiles* in the *HP Client Automation Enterprise Application Manager and Application Self-service Manager Installation and Configuration Guide* and then see Using HPCA Client Operations Profiles with OS Manager on page 203.

1 Create a CLIENT.LOCATION instance to specify your network.

2 Create a CLIENT.SAP instance for the CD-ROM. Be sure to:

- Set `TYPE` to `DATA`.
- Set `URI` to `cdr://`
- Set `ROLE` to `Z`.

3 Use the Admin CSDB Editor to connect the SAP instance to the LOCATION instance. Be sure to use the _ALWAYS_ connection with the Connect To Attribute description.

4 Insert the CD-ROM or the DVD-ROM into the target device.

5 Boot the machine. When the machine boots, it does a Client Operations Profiles resolution and installs the OS image from the CD-ROM or the DVD-ROM.

## Notifying Target Devices

Use the Notify task to perform an action on a target device that you select. For more information, refer to the *HP Client Automation Enterprise Portal Installation and Configuration Guide*.

### To notify a target device

1. Use the navigation aid to go to the Device class under the appropriate Zone.
2. In the OS Manager Administration task group, click **Notify**.
3. Select the Client Automation OS Manager task type.
   - No Client Automation OS Manager Task Selected

     Select this option to perform a standard notify operation.
   - Assign Role

     A list box appears and you must select a role. See Assigning Roles on page 130.
   - Bring Machines Under Management

     See Bringing Machines under Management on page 137.
   - Force OS Install

     See Forcing an OS Installation on page 134.
   - Re-evaluate/install OS

     See Re-evaluating the Operating System on page 133.
   - Remove Role

     The selected role is removed. See Removing Roles on page 130.
4. Click **Next**.
5. Select the devices that you want to Notify.
6. Click **Next**.
7. From the Notify Type drop-down list, select **OS Connect** to indicate that this connection is being performed for the OS Manager.

   The parameters in the Command box change, based on your selection.
8. In the Command box, modify the command line as necessary. For example, the Command box is pre-filled with the following command line:

```
radskman ip=|mgr_ip|, port=|mgr_port|,dname=OS,cat=prompt
,ulogon=n,context=m,ask=n,cop=y,catexp=ZOBJDOMN:OS,ver=y
```

If you are deploying Windows CE, use the following command line:

```
radskman SIP=|ip address of mms|,SPORT=3470,RPSADDR=|ip
address of Proxy Server|,RPSPORT=3466,DNAME=OS,ASK=N
```

You must replace information between the pipes (|) with the necessary information to perform the notification. For example, you might modify the command line above to read:

```
Radskman ip=10.10.10.1,port=3464,dname=OS,cat=prompt
,ulogon=n,context=m,ask=n,cop=y,catexp=ZOBJDOMN:OS,ver=y
```

If you repeat a Notify operation often, you may want to modify the appropriate Notify task so that it has default options that pertain to your organization. Refer to the *HP Client Automation Enterprise Portal Installation and Configuration Guide*.

9 In the Port number box, type the port number that the Notify daemon will be listening on. By default, the port number is 3465.

10 If necessary, in the User box, type the user name for the target device.

11 If necessary, in the User Password box, type the password for the target device.

12 Click **Next**.

The Schedule dialog box opens.

13 In the Schedule dialog box, specify when you want this job to run.

14 Click **Next**.

The Summary dialog box opens.

15 Click **Submit**.

The Job Status dialog box opens with list of the jobs. This dialog box automatically refreshes every 60 seconds.

— Click  to refresh the dialog box to display the latest status.

— Click  to view detailed information, such as the status of the installation.

16 When you are done viewing the job status, click  to close the Job Status dialog box, and return to the Portal.

# 7 Implementing the HPCA OS Manager Server in your Environment

At the end of this chapter, you will:

- Be able to initiate an installation via the network.
- Be able to initiate an installation locally.

After you have successfully installed your OS Manager infrastructure, consider how you want to implement the OS Manager in your environment. We recommend that you work with Professional Services to determine what is best for your unique situation. This chapter is intended to help you understand your options. They are:

- Installations initiated by the network
  This refers to the PXE-based environment. The OS Manager can assume management of the operating system on target devices that are booted from the network.
- Installations initiated locally
  This refers to the Local Service Boot (LSB). The OS Manager can assume management of the OS on target devices that are not booted from the network.

We strongly recommend that you choose one method for a particular target device. If you have a bare metal machine or a machine that needs disaster recovery, you *must* use PXE.

# About the PXE-Based Environment

The PXE-based environment allows the OS Manager to assume management of the OS on target devices that are booted from the network. Typically, we recommend that you use the PXE-based environment because it provides a fully automated solution for all scenarios.

## Best Practices for PXE-Based Implementations

If you already have Client Automation implemented in your environment and want to use a PXE-based environment for the OS Manager, we recommend the following:

1. Install the OS Manager Server infrastructure before making any changes to your target devices. See Chapter 3, Installing and Configuring the Server Architecture.
2. Agents that exist on your target devices will continue running any previously scheduled agent connects. The OS Manager will not make any changes to the device until you assign policy.

3 After your infrastructure is installed and stable, set the network boot as the primary boot device on your target devices.

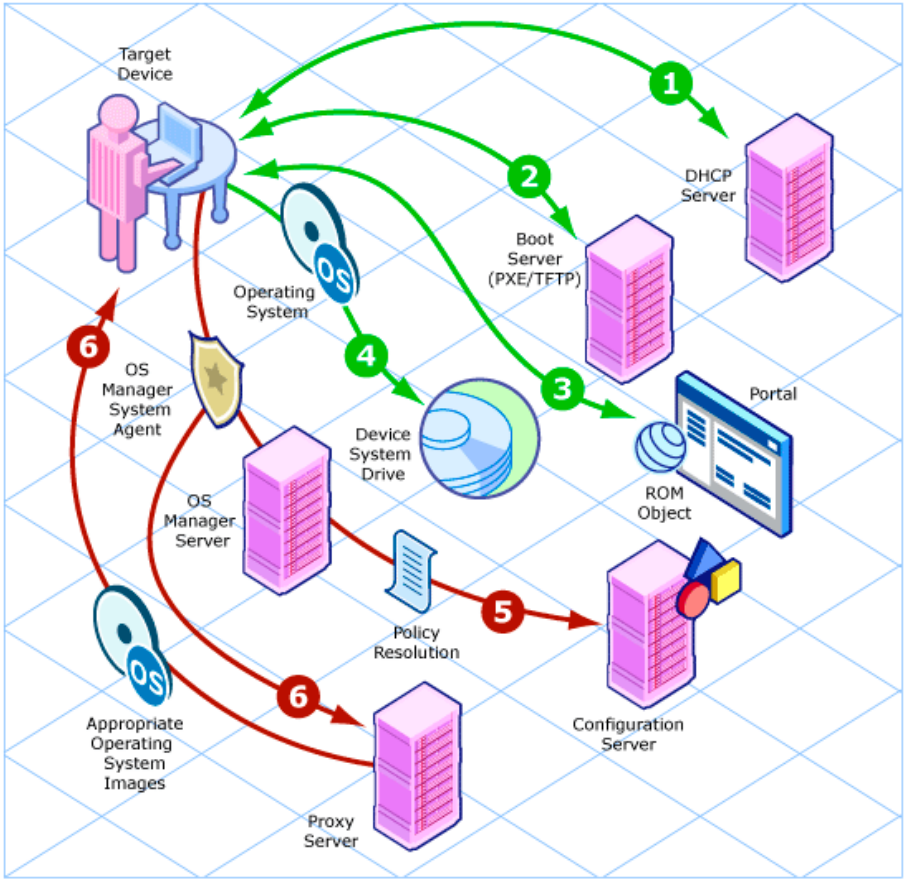
4 The next time the device boots, a ROM object will be created in the Portal. The OS Manager Server and the target device use the ROM object to communicate.

At this point, the OS Manager has discovered the target device, but its OS is likely considered unmanaged unless you assigned policy prior to booting the target device. The target device will continue to boot into its existing OS until you assign policy and perform an agent connect.

## Networking Boot with PXE

Figure 6 on page 156 and the text following it give an overview of the boot process.

**Figure 6 Networking boot with PXE process flow**




1 The target device obtains an IP address from a DHCP server.

2 The (managed) target device boots from the network (via the PXE server), and the TFTP server delivers the OS Manager Boot Loader to the target device.

3 The OS Manager Boot Loader looks at the Portal to see if a ROM object exists.

— If there is no ROM object, an object is created in the Portal.

— If there is a ROM object, it must be decided whether there is a valid OS or not.

4 If there is a valid OS on the machine, it boots to the existing OS located on the device's system drive.

   or

   If there is not a valid OS on the device, the boot process continues by loading the OS Manager System Agent from the TFTP server to the target device.

5 The OS Manager System Agent and the Configuration Server communicate through the OS Manager Server to handle policy resolution of the correct OSs for the target device.

6 The OS Manager System Agent downloads the appropriate images from the Proxy Server and installs them on the target device.

Check the HP support web site for product updates and release notes.

# About Local Service Boot

The Local Service Boot allows the OS Manager to assume management of existing OSs on devices that are not booted from the network.

The advantages of Local Service Boot are that existing machines do not need to be PXE-enabled and the boot order does not need to be configured locally in the BIOS for each target device. This option is also less network-intensive because the OS Manager System Agent is only downloaded when the LSB service is downloaded to the target device. Since this intermediate OS is local, it does not need to be downloaded again unless there is an update. In a PXE environment, the OS Manager System Agent is downloaded every time it is needed.

If you have a bare metal machine or a machine that needs disaster recovery, you *must* use PXE.

## Prerequisites

- You must have an operating system and the Application Manager installed on the target device so that you can deploy the LSB service.

- You must be using HPCA Client Operations Profiles as configured for the OS Manager Server and it must be enabled. See Using HPCA Client Operations Profiles with OS Manager on page 203.

The Image Preparation Wizard sets up Client Operations Profiles, and when the image is deployed, Client Operations Profiles is enabled. However, if you want to use the Local Service Boot on a machine where the OS has not been deployed by the OS Manager Server, you must enable Client Operations Profiles. To do this, use COP=Y on the radskman command line. Refer to *Configuring Client Operations Profiles* in the *HP Client Automation Enterprise Application Self-service Manager Installation and Configuration Guide*.

## Best Practices for Using Local Service Boot

If you already have HP Client Automation implemented in your environment and want to use the Local Service Boot for the OS Manager, we recommend that you:

1. Install the OS Manager Server infrastructure. See Chapter 3, Installing and Configuring the Server Architecture.
2. Use Client Operations Profiles to specify the IP address and port of the OS Manager Server in the form of a Service Access Profile (SAP) instance.

   When you set up the SAP, be sure to:

   — Set `TYPE` to `ROM` to identify this SAP as an OS Manager Server server.

   — Set `ROLE` to `Z`.

   — Set `URI` to specify the fully qualified IP address (or hostname) and port of the OS Manager Server that serves the agents on the subnet. For example:

   `http://OSManagerServer.domain.com:3469`.

   The value of the URL must be in lowercase text; otherwise the Local Service Boot will fail.

   You must create a LOCATION instance using the subnet with underscores as the name (10_10_10_0) and connect it to the SAP instance.

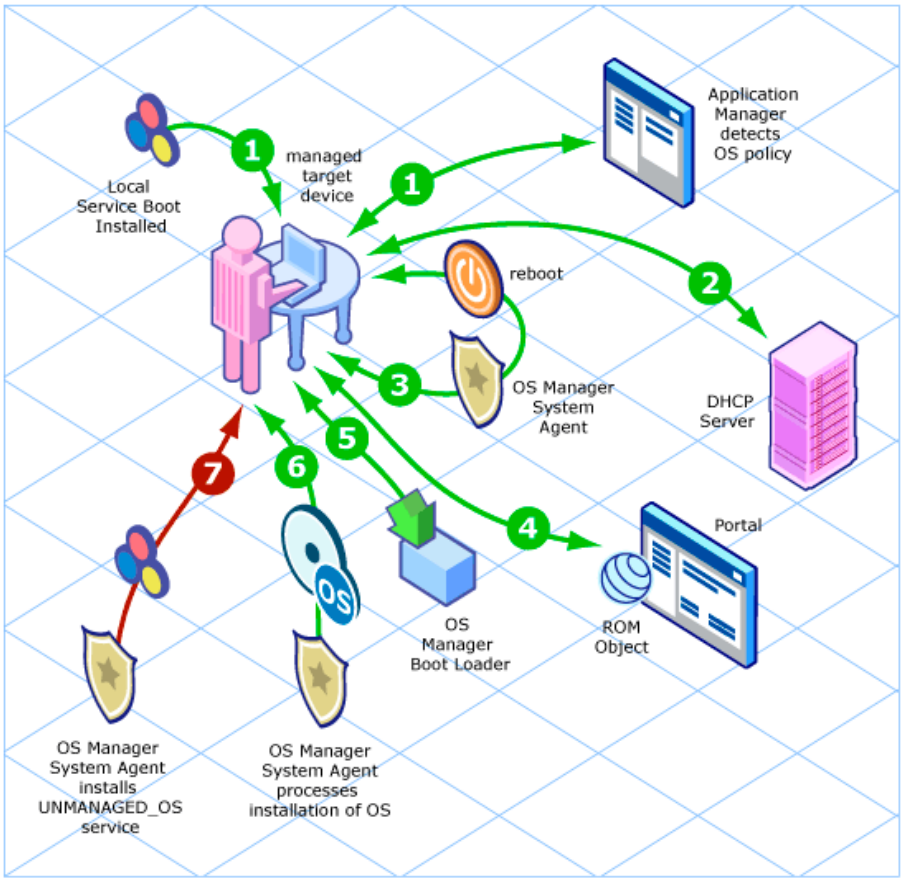
3 Set up policy to use the Application Manager to install the Local Service Boot service (LSB) on your target devices. Local Service Boot (LSB) must be distributed based on subnet, model or manufacturer.

After the LSB service is installed on the target devices (which creates the `Rombl.cfg` file on the root of the drive), they will reboot and be discovered. At this point, the OS Manager has discovered the target device, but its OS is still unmanaged. The target device will continue to boot into its existing OS until you assign policy and bring the machine under management.

## Booting with Local Service Boot

Figure 7 on page 160, and the text following it give an overview of the boot process.

**Figure 7 Booting with Local Service Boot**




1 After the Local Service Boot service is installed on a target device, the Application Manager is responsible for detecting OS policy changes on the managed target device.

2 The target device obtains an IP address from a DHCP server.

3 When the device restarts, the device boots into the intermediate Linux service OS and runs the OS Manager System Agent.

4 During this first boot after installation of the Local Service Boot service, a ROM object for the target device is created in the Portal (if one does not already exist). A ROM object will exist only if the device was previously under OS management.

5 During every subsequent reboot, the OS Manager Boot Loader will be loaded from the local file system.

6 If the HPCA OS connect detected a change in OS policy before the reboot, the OS Manager Boot Loader will load the intermediate Linux service OS, from the local file system, containing the OS Manager System Agent. The OS Manager System Agent processes the installation of the new OS, according to policy.

7 If no OS policy exists for this device, the OS Manager System Agent will install the _UNMANAGED_OS_ service (located in PRIMARY.OS.ZSERVICE). This special OS instance indicates that the device is under OS management, but that no OS has been selected for the device by policy.

Check the HP support web site for product updates and release notes.

# Managing Your Devices

Whether your devices are in a PXE-based environment or Local Service boot environment, after your existing devices are discovered and set to be unmanaged, nothing will happen until you take action.

If you want to change the OS, you must:

1 Specify policy.

2 Select the appropriate devices and use the Bring Machines under OS Management task.

3 This removes the unmanaged service (which was connected to your devices) and the device is considered managed.

4 Run an HPCA OS connect so the target devices can detect the policy changes.

5 If necessary, reboot the target devices.

This completes the description of how to implement the OS Manager in your environment.

We recommend that you work with Professional Services to determine what is best for your environment.

# 8 OS Manager Support for HP Blades

At the end of this chapter, you will:

- Be able to enable policy configurations for blades, enclosures, and racks.
- Be able to view blade information stored in the Chassis container in the Portal.
- Be able to assign policy based on enclosures, racks, slots, and enclosure configurations.

The OS Manager System Agent captures and reports all specific blade SMBIOS information to the Portal. Using the Portal, you can assign drive layouts, hardware configurations, and operating systems to your devices based on enclosures, racks, slots or enclosure configurations. To do this, you can use the OS Administration tasks Connect Operating System, Connect Hardware Configuration and Connect Operating System which are available for Blade.

For more information of Blade Management in Portal refer to the *HP Client Automation Enterprise Portal Installation and Configuration Guide*.

## Enabling Policy Configurations for Blades, Enclosures, and Racks

To enable resolution of policy for the objects related to blades, you must update the `rmp.cfg`.

### To enable policy configurations for blades, enclosures and racks

1. Open *`SystemDrive`*`:\IntegrationServer\etc\rmp.cfg`.
2. Add the following entry:

```
rmp::init{
   LINKS{ enclosureslotnumberdn enclosuremodeldn
enclosureconfigdn rackdn osdevicearchitecturedn }
 }
```

   The specific set of links to include in the entry will vary for each enterprise, depending on which entities and containers have been used for policy. Table 12 below describes the policy link that is enabled in the entry above. For example, if you have not assigned policy to the rack instances in your Zone, you may omit `rackdn` from the entry shown above.

**Table 12 Policy Resolution Links to Define in RMP.CFG**

| LINKS Parameter | Description |
|---|---|
| enclosureslotnumberdn | Links the blade device to the enclosure slot. |
| enclosuremodeldn | Links the blade device to the enclosure model. |
| enclosureconfigdn | Links the enclosure to its enclosure configuration. |

| LINKS Parameter | Description |
|---|---|
| osdevicearchitecturedn | Links the device to its device architecture (which is added by default). |
| rackdn | Links the enclosure to its rack (when policies are assigned to racks). |

## About HP Blade Discovery

Every time the target device boots, SMBIOS information (such as enclosure name and slots) from HP blades is sent to Portal through the OS Manager Server. The Portal will automatically create all related Blade information in the Chassis container.

### To view the blade information stored in the Chassis container

1. Log into the Portal.
2. Navigate to the appropriate Zone.
3. Click **Chassis** and then **Blade Enclosures** to see the discovered enclosures.
4. Click an enclosure name to display the slots discovered by the OS Manager.
5. Click a slot to display the discovered hardware device plugged into this slot.

## About HP Blade OS Policy Assignment

Using the Portal, you can assign operating systems, drive layouts and hardware configurations based on enclosures, racks, slots or enclosure configurations.

### To assign operating systems, drive layouts or hardware configurations

1. In the Portal, browse to the desired enclosure, racks, slots or enclosure configurations.
2. From the OS Manager Administration task group, select the appropriate task such as **Connect Operating Systems**.
3. From the Available list, select the desired OS.

4 Click **Next**.

The operating system is assigned to the selected enclosure name.

5 If you want to see the operating system assigned to enclosure, go to the enclosure and click **View Properties**  .

# 9 Multicast and the OS Manager

At the end of this chapter, you will:

- Understand the requirements for using multicast with the OS Manager.
- Be able to configure multicast for the OS Manager.
- Understand how to improve performance and reliability for multicast with the OS Manager.
- Understand how multicast transfers images.
- Understand the multicast parameters and their influence.
- Be able to identify, analyze and resolve multicast data transfer problems.
- Use a set of tools to manually test combinations of multicast parameters.

The OS Manager supports reliable delivery multicast so that you can rollout large numbers of OS images concurrently with improved performance.

In general, the same concepts apply when using the Multicast Server for the Application Manager or for the OS Manager. For a general understanding of the Multicast Server, refer to the *HP Client Automation Multicast Server Installation and Configuration Guide* on the HP support web site.

This topic covers how to use multicast with the OS Manager. Refer to the *HP Client Automation Multicast Server Installation and Configuration Guide* for installation instructions.

Spanned images are not supported with Multicast.

## Prerequisites

- An understanding of the Multicast Server.

## Requirements

- Multicast server version 3.1 or higher installed on a Windows machine.
- A reliable delivery Multicast-aware version of the OS Manager System Agent (supported in version 2.0 and higher of the OS Manager).
- The image will be downloaded only if the Service Multicast Eligible option is selected for the OS Service. To do this, use the Portal to navigate to the appropriate Operating System service.
  a. Click **Modify Instance**.
  b. In the workspace, click **Advanced**.
  c. Scroll to the bottom of the screen and make sure that Service Multicast Eligible is selected.
- Images must be a maximum of 4 GB. If they are larger than 4 GB, the image download will fail when using multicast.

# Configuring Multicast for OS Manager

To configure multicast for use with the OS Manager complete the following steps.

### To configure reliable delivery multicast

1 Go to the appropriate Behavior instance.

2 In the workspace, click **Advanced**.

3 Click **Modify Instance**.

4 Modify the ROMA Parameters field as follows:

```
-multicast multicastIPAddress:3463 -mcastretrycount 1
-mcastretrywait 240
```

**Table 13 Description of ROMA Parameters**

| Parameter | Description |
|---|---|
| `multicastIPAddress` | This parameter specifies the Multicast Server host. You can also use the host name. 3463 is the default Multicast Server port. |
| `mcastretrycount` | This parameter specifies the number of times that the client will retry multicast if there is a failure. The default value is 1. |
| `mcastretrywait` | This parameter specifies how long to wait before the client will start the retry. The default value is 240 seconds. |

5 Modify `SystemDrive:\Program Files\Hewlett-Packard\CM\MulticastServer\etc\mcast.cfg` as needed.

- `root`
  Specifies the root directory from which the Multicast Server will retrieve resources.
- `address`
  Specifies a range of multicast IP addresses available for use with dynamic windows. Refer to the *HP Client Automation Multicast Server Installation and Configuration Guide* for more information about dynamic windows.
- `Minref`
  Specifies the minimum number of clients that are required to contact the multicast server to start a multicast session. By default, `minref=2`. You may want to change this to take advantage of multicast's functionality.
- `CWINDOW`
  Specifies the length of the collection window; how long to wait for

clients to register for a given OS service before finalizing the setup of a multicast session. Change the value for this parameter based on your requirements.

Refer to the *HP Client Automation Multicast Server Installation and Configuration Guide* for more information about the parameters in this file.

6 If you made changes to `mcast.cfg`, restart the Multicast Service to implement your changes.

You may notice a `multicast.rc` file in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\MulticastServer\etc`.

Do *not* make any changes to this file.

# Improving Performance and Reliability for Multicast with OS Manager

The default values of the multicast parameters provide a good combination of reliability and performance in many environments. Optimal performance (transfer speed) is relative to your network environment. Therefore, you must determine what is optimal for your environment and then use the parameters defined in this topic to increase reliability and performance.

The fundamental problem surrounding the reliability and performance issues of the multicast transfer is packet loss. Because multicast is a UDP based protocol, delivery of packets is not guaranteed.

External factors that contribute to packet loss are:

- Network conditions. The amount of traffic on the network, the number of routers between the server and client, and faulty network connections, all can contribute to packet loss during multicast transfers.
- Agent conditions. The relative CPU, I/O and network performance of the agents can contribute to packet loss specific to the clients in question. If an agent is unable to read packets fast enough, some of those packets will be missed.

In any environment, packet loss is inevitable. The key is to find the balance between minimal packet loss and high data transfer rates in order to optimize actual throughput.

## Terminology

It is important to understand of how multicast handles the transfer of images. A sender (server) sends packets to a receiver (agent). The agent receives the data. If the data has not been received in its complete form, the client sends a resend request to the server. The server resends the packets to attempt to complete the transfer successfully. Below you will be introduced to some of the terminology that you will see used throughout this topic.

### actual throughput

The size of the operating system image divided by the time it takes to transfer the image.

### agent (receiver)

The agent that receives the multicast transmission.

### image

The data that is transmitted from the server to its clients in a single multicast session. For the OS Manager, this is an operating system image.

### multicast transfer

The process of sending data from the server to the client.

### packet

A unit of information sent over a computer network.

### packet loss

When the agent does not receive one or more packets sent by the server.

### performance

The time it takes to transfer the image.

### raw data transfer rate

The total number of packets (fixed size of data) sent over time, including packets that have been resent.

### reliability

The likelihood that the multicast transfer will complete successfully.

### resend block

A group of packets to be resent as a result of a resend request (NACK).

### resend request/negative acknowledgment (NACK)

A message sent from the client to the server indicating the client did not receive a specific piece of data .

### server (sender)

The agent that transmits the data to its clients via multicast. For the OS Manager, this data is an operating system image.

## About the Multicast Parameters

This section describes the multicast parameters whose values may need to be modified in order to increase performance and/or reliability.

**Table 14 Multicast parameters**

| Parameter | Used by | Definition | Default Value |
|---|---|---|---|
| `gddelaybp` | Sender | Inter-packet delay. The number of milliseconds to wait after sending a packet before sending the next one. | 0.0625 |
| `lingercount` | Sender | The number of times to check for resend requests (NACKs) after the last packet has been sent before determining that the transfer is complete. | 512 |
| `lingerdelay` | Sender | The delay, in milliseconds, between checking for resend requests (NACKs) after the last packet has been sent. | 32.0 |

| Parameter | Used by | Definition | Default Value |
|---|---|---|---|
| `lprcount` | Sender | The number of times the last packet of the image is retransmitted in order to increase the probability that the receiver sees the last packet.<br>Note that the receiver recognizes the last packet because it contains a flag indicating that it is the last packet. | 4 |
| `lprdelay` | Sender | The delay, in milliseconds, between each attempt to resend the last packet. | .25 |
| `maxrsndreq` | Receiver | The maximum number of resend requests (NACKs) that can be issued for a given block.<br>A block contains a number of packets. The size of a block is defined by the `numpktblks` parameter described below. | 4098 |
| `nacdelay` | Receiver | The delay, in milliseconds, between resends of a specific NACK. | 0.5 |
| `nacresend` | Receiver | The number of times to resend each NACK. | 2 |
| `netinacto` | Receiver | Network inactivity time-out. The number of minutes of network inactivity allowed between received packets before the receiver fails. | 5 |
| `numpktblks` | Sender or Receiver | Defines the size of the pool from which resend requests are fulfilled. | 64 |

| Parameter | Used by | Definition | Default Value |
|---|---|---|---|
| `pktsperblk` | Sender or Receiver | Specifies the number of packets within a resend block.<br>This is the minimum number of packets that will be resent as a result of a NACK. The total number of these packets is considered a resend block.<br>This value must be a multiple of 32. If you do not follow this requirement, your value will be adjusted and noted in the `gdmcsend.log` and the OS Manager System Agent logs. | 256 |
| `recvtimeout` | Receiver | The maximum time, in minutes, that is allowed for the total data transfer before it is considered a failed transfer. | 45 |
| `throtfreq` | Sender | Throttle frequency.<br>Specifies how often to check to see if the inter-packet delay should be adjusted. | 8 |
| `throthighth` | Sender | Throttle high threshold.<br>The number of average resends per block that will trigger an increment of the inter-packet delay. | -1 (disabled)<br>Note: To enable this, set it to a positive integer. |
| `throtincr` | Sender | Throttle increment.<br>The value, in milliseconds, that is automatically added to (or subtracted from) the current inter-packet delay each time the throttle is adjusted.<br>See Auto Throttle on page 178 for more information. | 0.01 |
| `throtlowth` | Sender | Throttle low threshold.<br>The number of average resends per block that will trigger a decrement of the inter-packet delay. | -1 (disabled)<br>Note: To enable this, set it to a positive integer. |

| Parameter | Used by | Definition | Default Value |
|---|---|---|---|
| throtmax | Sender | Throttle maximum.<br>The maximum inter-packet delay, in milliseconds, that can be set by the throttle. | 0.5 |
| throtmin | Sender | Throttle minimum.<br>The minimum inter-packet delay, in milliseconds, that can be set by the throttle. | 0.0 |
| ttl | Sender | Time to live.<br>The number of subnets that the packet will reach.<br>Every time a packet reaches a switch the ttl value is decremented until it reaches 0. If the value is 0, the packet cannot cross the switch.<br>This limits how far the packets can spread from the sender. | 3 |

## How the Parameters Influence Multicast Data Transfer

This section provides a more in-depth description of the parameters, including the influence they have on the multicast data transfer and their interaction with each other.

### Understanding Inter-packet Delay

The raw data transfer rate of the sender is influenced by the inter-packet delay parameter (gddelaybp).

Gddelaybp represents the number of milliseconds to wait after sending a packet before sending the next.

Increasing the inter-packet delay will decrease the raw data transfer rate of the sender. In general lower transfer rates will result in less packet loss. If the transfer rate is too low, it will have a negative impact on the actual throughput.

To give you a feeling for the impact this parameter can have on the actual throughput, consider the example of transferring a one gigabyte image using a 1 millisecond inter-packet delay. One gigabyte is 1,073,741,824 bytes. Assuming each packet is 1024 bytes, the image can be transferred in 1,048,576 packets at best. Given a one millisecond delay for each packet, the delays alone would total more than 1048 seconds. This means that it would take over 17 minutes to transfer the image, assuming no packet loss at all. In actuality, some packets probably will be lost, requiring some of the data to be resent; each resend packet consuming at least one millisecond.

Approaching this from the other direction, say we want to be able to transfer the one gigabyte image in under five minutes. Five minutes equals 300,000 milliseconds. Dividing that by 1,048,576 packets gives us about 0.3 milliseconds per packet. So, before we can even hope to transfer the image in under five minutes, the inter-packet delay must be less than 0.3. Unfortunately, lowering this value will more than likely result in greater packet loss and in turn, more resent packets.

To what degree lowering the inter-packet delay results in greater packet loss depends on the network and client conditions. While some conditions may support very low inter-packet delay values with minimal packet loss, others may not. Normally, when the conditions cannot support a given raw data transfer rate, the actual throughput will suffer due to the number of resends required to complete the transfer. In extreme cases however, the transfer may fail.

## About the Buffer Settings

While the buffer settings do not have an impact on the raw data transfer rate, they can have significant impact on the reliability and actual throughput of the transfer.

The buffer, as defined by the `numpktblks` and `pktsperblk` parameters, influences the following characteristics of the multicast transfer:

- The maximum number of packets the receiver can handle before it has the opportunity to write out the packets received first. For slower clients, there may be periods during the transfer where packets are being received faster than they can be written out, or an unfulfilled resend request may prevent a buffer from being written out, causing received packets to backup. During these periods, the overall size of the buffer (`numpktblks` * `pktsperblk`) defines the number of packets that can be received before the backup is alleviated. If the buffer limit is exceeded before the backup is alleviated, the transfer will fail.

- On the sender side, the number of packet blocks (`numpktblks`) defines the size of the pool from which resend requests are fulfilled. If a resend request is made for a block that is no longer in this pool, the server will not be able to fulfill the request.
- On the receiver side, the number of packet blocks, `numpktblks`, defines the size of the pool of blocks for which resend requests can be made.
- The size of each packet block (`pktsperblk`) defines the minimum number of packets that will be resent as a result of a resend request (NACK). The optimum packet block size depends on the overall distribution of lost packets. If lost packets are few and far between, then smaller packet blocks will minimize the overhead associated with the acquisition of each lost packet. If lost packets tend to be grouped together, then larger packet blocks may minimize the number of resend requests (NACKs) required to acquire the missing packets.

## Handling Special Packets

As we mentioned earlier, multicast, being a UDP based protocol, does not guarantee delivery of packets. The protocol used to send resend requests from the receivers to the sender is based on UDP as well, so delivery of resend requests is not guaranteed. However, we are relying on the resend requests to ensure the delivery of the packets. In addition, the last packet sent from the sender is used to trigger resend requests from the receiver as needed. If the last packet is lost, receivers will not know to request resends for the missing packets, including the last one.

Because we cannot rely on a resend request to ensure that a resend request is received, we must fall back on a more fundamental way to minimize the probability that these special packets will be lost. To do this, we send a fixed number duplicates for each of these types of packets, to ensure that at least one of them will be received by the clients. The parameters used to do this are:

- `nackresend` defines the number of times each NACK packet is retransmitted.
- `nackdelay` defines the delay between each retransmission.
- `lprcount` defines the number of times the last packet of the image is re-transmitted.
- `lprdelay` the delay between each retransmission.

The more clients participating in the multicast session, the lower the need for many NACK resends. Assuming many of the lost packets will be common to a

large number of receivers, more often than not, multiple receivers will NACK the same blocks.

## Handling the End of Image

After the multicast server has sent the last packet of the image, it needs to wait to see if there are any remaining NACKs that need to be serviced before exiting. The `lingercount` and `lingerdelay` parameters govern how this is done.

`Lingercount` - The number of times to check for resend requests (NACKs) after the last packet has been sent before determining that the transfer is complete.

`Lingerdelay` - The delay, in milliseconds, between checking for resend requests (NACKs) after the last packet has been sent.

Basically, the server checks for NACKs *`lingercount`* times and waits *`lingerdelay`* milliseconds between each check. If the server does not see a NACK in that period, it exits. If it does receive NACKs, it services them and starts checking all over again.

If these parameters are set too low, the server may exit before it receives the remaining NACKs from its clients. If this happens, the transfer to the clients with unfulfilled NACKs will fail. In the event of failure, the transfer will be retried if you have set `mcastretrycount` to a value greater than 0.

## Auto Throttle

The intent of this feature is to prevent adverse network and/or client conditions from causing the actual throughput from degrading to unacceptable levels, not to optimize throughput; although, in some cases, it may accomplish just that.

This feature attempts to keep the average NACKs per block within a predefined band. This is accomplished by modifying the inter-packet delay (`gddelaybp`) whenever the average NACKs per block falls outside the band. The band is defined by high (`throthighth`) and low (`throtlowth`) throttle threshold values, where the high threshold is the maximum desired NACKs per block and the low threshold the minimum.

After each packet block is sent for the first time, the n-moving average for the last *n* packet blocks is computed, where *n* is the number of packet blocks currently configured (`numpktblks`). When the throttle is checked, this moving average is compared to the high and low throttle thresholds, and the inter-packet delay is adjusted accordingly. If the moving average is greater than

the high throttle threshold, a configurable value (`throtincr`) is added to the inter-packet delay. If the moving average is less than the low throttle threshold, the same configurable value is subtracted from the inter-packet delay. High (`throtmax`) and low (`throtmin`) limits for the inter-packet delay are also defined. If a throttle adjustment would cause the inter-packet delay to exceed either of these limits, the adjustment will not be made.

The throttle is checked after every `throtfreq` packet blocks are sent. Here, `throtfreq` is the configurable throttle frequency. Actually, this is the throttle period, as it defines the number of packet blocks between throttle adjustments. The intent here is to give any previous adjustments an opportunity to influence the results, before checking the throttle again.

# Analyzing Problems

This section describes haw to identify, analyze and resolve multicast data transfer problems.

## About the Logs

The sender's log — `gdmcsend.log` — is typically stored in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\MulticastServer\logs`.

The receiver log is typically appended to the end of the OS Manager System Agent log for the device.

## Poor Performance

As mentioned before, poor multicast transfer performance is usually due to poor network and/or agent conditions. Such conditions result in the generation of an excessive number of resend requests (NACKs) from one or more of the clients, slowing down the entire transfer.

Before you can resolve the performance issue, you must first determine the root cause of the problem. To do so, examine the contents of the multicast sender's log file, `gdmcsend.log`. Review the following steps to guide you in determining the cause of the problem.

1. Determine is the average number of resends per block for the transfer in question. Look for the line in the log file in the form:

```
Avg resends per block = 0.00283688
```

Averages less than one are very good. This indicates that most of the packet blocks were sent only one time, with relatively few resends. Large values may indicate a problem. What to consider large depends on the value of the inter-packet delay, `gddelaybp`. Remember, there is a trade-off between raw data transfer rates and packet loss, so you can expect more NACKs when the inter-packet delay is small.

2 If the average resends per block indicates that there is a problem, examine the per-client statistics for the transfer. In the same log file, look for lines in the form:

```
Client stats:
Client: 16.119.237.171 (0xabed7710) NACKs = 19714
Client: 16.119.237.207 (0xabed7710) NACKs = 102
Client: 16.119.237.122 (0xabed7710) NACKs = 17
Client: 16.119.237.217 (0xabed7710) NACKs = 8
```

Each client is identified by its IP address. The client that has been issued the most resend requests (NACKs) appears at the top of the list.

If there are one or more agents that top the list whose NACK count far exceed those of the other agents, it is a strong indication that the problem is specific to the agents in question. After the problematic agents have been identified, you can try to determine what sets them apart from the others. Some considerations:

a Are the problematic clients on a different subnet than the others? If so, the problem may be specific to that subnet. Check the routers in the path from the server to the clients to see if any have seen a large number of errors on any of their ports. If so, it can be a router, port, or cabling problem.

b Are the agents in question slower than the others? Slow clients may be unable to keep up with high raw data transfer rates, causing them to miss more packets and in turn, NACK more often. If this is the case, you have a few options:

- Increase the inter-packet delay (`gddelaybp`) in order to lower the raw data transfer rate, so the slower agents will be better able to keep up. Even with the lower transfer rate, if the number of NACKs from these agents is significantly reduced, the actual throughput may increase.
- Whenever possible, do not include these clients in multicast sessions with faster agents. Put them in their own multicast session, or use unicast to deploy images to them.

c. If the clients are of comparable speed, the local network connections or cabling may be at fault. Check the cables and connections closest to the agents to see if they are causing the problem.

3. If all of the clients show a large number of NACKs, the problem is probably more systemic.

   a. The network may have been especially congested during the time of the transfer. Performing the transfer when the network is less busy may yield better results.

   d. Check the relevant network routers, connections and cabling as described above. This time, make sure to check the cables and connections from the server to the network.

   e. It could be that all of the machines are just too slow to keep up with the current raw data transfer rate. Increase the inter-packet delay to see if fixes the problem.

In some cases, enabling the auto-throttle feature is a better alternative than manually increasing the inter-packet delay. After the proper threshold values are set, the auto-throttle will adjust the inter-packet delay as needed.

## Client Time-out

Agents can time out for one of two reasons:

1. **Total image transfer time-out** occurs when the total time it takes to transfer the image exceeds the value of the recvtimeout parameter.
2. **Network inactivity time-out** occurs when the time between received packets exceeds the value of the `netinacto` parameter.

When a client times out, the type of time-out can be determined by examining the client's log file.

### Total Image Transfer Time-out

In the log file, a total image transfer time-out is indicated by a message in the form:

```
Module has timed out (timeout = nnn)
```

where *nnn* is the time-out value that has been exceeded.

Extreme cases of poor performance can lead to this type of failure, when the performance degrades to the point where the image cannot be transferred in

the time defined by the recvtimeout parameter. When this is the case, the same techniques described in Poor Performance on page 179, can be used to identify and resolve the problem.

### Network Inactivity Time-out

A log file message in the form:

```
Inactivity timeout has been exceeded.
```

is indicative of a network inactivity time-out.

This type of failure can be caused by almost anything that disrupts the flow of data from the server to the client. Premature termination of the multicast sender and various network problems can occasionally be at fault.

In some cases, it can result from the loss of one or more strategic packets. For example, the client in question may not have seen the last packet of the image. If this is the case, it will not know it needs to NACK the missing data. Having sent the last block and not seeing any NACKs, the server will not send more data. Expecting more data, the client will wait for the next packet until `netinacto` has been exceeded.

We can determine if the client missed the last packet of the image by examining the log files. In the sender's log file, `gdmcsend.log`, look for two lines in the form:

```
Last block: 3524
Packets in last block: 54
```

If they exist, then you know the sender sent the last packet.

Now, in the client's log file, look for a line like:

```
Last buffer size = nnn
```

If this line is not there, then you know the client did not see the last packet.

To remedy this problem, increase the value of the `lprcount` parameter. This will cause the last packet of the image to be retransmitted more times, increasing the probability that the client will see at least one of the redundant packets.

## Buffer Overflow

The primary causes of buffer overflow are slow clients and missing data.

## Slow Client

If the client is too slow, it may not be able to write out data fast enough, causing its buffer capacity to be exceeded. To determine if this is the case, look to the client's log file.

First, look for a line in the form:

```
Current block: 3289, High block: 3353
```

In this example, the value of the `numpktblks` parameter is 64. The fact that the difference between the current block (3289) and the high block (3353) is 64 indicates that all the buffers are in use.

Following this line are entries for every block that is not full. If there are no such entries or just a few near the high block range, it shows that most of the buffers are full, but the agent has not had the chance to write them out yet. For example, if the following line is:

```
Block: 3353, 32 packets of 256
```

It shows that all but the high block are full. This indicates that the agent may be too slow for the current raw data transfer rate. Here, you may want to consider increasing the inter-packet delay to see if the agent can better keep up with the lower raw data transfer rate.

## Missing Data

On the client, if a block is missing data, it cannot be written out. After that block becomes current, writing will stop and will not resume until the missing data is filled in. In the meantime, the remaining buffers are used to hold the incoming data. If the missing data is not filled in soon enough, the buffers may overflow. Normally, the client will NACK the missing data and the holes will be filled in long before this happens.

In the client's log file, the indicators of this condition are similar to those of the slow client case. The line:

```
Current block: 3289, High block: 3353
```

should look essentially the same, showing all of the buffers in use.

In this case however, the following line will show that the current buffer is not full:

```
Block: 3289, 32 packets of 256
```

Now the question becomes, why is this data missing? The agent should have sent a NACK requesting that this block be resent and the data should have been resent by the server.

There are two possibilities: the NACK was never sent or the server never received it.

First, let us see if the block was indeed NACK'ed. In the client's log file, look for the statistics associated with the block in question:

```
Block: 3289, 32 packets of 256
Resends requested: 1
```

Here you see one NACK was sent for the block.

Now, see if all of the NACKs the client sent got through to the server. In the client log file, there should be a line in the form:

```
Total resend requests = 8
```

Here, you see that the agent sent eight NACKs to the server. In the server log file, look at the per- agent data. After the line:

```
Client stats:
```

is a list of agents and the number of NACKs the server has received from each. Using the agent's IP address, find the line associated with the client in question. It should look something like this:

```
Client: 16.119.237.171 (0xabed7710) NACKs = 8
```

Here you can see that the server did receive all the NACKs the client sent. If these numbers were not the same, it would indicate that one or more NACKs had been lost. In that case, you should increase the value of the `nackresend` parameter. This will cause each NACK packet to be retransmitted more times, increasing the probability that the client will see at least one of the redundant packets.

For the case where the server has seen all the NACKs sent from the client, it probably indicates that the client did not issue a NACK when it needed to.

In the agent log file, look for the following line:

```
Max resend hits = n
```

Here, `n` is the number of times the client did not issue a NACK because the value of the `maxresendreq` parameter had been exceeded. If you cannot remedy the cause of the excessive number of NACKs, you may want to increase the value of `maxresendreq`, thus enabling the client to NACK a given block more times.

# Test Modules

The following commands are provided as test tools that you can use to manually test different combinations of parameters, rather than running tests in the full OS Manager environment.

## Using GDMCSEND

The `gdmcsend` command can be run from a Windows environment only.

`gdmcsend` is the server side multicast send command.

On the 5.00 media in `Infrastructure\extended_infrastructure\multicast_server\multicast_test_modules\` there is a script called `gdmsend.cmd` that can be used for testing.

### To start the multicast test sender module

1. Copy the multicast test send modules (`gdmcsend.exe`, `gdmcsend.cmd`, and `TESTDATA0004`) from the `extended_infrastructure\multicast_server\multicast_test_modules` directory on the infrastructure CD to a temporary directory.
2. Rename `TESTDATA0004` to `GDMCTESTDATA`.
3. Edit `gdmsend.cmd` and change `DP` on line 19 from `0.0` to `0.5`.
4. Edit `gdmsend.cmd` and change `OFFSET` on line 49 from `60` to `0`.
5. Run `gdmsend`.

If you want to modify the script, use a text editor to open the file and modify the parameters. Then, you can run this file to test the changes you made. See Example of Using the Test Modules on page 193.

When setting values for parameters that apply to both `gdmcsend` and `gdmrecv`, the values must match.

Below are two forms of the command and the valid options for each. Explanations of the parameters follow.

Use this command if you are using reliable delivery resend mode.

```
gdmcsend -rm D|B -ma multicast_address -mp multicast_port -np
nac_port-f file_name -npb nblocks -ppb npackets[-dp1 delay] [-
```

```
dp delay] [-dl delay] [-lc n] [-lf log_file][-nr n] [-ttl n]
[-lpr n] [-lprd delay] [-offset n_bytes][-ni ip_address][-tf
throttle_frequency] [-ti throttle_increment][-tmax
throttle_maximum] [-tmin throttle_minimum][-tthigh
high_throttle_threshold][-ttlow low_throttle_threshold]
```

Use this command if you are using the fixed resend mode, which resends each packet block a fixed number of times.

```
gdmcsend -rm F -ma multicast_address -mp multicast_port -f
file_name-ppb npackets -nr number_of_resends[-dp1 delay] [-dp
delay] [-lf log_file] [-nr n] [-ttl n][-lpr n] [-lprd delay]
[-offset n_bytes] [-ni ip_address]
```

**Table 15 gdmcsend command options**

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **-dl** *linger_delay* | lingerdelay | The delay, in milliseconds, between checking for resend requests after the last packet has been sent. | 64.0 |
| **-dp** *delay* | gddelaybp | Delay, in milliseconds, after sending each packet. | 0.0625 |
| **-dp1** *delay* | N/A | Delay, in milliseconds, after sending the first packet. | 5 |
| **-f** *filename* | N/A | Name of the file containing the data to be sent. | N/A |
| **-lc** *n* | lingercount | Linger count. The number of times to check for resend requests (NACKs), after the last packet has been sent. | 256 |

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **-lf** *log_file* | N/A | The name of the log file. The log file is stored in the directory where you execute the command.<br>You may use this parameter to change the name of the log file or provide an absolute or relative path. | `gdmcsend.log` |
| **-lpr** *n* | `lprcount` | Last packet resend. The number of times to resend the last packet. | 4 |
| **-lprd** *delay* | `lprdelay` | Last packet resend delay. The delay, in milliseconds, between last packet resends. | 0.25 |
| **-ma** *multicast_address* | N/A | Multicast address. The address to which the data is sent. | N/A |
| **-mp** *multicast_port* | N/A | Multicast port. The port to which the data is sent. | N/A |
| **-ni** *ip_address* | N/A | Network interface. The IP address identifies the specific local network interface to use when sending data. | selected automatically |
| **-np** *nac_port* | N/A | NACK port. The port from which resend requests are read. | 9514 |

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **-npb** *nblocks* | N/A | Number of packet blocks. The number of packet blocks available to be resent. | N/A |
| **-nr n** | | The number of times to resend each packet.<br>This option only applies when resend mode (**-rm**) is set to **F**. | 0 |
| **-offset** *n_bytes* | N/A | Skip the first *n_bytes* bytes of the file. | 0 |
| **-ppb** *npackets* | N/A | Packets per block. The number of packets in each packet block (must be a multiple of 32). | N/A |
| **-rm F\|B\|D** | N/A | Resend mode.<br>**F = fixed**<br>Each packet block is resent a fixed number of times (as specified by the **-nr** option).<br>**B = backup**<br>Resend all blocks from the lowest number requested to the current block (last block sent by the sender).<br>**D = discrete**<br>Resend only requested blocks. | B |

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **-tf** *throttle_frequency* | throtfreq | The minimum number of packet blocks between throttle adjustments. | 8 |
| **-ti** *throttle_increment* | throtincr | The value, in milliseconds, that is added to (or subtracted from) the current inter-packet delay each time the throttle needs to be adjusted. | 0.01 |
| **-tmax** *throttle_maximum* | throtmax | The maximum value of the inter-packet delay before throttling will stop. | 0.5 |
| **-tmin** *throttle_minimum* | throtmin | The minimum value of the inter-packet delay before throttling will stop. | 0.0 |
| **-tthigh** *high_throttle_threshold* | throthighth | The average number of resends per block that will trigger an increment of the inter-packet delay. | -1 (throttling disabled) |
| **-ttlow** *low_throttle_threshold* | throtlowth | The average number of resends per block that will trigger a decrement of the inter-packet delay. | -1 (throttling disabled) |
| **-ttl n** | ttl | Time to live.<br>The number of subnets that the packet will reach. | 3 |

## Using GDMCRECV

`Gdmcrecv` is the client side multicast receive command.

The `gdmcrecv` command can only be run from the Service Operating System as booted from the OS Manager CD-ROM in TESTMODE. If necessary, use a nano editor to modify the shell script, `gdmrecv.sh`. For an example of how this may be used, see Example of Using the Test Modules on page 193.

When setting values for parameters that apply to both `gdmcsend` and `gdmrecv`, the values must match.

Below are two sample commands and explanations of the parameters follow.

Use this command if you are using reliable delivery resend mode.

```
gdmcrecv -rm D|B -ma multicast_address -mp multicast_port -np
nac_port-na nac_address -npb nblocks -ppb npackets[-t
timeout_minutes] [-nit timeout_minutes][-mr max_resend_req] [-
nd nac_delay] [-nr nac_resends][-lf log_file] [-bt
block_threshold] [-ni ip_address][-pmf freq] [-stderr]
```

Use this command if you are using the fixed resend mode which resends each packet block a fixed number of times.

```
gdmcrecv -rm F -ma multicast_address -mp multicast_port -ppb
npackets[-t timeout_minutes] [-nit timeout_minutes][-lf
log_file] [-ni ip_address]
```

**Table 16 gdmcrecv command options**

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **`-bt`** *`block_threshold`* | N/A | Block threshold. When the number of used blocks exceeds this value, resend requests are sent even if all data has been received in order to slow down the sender. | 0 |

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **-lf** *log_file* | N/A | Name of log file.<br>The log file is stored in the directory where you execute the command.<br>You may use this parameter to change the name of the log file or provide an absolute or relative path. | gdmcrecv.log |
| **-ma** *multicast_address* | N/A | Multicast address. The address from which data is read. | N/A |
| **-mp** *multicast_port* | N/A | Multicast port. The port from which data is read. | N/A |
| **-mr** *max_resend_req* | maxrsndreq | The maximum number of times a resend can be requested for each block. | 128 |
| **-na** *nac_address* | N/A | NACK address. The address to which resend requests are sent. | N/A |
| **-nd** *nac_delay* | nacdelay | The delay, in milliseconds, between sending resend requests. | 0.5 |
| **-ni** *ip_address* | N/A | Network interface. The IP address that identifies the specific local network interface to use to receive data. | selected automatically |

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **-nit** *timeout_minutes* | netinacto | The time to wait, in minutes, between received packets before failing. | 5 |
| **-np** *nac_port* | N/A | NACK port. The port to which resend requests are sent. | 9514 |
| **-npb** *nblocks* | numpktblks | Number of packet blocks. The maximum number of packet blocks that can be serviced by resend requests at any point in time. | N/A |
| **-nr** *nac_resend* | nacresend | The number of times each NACK should be resent. | 4 |
| **-pmf** *freq* | N/A | Progress meter frequency. The progress meter is updated after every freq packet blocks have been written out. A value of zero disables the progress meter. | 0 |
| **-ppb** *npackets* | pktsperblk | Packets per block. The number of packets in each packet block (must be a multiple of 32 and match the value used by the sender). | N/A |

| Option | Corresponding parameter in mcast.cfg | Description | Default |
|---|---|---|---|
| **`-rm F\|B\|D`** | N/A | Resend mode.<br>**F = fixed**<br>Each packet block is resent a fixed number of times (as specified by the -nr option).<br>**B = backup**<br>Resend all blocks from the lowest requested to the current. The receiver will only send resend requests (NACKs) for the lowest block needed.<br>**D = discrete**<br>Resend only requested blocks. The receiver will send resend requests (NACKs) for every block needed. | B |
| **`-stderr`** | N/A | Write log messages to *`stderr`* (standard error), as well as the log file. | FALSE |
| **`-t`** *`timeout_minutes`* | `recvtimeout` | The maximum time, in minutes, before the data transfer fails. | 45 |

## Example of Using the Test Modules

This is an example of how to transfer a test image from the sender to the receiver with parameters specified in `gdmsend.cmd` and `gdmrecv.sh`.

## Sample Test Configuration

- A multicast server, named mserver1 with an IP address of 192.168.1.4.
- A multicast client (used for testing) mclient1 with an IP address of 192.168.1.50.
- A multicast transfer will use the multicast address 231.1.222.8 and port of 9511.

You must start the receiver before the sender.

### To start the receiver on the multicast client

1 Use the OS Manager media to boot the machine named mclient1.

2 At the boot prompt, type **`testmode`** and press **Enter** on your keyboard.

When Linux is finished booting, you will see the following on screen.

Use **Alt-F1**, **Alt-F2**, and **Alt-F3** to switch between virtual terminals.

Hold down the **Alt** key and press the **F2** key.

3 At the bash prompt (#), type **`cd /work`** and press **Enter** on the keyboard.

4 Type **`./gdmrecv.sh 192.168.1.4`** and press **Enter** on the keyboard. 192.168.1.4 is the NACK IP address for mserver1.

If you want to change parameters passed to `gdmcrecv`, use a nano editor to modify the shell script.

### To start the sender on the multicast server

1 If necessary, change to the directory where the `gdmsend.cmd` is located.

2 From a command prompt, type **`gdmsend.cmd`** and press **Enter**.

# 10 Advanced Features

At the end of this chapter, you will:

- Be able to restore operating systems in a last resort situation.
- Be able to capture, recover or migrate user data and settings.
- Be able to use HP Client Automation Client Operation Profiles with the OS Manager.

This chapter discusses advanced features that are available with the OS Manager. These features are for use by those who are extremely comfortable with HP Client Automation.

# Restoring Operating Systems

The OS Manager allows you to restore your operating system in last resort situations. Restoring the operating system provides you with a working operating system however *you will lose all data* and you may need to perform some customizations such as changing the computer name or installing the agent.

The ROM object will not be updated and therefore may not reflect the device's actual state.

### Pre-requisite

- The ImageDeploy media. See Product Media on page 29 if you need more information about how to create this media.
- A working operating system stored on the network, to a cached location or on a CD/DVD.

### To recover your operating system

1. Insert the CD-ROM that you created from the ImageDeploy`.iso` in the `\service_cd` folder on the product CD-ROM.
2. Boot the target device.
3. When asked which Service OS to use, select _SVC_LINUX_ or SVC_PEX86_.
4. You will see several messages and then a menu opens with the following choices:
   - 1. Service OS networking (default selection if no option is chosen)
   - 2. Install OS from cache partition
   - 3. Install OS from CD or DVD
5. Type the number corresponding to the action you want. If you select:
   - 1. Service OS Networking you must be connected to a network.

If you chose to use the Linux Service OS, and DHCP is found, you will be prompted for the OS Manager Server's IP address and then the appropriate OS image will be installed to your device.

or

If DHCP is not found, you will be prompted for network information such as the following before the appropriate OS image can be installed to your machine:

- IP address for the target device
- Default gateway
- Subnet
- Subnet mask
- DNS address
- OS Manager Server IP address

You may choose to store the network information on a USB drive or floppy disk. To do this, prepare the following `.ini` files:

- `romsinfo.ini`
  This includes information about the OS Manager Server. It should be ordered from the top down with the most-specific information to the least-specific information. When a match to the OS Manager Server s found on the left, the information on the right will be used.

  In the sample romsinfo.ini file below:

  ```
  [ROMSInfo]

  192.128.1.99=192.168.123.*, 192.168.124.*,
  192.128.125.*

  osm.usa.hp.com=192.168.*

  osm.hp.com=*
  ```

  The first line looks at the machine to see if it falls within one of the subnets listed (192.168.123.*, 192.168.124.*, 192.128.125.*). The asterisk is used as a wildcard. If there is a match, then the machine will use the OS Manager Server with the IP address specified on the left (e.g., 192.128.1.99).

  If no match is found, then the second line of the file is used. This one looks at the machine to see if it falls within a subnet that begins with 192.168.*. If so, the machine will use osm.usa.hp.com to find the OS Manager Server.

If no match is found again, the third line of the file is used. This one indicates that osm.hp.com should be used to find the OS Manager to be used by the machine, no matter what subnet it is part of.

```
[ServiceCD]
source=net
netif=eth0
```

The first line defines where to get the image. Valid values are net, cd, or cache. Use this if you want to prevent the user from being prompted for this information.

The second line defines which NIC to use. If there are multiple NIC cards and you do not specify this parameter, then the first NIC card that is discovered will be used. Valid values are eth0 – eth3.

– `netinfo.ini`
This includes the networking information. If there is more than one section (such as a [SubnetDisplayName2], you will be prompted about which information to use.

You can use `addr` to specify a range of IP addresses. This allows you to store the information on one USB drive or floppy disk that will be useful for multiple machines.

```
[SubnetDisplayname1]
addr=192.168.123.50-192.168.123.69
gateway=192.168.123.254
subnet=192.168.1.0
netmask=255.255.255.0
dns=192.168.123.1
```

If you do not know the DNS, leave the keyword `dns=` in the `.ini` file.

Insert your recovery CD-ROM and then insert the USB drive or floppy disk shortly after the device begins to boot. When configuration is complete, you will see the message “Network configuration successful.”

— 2. Install OS from cache partition.

  If you have a target device that is managed by the OS Manager and you created a cache type partition as described in Table 10 on page 139, select this option to restore the operating system. You will be reminded that you will lose all data in the current partition. Then, you will see a message that says “Installing OS from cache partition”. This remains on screen for several minutes. When it is done, a message says to see the logs and provides you with the ability to switch consoles. Remove the Service CD and reboot the machine.

— 3. Install OS from CD or DVD

  If you have a target device that is managed by the OS Manager and you used the Download Resources task to create a CD or DVD, select this option to restore the operating system.

# Addressing Requirements for Capturing, Recovering, and Migrating Data

If you want to capture, recover, or migrate user data and settings (such as personality information), HP provides the ROM Client method (`romclimth.tkd` ), which has two exit points. This method is stored in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent`.

The exit points call two optional scripts—`Novapdc.cmd` (data capture) and `Novapdr.cmd` (data restore)—that must be also stored in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent`. You can use these scripts to customize data capture, recovery, and restoration for any product that you would like to use.

Capturing, recovering and migrating data relies on the OS Manager User Agent because data can be captured only when the OS is running. The Application Manager senses the change to a device's desired state and triggers the data capture if `Novapdc.cmd` is available in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent`. Then, the target device reboots and the new operating system is installed. If `Novapdr.cmd` is available, the ROM Client method begins the restore process after the OS has been installed on the target device.

## Sample Command Lines

The following is a sample of a command line used to capture data using HP Client Automation Settings Migration Manager.

```
Path\SE.exe /autoextract /http IntegrationServer:Port
UniqueName overwrite:yes /allusers
```

The following is a sample of a command line used to restore data using HP Settings Migration Manager.

```
Path\SE.exe" /autoinject /http IntegrationServer:Port
UniqueName /allusers
```

See *HP Settings Migration Manager's* documentation for more details.

## Return Codes for HP Exit Points

The following return codes are returned from the HP exit points `Novapdc.cmd` and `Novapdr.cmd`. The values may vary depending on the software that you are using with these exit points. If the return value of the method is not equivalent to the following, use the standard batch error level conditional processing and the exit command to make them correspond to the following:

**Table 17 HP Exit Point Return Codes**

| Code | Description |
|---|---|
| 0 | Successful. |
| 1 | An error occurred and will be logged, but processing will continue. The log is located in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log`. |
| 2 | For `Novapdc.cmd` (capture):<br>• A fatal error has occurred and will be logged. The log is located in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log`. Processing of the service has ended.<br>For `Novapdr.cmd` (restore):<br>• An error has occurred and will be logged. The log is located in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log`. The service is flagged but at the next HPCA OS connect, the Application Manager will attempt to install the service again. |

# Using HPCA Client Operations Profiles with OS Manager

Client Operations Profiles allow you to dynamically assign and select a target device's available Client Automation servers based on network location, network speed, or other criteria. For example, you may want to use this capability to assign Proxy Servers to your managed devices or designate fail-over Proxy Servers. The ability to specify Service Access Points (SAPs) so that managed devices can access alternate sources for image download is a OS Manager-specific extension to Client Operations Profiles.

When using Client Operations Profiles with the OS Manager, the OS Manager uses only the Configuration Server specified in `roms.cfg`. Therefore, fail-over for multiple Configuration Servers is not supported.

## Requirements

If you are using Client Operations Profiles for the OS Manager Server, you must use the same Configuration Server for both application deployment and operating system deployment.

- If you are using Local Service Boot:
  - your machine must be managed by the OS Manager.
  - If you are creating an SAP for the OS Manager Server, the TYPE must be set to ROM and the ROLE must be set to Z.

  See About Local Service Boot on page 157 for more information.
- Name instances in PRIMARY.CLIENT.LOCATION only by subnet.
- If you are using Client Operations Profiles, failover for the location of data is supported in the following scenarios:
  - If the first SAP is a CD but there are no valid resources on the current CD or there is no CD.
  - If there is more than one SAP for a Proxy Server, the OS Manager will failover from one SAP to another, respecting the connection order in the LOCATION instance. Client Operations Profiles can only be used to redirect the Application Manager and/or OS Manager Server to an alternate data source.

- If you want to deploy an image using a CD resource, set TYPE to DATA and ROLE to Z. Then, specify the URI as `cdr://` to indicate that you want to use the agent's local CD/DVD drive. The first CD/DVD drive detected is used.

## Using the Proxy Server with OS Manager Server and Client Operations Profiles

If you have a Proxy Server that contains OS images and applications, you would set up your SAP instances as follows:

- For the Proxy Server that contains OS images, create an SAP instance with the following settings:
  - TYPE=DATA
  - ROLE=Z
- If there is a Proxy Server that contains the all other data (such as applications), create the SAP instance with the following settings:
  - ROLE=D
- If there is a Proxy Server that contains all data, create SAP instances with the following settings
  - ROLE=DZ

# 11 Building a Custom WinPE Service OS

At the end of this chapter, you will:

- Be able to update the WinPE Service OS.
- Add extra drivers or packages to the WinPE SOS.
- Create a new ImageCapture.iso.
- Create a new ImageDeploy.iso.
- Be able to add support for Chinese, Japanese and Korean languages.

HP provides a script that allows you to:

- Update the WinPE Service OS when a new `winpe.wim` is made available through an updated WAIK. The `winpe.wim` from the WAIK is used as the basis for building the customized WinPE SOS.
- Add extra drivers or packages that do not exist in the WinPE SOS provided. Follow the instructions below in conjunction with your knowledge of Microsoft's Windows Automated Installation Kit to rebuild the WinPE Service OS with the drivers and packages necessary for your environment.
- Add support for Chinese, Japanese and Korean languages.
- Create a new ImageCapture.iso if you have updates that need to be applied such as a change to the default Service OS or to the configuration of the boot menu.
- Create a new ImageDeploy.iso if you have updates that need to be applied such as a change to the default Service OS or to the configuration of the boot menu.

## Prerequisites

- A machine with Windows Automated Installation Kit (WAIK) installed.

Do not use the machine where your Boot Server is installed.

- A good understanding of Microsoft's process to add drivers and other information to the WinPE SOS.
- Go to `\custom_build` on the product media and copy `build_scripts.zip` to the machine.
- Image Capture and Image Deploy CDs.
- Do not run this script on a machine that has cygwin installed as this is not supported.
- If you are generating a new `ImageCapture.iso` or `ImageDeploy.iso`, you must do the following to include the updated files necessary for your ISO.

  a. Create a build items directory on the machine such as `c:\build_items`.

b Copy the updated files that you received from CPE to the build items directory. Create subdirectories as needed, based on the structure on the Image Capture or Image Deploy media. If any required files are not in this directory, you will be prompted to insert the previous Image Capture or Image Deploy media so the files can be copied.

c (Optional) You can include `romsinfo.ini` (on page 199) or `netinfo.ini` (on page 200) in the build items directory for use on the ImageDeploy CD.

d (Optional) You can include `rombl_capture.cfg` and `rombl_deploy.cfg` in the build items directory for use on the appropriate iso. To create these files, copy `rombl.cfg` from the previous `ImageCapture.ISO` or `ImageDeploy.ISO`, modify and rename them as necessary. The files contain information such as the menu timeout settings, and the default Service OS.

If you do not include these files in the directory, the script prompts you for the previous CD-ROM and retrieves the files from the media. If you choose not to insert a CD-ROM then a standard `rombl.cfg` file will be created automatically.

- If you want to add support for Chinese, Japanese and Korean (CJK) without making additional changes to the iso:
  - Remove any existing `winpe.wim` files from the `build_items` directory.
  - Copy `winpe_cjk.wim` from the `\custom_build\lang_support` directory on the product CD-ROM to the build_items directory.
  - Rename `winpe_cjk.wim` to `winpe.wim`.
  - See Building a Custom WinPE Service OS and Maintaining the Image Capture/Deploy ISOs on page 208 to run the script.

If you want to use the CJK-enabled winpe.wim file without rebuilding the `winpe.wim` file, be sure to type N when prompted to recreate the `winpe.wim`.

  - If you are using the ImageDeploy CD to install from CD or are installing from a cache and want messages to appear in your local language, copy the `\custom_build\lang_support\i18n` directory from the product CD-ROM to the `build_items` directory. You may remove the `.msg` files that are not needed for your local language.
- (Advanced option) If you are using a pre-existing `winpe.wim` file:

- It is strongly recommended that the pre-existing winpe.wim was built using the same version of WAIK that is installed on the computer where you are executing the build scripts.
- The file must have the following packages installed:
  - WinPE-HTA-Package
  - WinPE-Scripting-Package
  - WinPE-XML-Package
  - WinPE-WMI Package
- If your `winpe.wim` file has been prepared using the `peimg /prep` command see Microsoft WAIK, peimg, and ImageX documentation for restrictions.

## Adding Drivers to the WinPE Service OS

If you would like to add drivers to the WinPE Service OS, you can do this when running the build scripts. For example, if you have a driver that needs a reboot, you must do it in "offline" mode, which means that the build_script will pause and you can make any necessary changes at that time. This is described in detail in the steps below.

Additionally, you can add drivers to WinPE while it is running ("online"). The drivers must be fully contained without need for a reboot and the device must have connectivity to the OS Manager Server. During the startup of the WinPE SOS, any drivers that exist in `C`*`SystemDrive:`*`\`*`Program` `Files\Hewlett-Packard\CM\OSManagerServer\SOS\WinPE\drivers` will be downloaded and installed using drvload.exe.

## Building a Custom WinPE Service OS and Maintaining the Image Capture/Deploy ISOs

Be sure to review Prerequisites on page 206 before using the script.

### To use HP's script

1. Copy `Build_scripts.zip` to a location on the machine with WAIK installed.
2. Unzip `Build_scripts.zip` to a directory such as `C:\Build_scripts.`
3. Go to a Windows command prompt and change to the new directory. In this example, the directory would be `C:\ Build_scripts.`
4. Type **`run`**.
5. When asked whether you want to create a new WIM file, type **`Y`** or **`N`**.

If you are using `winpe_cjk.wim` and do not want to rebuild the winpe.wim file, be sure to type N when prompted to recreate the winpe.wim

6. If you type **`Y`**, you will be prompted to type the path to your Windows AIK tools directory, type the directory such as `C:\Program Files\Windows AIK\Tools`.
7. When asked whether you want to use the `winpe.WIM` file from the Microsoft Windows AIK, type **`Y`** or **`N`**.

It is strongly recommended that you use the `winpe.WIM` file from the Microsoft Windows AIK.

If you type **`N`**, you will be reminded to ensure that your pre-existing winpe.wim file is built according to specifications. Then, you will be prompted to specify the fully qualified path of the pre-existing `winpe.WIM` file.

8. When asked whether you want to include the local font support packages (Chinese, Japanese and Korean), type **`Y`** or **`N`**.
9. When asked whether you want to pause the WIM creation process to add extra drivers or packages, type **`Y`** or **`N`**.
10. When asked whether you want to create a new Image Capture ISO, type **`Y`** or **`N`**.
11. When asked whether you want to create a new Image Deploy ISO, type **`Y`** or **`N`**.

12 When asked which Service OSs to include on the ISOs, type the appropriate selection. Then, press Enter.

13 When asked if you want to create a new `rombl.cfg` or use a pre-existing `rombl.cfg` type the appropriate number. If you choose to use a pre-existing `rombl.cfg`, skip to step 17.

14 When asked which Service OS you want to boot by default, type the appropriate selection. Then, press Enter.

15 When asked to configure the boot menu for the Image Capture CD/DVD, type the appropriate value for your environment based on the on-screen description.

16 When asked to configure the boot menu for the Image Deploy CD/DVD, type the appropriate value for your environment based on the on-screen description.

17 When prompted to type the fully qualified path to the build items, type the directory such as `C:\build_items` and press Enter.

18 When prompted to type the fully qualified path for the temporary work directory, type a directory such as `C:\build_work`. This directory will be referred to as the `<work-dir>` in later steps.

If the directory already exists and has information in it, you will be asked whether you want to delete the information or not. If you choose no, you will be asked to type a directory again. If you prefer to exit, press **Ctrl + C** to exit the process. If you choose yes, the information will be overwritten.

19 When prompted to type the fully qualified path for the output directory, type a directory such as `C:\build_output`.

If you are prompted to create ISOs for CAS, type **`N`**.

20 If files that are required to build the ISO are not in the build items directory, you must insert the CD/DVD and the files will be copied. If you choose not to insert the CD/DVD, the build process will terminate.

21 The information you entered will be saved and the WinPE directory creation begins.

22 If you indicated that you wanted to pause the WIM creation process to add extra drivers or packages, the process will pause after the WinPE directory is created and the contents of `winpe.wim` are extracted into the WIM directory, e.g., `C:\build_work\WIM`,. There are two ways to do this:

a. Use the peimg command to make your modifications. This uses PEImg.exe which is included in the WAIK in C:\Program Files\Windows AIK\Tools\PETools\PEimg.exe. See the WAIK documentation for information about how to use this command or type **peimg /help**.

   This method is useful for testing the additional drivers and packages you are including. After you have successfully added the drivers and packages, you may want to use the next method so that you do not have to repeat this step manually each time you build a new winpe.wim.

b. Add drivers to a driver list. After you see a message indicating that all required information is gathered, build.config will be created in C:\ Build_scripts to store this information that is needed to build the winpe.wim and ISOs. Use a text editor to open this file and add the appropriate drivers below the empty DRIVERS list. For example:

```
declare DRIVERS = " \
        cdrom.inf \
        e:\\tmp\\work\\WIM\\windows\\inf\\adp94xx.inf \
        e:\\tmp\\work\\WIM\\windows\\inf\\3com*.inf \
"
```

   If you do not specify a directory, the script will search for the driver in the <work-dir>\WIM\Windows\inf. If you prefer, provide a fully qualified path that specifies the location and driver, such as c:\\anydirectory\\mydrivers.inf. The last option is to provide a path with a filename containing a wild card, such as c:\\anydirectory\\md*.inf which will install all md*.inf files found in c:\anydirectory.

   After you are done, type **run** to continue and the drivers will be added to winpe.wim.

   If you run the script again in the future, you will be prompted about whether you want to keep the build.config file or replace it with a new one. Also, the script will pause automatically. If you do not have additional packages or drivers to add, simply type **run** to continue.

23. This process takes some time as you will see from the messaging on screen. When done, you will see a message indicating that the SOS creation process completed successfully and be returned to a command prompt.

24 Go to the directory where the `WinPE.wim` was built, such as `C:\WinPE_output` and

- For PXE, copy `winpe.wim` to *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot`.
- For LSB, use the CSDB Editor to replace the `winpe.wim in the LSB package`.
- For the CD, you must create a new ISO using the winpe scripts.

If you chose to create a ImageCapture.iso or ImageDeploy.iso, it will be stored in this directory as well.

## Using Customized build.config Files (Advanced Option)

If you choose, you can take an existing `build.config` file and save it with another name. You may want to do this if you need to maintain varying sets of configurations or if you are testing based on an existing configuration. You can add drivers to the file as specified above.

Place the file in the directory where you unzipped the `build_scripts.zip` file, such as `C:\build_scripts`.

When you run the script, instead of typing **`run`** use the following command:

```
run.cmd -f mybuild.cfg
```

If you do not include the –f parameter, the default build.config will be created and used.

# 12 Double Byte Character Support

At the end of this chapter, you will:

- Know what languages are supported.
- Be able to add support for a supported language in a PXE environment.
- Be able to add support for a supported language when restoring from a CD-ROM.

This chapter discusses the changes made to the OS Manager for internationalization. These changes set the locale for the service operating system (SOS) and OS Manager System Agent messaging.

Internationalization is currently supported for the Linux service operating system only.

When creating an image (with the HPCA OS Manager Image Preparation Wizard or the HPCA Windows Native Install Packager) the locale for your reference and target devices must match. For example, if you want to create a Simplified Chinese OS image, you must run the Image Preparation Wizard or the Windows Native Install Packager on a Simplified Chinese reference machine.

If there are no double-byte requirements, do not make any of the following changes.

# Supported Languages

- Simplified Chinese
- Japanese
- Korean

# Changing the Locale

### To add support for Simplified Chinese, Japanese, or Korean in a PXE environment

1. Use a UNIX based text editor to open `C:\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot\linux.cfg\default`.

Do not use editors that automatically convert to Windows format, such as Notepad. You may use Nano or WordPad to modify the Boot Server's configuration files.

The file looks similar to the following:

```
[OS Manager]
DFLTSVOS=_SVC_LINUX_
ISVR=10.10.10.1:3469
[_SVC_LINUX_]
KERNEL=bzImage
APPEND initrd=rootfs.gz root=/dev/ram0 rw quiet pci=nommconf
[SVC_PEX86]
PEBCD=rombl.bcd
PEAPPEND=initrd=winpe.wim
```

Add the LANG parameter to the end of the APPEND line and set it to LANG=CJK. As a result, the line will look similar to the following:

```
APPEND initrd=rootfs.gz root=/dev/ram0 rw LANG=CJK
```

2 Save and close the default file.

### To add support for Simplified Chinese, Japanese, or Korean when restoring from the Service CD-ROM

- Specify LANG=CJK in the ServiceCD section of the `romsinfo.ini` file.

## Setting the System Language Parameter

In this section, you will set the System Language parameter in the Behavior instance. Doing so sets the locale for the service operating system and OS Manager System Agent messaging. This affects PXE environments, LSB environments and restoring operating systems from a CD-ROM or DVD.

### To set policy to enable support for other languages

1 Log in to the Portal as the OS Manager Administrator (by default the user id is **`romadmin`** and the password is **`secret`**).

2 Use the navigation aid to select the appropriate Configuration Server.

3 In the workspace, click **Behavior**.

4. Click the appropriate instance in the workspace and then click **Modify** to make changes.
5. Click **Advanced** to open the Advanced Properties section.
6. Change the System Language parameter to the appropriate language.
   - en_US = English
   - zh_CN = Simplified Chinese
   - ja_JP = Japanese
   - ko_KR = Korean
7. Set policy to deploy the images to the appropriate users.

## Double-byte support for Sysprep or Unattend.txt files

If using double byte char in Sysprep or unattend.txt the file must be encoded in UTF-8 coding.

# 13 Troubleshooting

At the end of this chapter, you will:

- Know where to find the OS Manager Server logs.
- Know where to find the Configuration Server and Configuration Server DB logs.
- Know where to find the HPCA OS Manager Image Preparation Wizard log.
- Know where to find the agent logs and objects.
- Know where to find the logs created when capturing, migrating, or recovering data.
- Be familiar with some basic infrastructure tests to determine whether your environment is configured properly.
- Understand what to provide to Technical Support when requesting help.
- Know what the Discover Boot Server Utility is and how to use it.

If your environment uses Core and Satellite servers, first read the *Core and Satellite Servers Getting Started Guide* as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

## OS Manager Server Logs

The OS Manager Server writes several logs, which can be used to track progress and diagnose problems. The log files for the OS Manager Server are:

- `httpd-`*`port`*`.log`
  This is the main log, stored by default in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\logs`. It contains information about the actions that you perform, as well as version and build numbers.

  Replace *`port`* with your port number, for example, `httpd-3469.log`.

  Each time you start the web server a new log is written. The old log is saved as `httpd-`*`port`*`.nn.log`.

- `httpd-`*`port`*`.YY.MM.DD.log`
  This log, stored by default in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\logs`, contains the web server activity for each day. If the log is empty, it means that there was no activity that day.

- `httpd-`*`port`*`.error.txt`
  This log, stored by default in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\logs`, contains messages written to any logs that contain the prefix ERROR. This allows you to view all errors in a single location.

- `machineID-all.log`
  This log, stored by default in *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload`, is a comprehensive log that is written after the OS Manager System Agent is executed. You will find one log for each device managed by the OS Manager. Open this log with WordPad, rather than Notepad.

  This log may be named `macAddress-all.log` if the machine instance has not been created.

The following example from this log shows that the Configuration Server and Proxy Server address are in use, which confirms a successful image deployment.

```
20030703 10:10:01 Info: ::HOSTINFO(RCSHOST)
:10.10.10.2:3464

20030703 10:10:01 Info: ::HOSTINFO(RPSHOST)
:10.10.10.2:3466
```

## Locating the Payloads

Payloads are the files that contain the modules that run under the Service OS. These files are provided by HP and can be found:

- in `\OSManagerServer\OSM\SOS\linux\payload` for Linux
- in `\OSManagerServer\OSM\SOS\winpe\payload` for WinPE

The payload file for Linux is named `LNX-`*`version`*`_00000.tgz` and the payload file for WinPE is named `WPE-`*`version`*`_00000.tgz`. The second three digits are the version number and the last five digits are the build number

## Configuration Server and Configuration Server DB Logs

Refer to the *HP Client Automation Enterprise Configuration Server User Guide.*

## Image Preparation Wizard Log

- `setup.log`
  This log is created while the Image Preparation Wizard is running in Windows. It is located in the `\setup` directory of the TEMP environment variable. It may be in a location similar to `c:\winnt\temp\setup.log`.

  `osclone.log`
  This log is created while osclone is running and is found in the local directory from which osclone is run (the Service OSs `\work` directory). When osclone is complete, the osclone.log is uploaded to the OS Manager's `\upload directory` as *`imagename`*`.log`.

## Agent Logs and Objects

Use the agent logs (*SystemDrive*:/Program Files/Hewlett-Packard/CM/Agent/Logs) and agent object information (*SystemDrive*:/Program Files/Hewlett-Packard/CM/Agent/LIB) on the managed device to confirm that the following OS Manager Server services have installed successfully during the first agent connect:

- Operating System Service
- OS Manager Server agent files

If policy dictates that the Local Service Boot service is installed, you can also confirm that the LSB service has been installed.

You may want to review the following agent logs located in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent\Logs:

- Connect.log
- Romclimth.log
  This log stores information about operating system (OS) service resolution.
- LSB.log
  This log contains information about LSB installation.

You may want to review the following agent object information (located in *SystemDrive*:\Program Files\Hewlett-Packard\CM\Agent\LIB):

- OS/ZSERVICE/MASTER.edm
  Review the ZMASTER object for the OS Service.

## Capturing, Migrating, or Recovering Data

If you use this capability, logs will be available in C:\Program Files\Hewlett-Packard\CM\Agent on the managed device.

# Basic Infrastructure Tests

After you have installed your OS Manager Server infrastructure, the following tests may help you to determine whether your environment is properly configured.

### Test 1: For use in an environment without bare metal machines

If you can answer yes to all of the following questions:

- Are you able to boot (via PXE) to a device that has not been discovered by OS Manager Server and does not have an OS that is managed by OS Manager Server?
- Does a device object get created in the Portal when a device is discovered?
- When a device is discovered, is a log uploaded to the OS Manager's `\upload` directory?

Then the following are working correctly:

- DHCP, PXE/TFTP Server, Configuration Server, Portal, and OS Manager Server are working correctly.
- The Configuration Server has the files needed to handle OS Manager Server objects.
- Service OS (Linux and/or WinPE) is able to handle the target device.

### Test 2: For use in an environment with bare metal machines

If you can answer yes to all of the following questions:

- Are you able to boot a bare metal machine via PXE?
- Does a device object get created in the Portal when a device is discovered?
- When a device is discovered, is a log uploaded to the OS Manager Server's `\upload` directory?
- Is an OS installed on the machine?

Then:

- DHCP, PXE/TFTP Server, Configuration Server, Portal, and OS Manager Server are working correctly.
- The Configuration Server has the necessary files to handle OS Manager Server (COP) objects.

- Service OS (Linux and/or WinPE) is able to handle the target device.
- OS Policy correctly chose one OS.
- The OS State for the MACHINE instance is set to DESIRED.

### Test Results

If any of the tests failed, you may have some problems with your infrastructure. Be sure to collect the following information:

- How are you trying to set up the infrastructure?
- In what order did you install the components?
- Gather the necessary logs related to your problem.

## Collecting Information for Technical Support

If you need to contact Technical Support for assistance, be sure to review the latest release notes and confirm that you have installed any fixes. If you still need assistance, then collect the following information:

- Hardware information (including manufacturer, model, BIOS/firmware version for the NIC card, hard drive controller card, and hard drive).
- Gather the following files or folders:
  - *SystemDrive:*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID-all.log`
  - *SystemDrive:*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID_rnl.log`
  - *SystemDrive:*`\Program Files\Hewlett-Packard\CM\OSManagerServer\logs` directory

    or

    *SystemDrive:*`\Program Files\Hewlett-Packard\CM\OSManagerServer\RomVer.log`
  - *SystemDrive:*`\Program Files\Hewlett-Packard\CM\ConfigurationServer\log\`*nvdmr001*`.log`. The 001 represents the ID used during the installation of the Configuration Server.

— If specifically requested, gather the `.MBR` and `.PAR` files from *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\UPLOAD` on the OS Manager Server.

- What results you were expecting, what actually happened, and any other related details.
- Whether the problem can be reproduced. If so, specify the exact steps (providing detailed information) to reproduce the issue.
- Specify whether the issue occurs on more than one device.
- Indicate whether the image was ever successfully deployed. If so, what has changed since the successful deployment?
- If deployment of an image stops and goes to a bash prompt, be sure to collect the `OSSELECT.log` file. Use the following command to copy the `OSSELECT.log` to the Integration Server `\upload` folder:

```
curl -T osselect.log
http://$ISVR:$ISVRPORT/upload/osselect.log
```

# Gathering Version Information

## OS Manager Server Components

To determine the versions of the OS Manager components, go to *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer` and run `Romver.cmd`. The log is created in the same directory.

## OS Manager Admin Module

To determine the versions of the OS Manager Admin Module components, go to *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\ManagementPortal` and run `Romadver.cmd`. The log is created in the same directory.

To determine the versions of the Configuration Server, go to *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\ConfigurationServer` and run `Rcsver.cmd`. The log is created in the same directory.

## NVDKIT.EXE and .TKD Files

- The module and version information for the following items can be found by running the `Romver.cmd` mentioned above.
  - `nvdkit.exe`
  - `expandsmbios.tkd`
  - `roms.tkd`
  - `roms_udp.tkd`
- See the `httpd-port.log` for version and build information.

## Configuration Server and Configuration Server Database

*HP Client Automation Enterprise Configuration Server User Guide*

## SOS/Payload/OS Manager System Agent

To determine the version of the SOS and payload that you were running, you can use a text editor to open *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID_rnl.log`. Look for `Extracting payload file` and check `LNX-`*`version`* for the Linux SOS and `WPE-`*`version`* for the WinPE SOS. If you find `OSD-50` this indicates you are using a 5.0 payload. Next look for `SOSVERSION=` to determine the version of the SOS.

To determine the version of the OS Management System Agent that you are running, you can use a text editor to open *`SystemDrive:`*`\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID-all.log`. The line will read similar to the following:

```
TKD Version: 7.20 Build ROMA Repository Revision:
$Revision: 1.106 $ running
```

## OS Manager Boot Loader

The version of OS Manager Boot Loader is displayed during the boot sequence. To find out the version number, you should do a PXE boot and one of the first lines will contain the version number. The version can also be found in `ROMBL_REV=` in the `machineID-all.log`.

# Frequently Asked Questions

- Can I upgrade from my previous version?
  See the *HP Client Automation Enterprise OS Manager Migration Guide*.
- Can I use the Linux SOS for Hardware Configuration Elements if I'm deploying Windows Vista and WinPE?
  Yes. In the Hardware Configuration Element class use the variable `Service OS Needed to Run Method (ELGBLSOS)` and in the Operating System class, use the variable `Service OS List (ELGBLSOS)` to define the Service OS. If the Service OS (SOS) for the Hardware Configuration Element and the Operating System do not match, the target device will reboot into the appropriate SOS as needed. The same applies if you are deploying a sequence of Hardware Configuration Elements, some of which need to use the Linux SOS and some of which need to use the WinPE SOS.
- Can you use varying versions of the OS Manager Server modules?
  Mixing and matching OS Manager Server modules is not supported unless you are directed by HP's Technical Support team to do so.
- Will my data partitions be captured with the system partition during the Image Preparation process?
  Multiple partitions on the source image will cause image deployment failures. Remove all partitions on the source other than the one that you want to capture. It is recommended that the partition contain only 100 MB of free space.
- What should I do if my image was not captured properly?
  Ensure that you prepared your reference machine correctly. See Preparing and Capturing OS Images on page 61 for details.
- Are dynamic disks supported with OS Manager Server?
  Not yet.
- What if I want to kick off a batch file to execute a backup program before sending a new image to a machine?
  Use the exit point (`Novapdc.cmd`). Rename your batch file (which contains the backup program) to `Novapdc.cmd` and store it on the target device in *`SystemDrive`*`:\Program Files\Hewlett-Packard\CM\Agent`. This will run before the new OS is deployed.

  Use novapdr.cmd to restore your data. For more information see Addressing Requirements for Capturing, Recovering, and Migrating Data on page 201.

- What is the best way to size down a partition on a source machine?
  Use the option in the Image Preparation Wizard. If you do not use this you can use Partition Magic or another vendor's non-destructive partitioning. You can also Fdisk the partition to the correct size prior to installation of OS.
- What protocol is used to download the Service OS in a PXE-based implementation?
  The Service OS is served by the TFTP server using TFTP protocol.
- What protocol is used to download an OS image?
  HTTP.
- What must be enabled in a router to allow PXE to traverse subnets?
  The DHCP helper, which allows traversal of broadcast traffic on the DHCP ports, since broadcast is typically turned off on routers.
- What are the conditions in which the OS Manager System Agent will be booted on a machine?
  Whenever the target device must be re-imaged, it will boot into the appropriate SOS (Linux or WinPE) and the OS Manager System Agent continues the process. If the target device is already in its desired state, the device will not boot into an SOS.
- Why is my TFTP server shutting down after starting?
  You may have another TFTP server running on the same computer.
- How can I check that the Boot Server is successfully installed?
  Press **Ctrl** + **Alt** + **Delete**, go to Task Manager, and review the list of Processes. `PXE.exe` and `Inetd.exe` should be running.

  or

  Go to the Event Viewer and check the application events. You will see when the process starts. Entries for problems will appear soon after the event starts.

  or

  In Windows 2003, go to a command prompt and type **`netstat /all`**. If you find `boot.ps` and `tftp`, the installation was successful.
- How do I know if the appropriate port is listening?
  From the command prompt `netstat -a`,
  you will receive a list of the ports and an indication of whether they are listening.
- What do I do if I receive a message that says “Checking Machine Status Times Out” or “Cannot find ROMS infrastructure?”
  You may receive this message if you are blocking ports or using a

firewall. Be aware that you must be using both UDP and TCP. Verify that your ports are open, in particular ports 3469, 3471 and 2074. Go to the .cfg for each HPCA IS product that you are running and find the value for the port. After you know which port is not working, you can check your firewall to make sure it is not blocking the specified port.

- What do I do if I receive a message similar to the following during image deployment:

```
20061127 13:37:18 Info: *** Installing Standard Image

20061127 13:37:18 Error: InstallNvdm: An error occurred
retrieving Current Partition information, err:

sfdisk: ERROR: sector 0 does not have an msdos signature

20061127 13:37:18 Info: Partitioning Hard Disk 20061127
13:37:18 Info: rpsadr: CASSERVER:3467

20061127 13:37:18 Info: rpshost: CASSERVER

20061127 13:37:18 Info: rpsport: 3467

20061127 13:37:18 Error: GetState Error: couldn't open socket:
host is unreachable

20061127 13:37:18 Error: Please check the Server configuration

20061127 13:37:18 Error: InstallNvdm: Error getting partition
information

20061127 13:37:18 Info:

20061127 13:37:18 Info: > sending AppEvent to
http://CASSERVER:3461/proc/appeventxml

20061127 13:37:18 Info:

20061127 13:37:18 Error: Error sending AppEvent: couldn't open
socket: host is unreachable

20061127 13:37:18 Error: InstallOSerr: Error(s) occurred
during OS install, stopping

20061127 13:37:18 Error: This machine is in the process of
having an OS installed. However, a critical aspect of the
installation has failed. The machine will shut down until an
administrator fixes the problem and performs a Wake On LAN.
Please contact your adminstrator.

20061127 13:37:18 Info: *** Start of Update Machine
=======================*** Start of Update Machine
=======================
```

Check the configuration of your DNS server. Depending on the configuration, you may experience difficulties working with the short name and may need to use the IP address or fully qualified name.

## Using the Discover Boot Server Utility

Use the following command to send out a DHCP discover request in order to identify the PXE servers that are in the environment. This is an essential command when trying to determine if a machine is able to access the PXE server.

```
./discoverbootserver.sh
```

Note that the results may be complicated to read. Contact Technical Support for more information.

# A AppEvents

The following AppEvents are stored in the Events section in the ROM object.

**Table 18 AppEvents**

| Message | Description |
|---|---|
| CD install, no CD drive | A CD-based installation was requested but no CD-ROM drive exists on the machine. |
| Partition error | The OS Manager System Agent was unable to retrieve partition information (file retrieval problem). |
| Boot partition problem | The OS Manager System Agent was unable to determine the boot partition after the disk was partitioned. |
| Error Installing MBR | The OS Manager System Agent encountered an error while installing the Master Boot Record (MBR). |
| Error installing image | The OS Manager System Agent received an error while installing the OS image. |
| unattend.txt error | The `unattend.txt` file could not be retrieved from the server. |
| Sysprep.inf error | The `sysprep.inf` file could not be retrieved from the server. |
| OS install Successful | OS was successfully installed. |
| NOOP install Successful | No OS install was required. Hardware Configuration Elements may have been processed and the OS Manager may have been updated to indicate that the machine is in desired state with respect to the OS currently installed OS. |

| Message | Description |
|---|---|
| HW config element apply failed | The application of a HW Configuration Element failed. Errors or warnings may be available in the log file. |
| Shadow HW config element apply failed | The application of a Shadow Hardware Configuration Element failed. You can find errors or warnings in osselect.log. |
| Admin activity required - Invalidate OS state | A Hardware Configuration Element failed or the installation of the OS failed. The OS state will be set to INVALID due to the failure. |
| Admin activity required - Multiple HW configurations resolved and central control | More than one HW Configuration was determined by policy. The target device could not determine which of these HW Configurations to use to reach desired state. The administrator or user must select the HW Configuration that needs to be applied to reach desired state. |
| Admin activity required - no eligible OS, unusable machine, machine shutdown | During policy resolution, no eligible OS was found for the device. The device may have no local OS or the device may be managed but the OS must be repaired (_INCONSISTENT_OS).<br>The device is unusable and the OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the machine. |
| Admin activity required - Multiple OSs resolved and central control | Multiple OSs were resolved for this device and administrative action is required because the user was not given the option to select the OS. |
| Admin activity required - Multiple OSs resolved and central control | During policy resolution, several eligible OSs were found for the device. However, the behavior setting does not allow for user selection of the OS. Therefore, the administrator must intervene and determine what OS should be installed on the device. Until then, the device is usable as long as the OSSTATE is not set to INVALID. |

| Message | Description |
|---|---|
| Admin activity required - No OS has been selected | During policy resolution, no eligible OS was found for the device. The device may have no local OS or the device may be managed but the OS is in need of repair (_INCONSISTENT_OS).<br>The device is unusable and the OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the machine. |
| Admin activity required - OSSTATE set to _INCONSISTENT_ | On a managed device that was in its desired state, `Rombl.cfg` was lost. This may indicate serious corruption and therefore, the OS Manager changed the value of OS State to _INCONSISTENT_ and will allow the device to be used “as is”.<br>If possible, during the next HPCA OS Connect, `Rombl.cfg` will be recreated. If this does not happen, the administrator should force a reinstall of the OS. |
| Admin activity required - _UNMANAGED_OS_ is resolved through general policy criteria | An _UNMANAGED_OS_ was resolved for the device and administrative action is required. |
| Admin activity required - Corrupted OS, unusable, shutdown | The client’s OS is corrupt and we do not have enough information or the permission to overwrite the broken installation. |
| %1$s %2$s has been selected | %1 = "OS" or "Hardware Configuration"<br>%2 = The name of the OS or LDS<br>Indicates what has been selected based on policy. |
| %1$s %2$s already installed | %1 = "OS"<br>%2 = "OS name"<br>The OS referenced has previously been installed. |

| Message | Description |
|---|---|
| %1$s %2$s was installed | %1 = "OS"<br>%2 = "OS name"<br>The OS referenced was installed successfully. |
| No to install | A valid OS exists on the device and the user responded No to the prompt to perform an OS installation. |
| No was entered to Install acknowledgement | The user declined to reinstall an OS that policy dictated should be reinstalled. |
| Installing [%1$s] on [%2$s], OS type: [%3$s] | %1 = "OS name"<br>%2 = "partition or disk ID"<br>%3 = "OS type" |
| Partitioning Hard Disk... | The deployment system is in the process of partitioning the hard disk that the OS will be installed to. |
| Please check the RPS configuration | The OS Manager failed to find files on the OS Manager Server or the Proxy Server. The OS Manager will continue with a warning but the deployment may fail because the files are missing. |
| Admin activity required - _UNMANAGED_OS_ is selected where an OS is to be installed | _UNMANAGED_OS was resolved for the device because it has no OS or because the device is managed but the OS must be repaired (_INCONSISTENT_OS).<br>The device is unusable and the OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the device. |
| Admin activity required - No OS has been selected | No OS was selected for this device and administrative action is required.<br>This can occur when multiple OSs resolve and the behaviors are configured for CENTRAL selection. The administrator must arbitrate the OS. |

| Message | Description |
|---|---|
| OSSTATE has been set to _DESIRED_ | The OS has been installed according to policy. |
| OSSTATE set to _DESIRED_ | The OS Manager determined that it was not necessary to install an OS and set the system to desired state.<br>OR<br>The OS Manager determined that a selected OS needed to be installed; it installed successfully and the system was set to desired state. |
| Rebuilt ROMBL.CFG, OSSTATE was _INCONSISTENT_, now _DESIRED_ | The OS Manager detected that the OSSTATE was INCONSISTENT. But, the OS Manager then determined that the system's install is OK and set the system to desired state. |
| Machine under OS management missing machine instance in Client Automation Portal | A managed device does not have a device object; one is created. |
| A machine previously having been in _DESIRED_ state came up with corrupted MBR/boot partition. Admin has to either manually repair this situation or explicitly invalidate it to force re-install according to policy. | A machine has been determined to be in a disaster recovery situation. Some part of the current install was detected to be broken, corrupt or is in another failure state. We have to wait for the Admin to force a re-install or if the local user is allowed to force a re-install. |

# B User Messages

The following messages may be displayed to the user. If the message does not require a response from the user, the message displays for the number of seconds specified in the USERTO attribute in the BEHAVIOR class and then the machine will shut down. If USERTO is set to –1, then the machine will wait for a user response indefinitely.

**Table 19 Messages for Timeouts**

| Messages | User Action |
|---|---|
| This machine is installed with a factory pre-imaged OS that is managed by the Client Automation OS Manager. The Client Automation OS Manager System Agent is unable to connect to the Client Automation OS Manager infrastructure to configure this machine. The machine cannot be used. The system will retry later. | N/A |
| The local machine does not contain a usable OS. Networking problems prevented the Client Automation OS Manager System Agent from connecting to the Client Automation OS Manager infrastructure to install this machine. The machine cannot be used. The system will retry later. | N/A |
| The local machine contains a usable OS. Networking problems prevented the Client Automation OS Manager System Agent from connecting to the Client Automation OS Manager infrastructure to determine policy for this machine. The machine will be booted to the local Operating System. | N/A |
| This machine has an OS installed but is not currently managed by the OS Manager. It contains a local partition but no management marker and no machine object. Select install to install an operating system according to policy or use to keep the existing operating system for now. Please select install or use. | Select **install** to install the resolved OS, or select **use** to continue to use the existing OS. |

| Messages | User Action |
|---|---|
| This machine is new to the OS Manager. The attempt to register this machine in the device information repository failed and it is not allowed be used. The system will retry later. | N/A |
| Please select one of the following roles which will be used, along with other policy criteria, to determine the correct configuration for this machine. | Select a role. |
| This machine has no local OS or the OS is invalid. An OS must be reinstalled. Policy indicates that there are no eligible OSs assigned to this machine. The administrator should verify that at least one of the OSs selected for this machine have the following characteristics:<br>ACPI: $::acpi<br>APIC: $::apic<br>Minimum CPU speed: $::cpuspeed<br>Minimum RAM size: $::mem<br>Boot Hard Drive Type: $::boottype<br>Minimum Hard Drive Size: $::hdsize<br>The machine cannot be used and will shut down until an administrator specifies policy and performs a Wake On LAN. | N/A |
| The current state of this machine is unusable. Policy returned multiple OSs for this machine. The machine will shut down until an administrator selects an eligible OS and performs a Wake On LAN. | N/A |
| The current state of this machine is unusable. Policy returned multiple Hardware Configurations for this machine. The machine will shut down until an administrator selects an eligible Hardware Configuration and performs a Wake On LAN. | N/A |
| Policy requires that the OS must be reinstalled on this machine. Select an OS from the following list: | Select an OS. |
| Policy requires that the Hardware Configuration must be reinstalled on this machine. Select a Hardware Configuration from the following list: | Select a Hardware Configuration. |

| Messages | User Action |
|---|---|
| This machine has no local OS or the OS is invalid. It must be reinstalled. However, no eligible OSs have been returned for this machine. The machine cannot be used and will shut down until an administrator changes policy and performs a Wake On LAN. | N/A |
| This machine has no local OS or the OS is invalid. It must be reinstalled. However, the intended OS for this machine cannot be determined due to an error during resolution. The machine cannot be used and will shut down until an administrator changes policy and performs a Wake On LAN. | N/A |
| Policy requires that the OS for this machine must be reinstalled. Is it ok to install the new OS now? | Indicate whether it is okay to continue the installation. |
| Policy requires that the OS for this machine should be reinstalled. The selected OS is the same as the currently installed OS. Do you want to use the current installation or do you want to refresh the OS? | Specify whether to use the existing installation or to refresh the current OS. |
| This machine is in the process of having its Hardware Configuration modified. However, a critical element of the configuration has failed. The machine will shut down until an administrator fixes the problem and performs a Wake On LAN. Please contact your administrator. | N/A |
| This machine is in the process of having an OS installed. However, a critical aspect of the installation has failed. The machine will shut down until an administrator fixes the problem and performs a Wake On LAN. Please contact your administrator. | N/A |
| This machine is in the process of having its Hardware Configuration modified. However, a critical Hardware Configuration Element has failed due to incorrect or corrupt instructions. The machine will shut down until an administrator fixes the problem and performs a Wake On LAN. Please contact your administrator. | N/A |

# C Storing Multiple Logs

Typically, after an OS is installed, the logs stored on the OS Manager Server are rewritten each time. Now, you have the option to store multiple logs per machine on the OS Manager Server.

### To store multiple logs on the OS Manager Server

1. Use a text editor to open `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\put.cfg`.

```
# ------------------------------------------------------------------------
# - RIS Put Server - for file uploads
#
#   Put::cfg array is used by the PutEnter proc to allow a user-specified
#   number of previous files with the identical name to be saved.
#       -ROLLOVER is the max number of files to keep, each file has the
#           same root name with the suffix of .1, .2, etc.
#       -TYPELIST may include any number file extensions: e.g., ".log .txt .edm"
#   The default of -ROLLOVER is 0 (zero) and only the current version is stored.
# ------------------------------------------------------------------------

file mkdir [set dir $Config(ROOT)/upload]

Put_AddRoot /upload $dir

namespace eval Put {
    array set cfg [list \
        -ROLLOVER   0   \
        -TYPELIST   ".log"
    ]
}
```

2. Set -ROLLOVER to the number of logs that you want to be able to store. For example, if you set –ROLLOVER to 3, you will be able to store and review the previous three actions performed on the target device.

# Index

## D

## E



## F



## G



## H

## I



## J



## K



## L

## M

## N



## O

## P

## R

## S

## T



## U



## V

## W