HP Client Automation

OS Manager

for the Windows® operating system

Software Version: 7.90

System Administrator Guide

Manufacturing Part Number: None
Document Release Date: May 2010
Software Release Date: May 2010

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

Trademark Notices

Documentation Updates

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

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

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

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

This site requires that you register for an HP Passport and 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.

The following table indicates changes made to this document since the last released edition.

Chapter	Version	Changes
All	7.20	General edits and rebranding. Removed version number for WinPE. Added cautions regarding Core and Satellite environments.
Chapter 5 Chapter 6 Chapter 7 Chapter 11 Appendix D Appendix E Appendix F	7.90	Updated and reorganized document to reflect usability improvements to the image capture and deployment process.
Chapter 1	7.20	Added information about the HP Client Automation Mini Management Server.

Chapter	Version	Changes
Chapter 1	7.20	Changed the note under Machine 2 in Image Deployment Infrastructure on page 25.
Chapter 1	7.20	Updated version number in Product Media on page 34.
Chapter 1	7.50	Added Support for SSL on page 24.
Chapter 2	7.20	Added information about thin clients in Target Devices on page 39.
Chapter 2	7.20	Removed list of operating systems in Server on page 38.
Chapter 2	7.20	Added topic "Firewall Settings for Windows XPe Thin Client Devices."
Chapter 2	7.50	Removed topic "Firewall Settings for Windows XPe Thin Client Devices."
Chapter 2	7.50	Added Symantec Endpoint Protection Agent Settings for Windows XPE and WES on page 42.
Chapter 2	7.50	Removed topic "Installing the Application Manager on Thin Client."
Chapter 2	7.80	Added requirement that a virtual target machine must have the same virtual hardware configuration as the virtual reference machine for Windows XP and Windows 2003.
Chapter 3	7.20	Updated the Prerequisites on page 46.
Chapter 3	7.20	Updated name of log in the note on page 49.
Chapter 3	7.20	Added Installing the Client Automation Mini Management Server on page 58.
Chapter 3	7.50	Added topic IP Networking Support on page 46.
Chapter 3	7.50	In Installing the OS Manager Server on page 48, added a caution and modified the instructions slightly.
Chapter 3	7.50	In About the Boot Server on page 53, added a caution.

Chapter	Version	Changes
Chapter 3	7.50	Added Enabling SSL Communication on page 52.
Chapter 3	7.50	In Configuring the Portal on page 55, removed information about updating modules, adding directory services and modified the instructions for Configuring the Default Behaviors Instance to use the CSDB Editor.
Chapter 3	7.50	Removed the section about the Admin Publisher.
Chapter 4	7.50	Added Chapter 4, Disk Encryption.
Chapter 5	7.20	Updated Deployment Methods on page 70.
Chapter 5	7.20	In Capture Pre-Windows Vista for Legacy Deployment on page 63, modified the note in Task 2.
Chapter 5	7.20	In Capture Pre-Windows Vista for ImageX Deployment on page 65, modified the note in Task 2.
Chapter 5	7.20	Added a task to copy the utilities to the HPCA OS Manager Server to Capture Windows Vista or Windows Server 2008 for ImageX Deployment on page 67 and Capture Windows Vista or Windows Server 2008 for Windows Setup Deployment on page 79.
Chapter 5	7.20	Updated To use the Image Preparation Wizard on page 82.
Chapter 5	7.20	Added Preparing and Capturing Thin Client OS Images on page 80.
Chapter 5	7.50	Added note on related to capturing images when using supported disk encryption products.
Chapter 5	7.50	In About the OS Image Capture Tool on page 72, added information about exit points for the Image Preparation Wizard.
Chapter 5	7.50	Added Using the Image Preparation Wizard Exit Points on page 87.
Chapter 5	7.50	Added Preparing To Capture Remote Images on page 88.

Chapter	Version	Changes
Chapter 5	7.50	Updated note and changed it to a caution on page 90.
Chapter 5	7.50	Added information about the Select Image Preparation Wizard Payload window on page 92.
Chapter 5	7.50	Added Using the Image Preparation Wizard in Unattended Mode on page 96.
Chapter 5	7.50	Updated the Install the HPCA Agent on the Embedded Linux thin client on page 89.
Chapter 5	7.80	Added support for Windows 7 and Windows Server 2008 Release 2 (R2) x64.
Chapter 6	7.20 August 7, 2008	In Publishing Operating System Images, modified step pertaining to the Select window.
Chapter 6	7.20	In Publishing Operating System Images, modified step pertaining to the Deployment Method drop-down menu.
Chapter 6	7.20 August 7, 2008	In Publishing Operating System Images, modified step pertaining to the Configure window.
Chapter 6	7.50	Updated information about spanned images in Prerequisites for Publishing .WIM images on page 101.
Chapter 6	7.50	Added topic Publishing OS Add-Ons and Extra Production OS (POS) Drivers on page 107.
Chapter 6	7.80	Added support for Windows 7 and Windows Server 2008 Release 2 (R2) x64.
Chapter 7	7.20	Added a note about thin client limitations on page 114.
Chapter 7	7.50	Updated table Expected Results on Target Device on page 114 with encryption information.

Chapter	Version	Changes
Chapter 7	7.50	Renamed chapter from "Operational Overview" to "Preparing Content." Removed instructions on using the OS Manager Admin Module and replaced with instructions about how to use the CSDB Editor to perform tasks. Several topics were removed.
Chapter 7	7.50	Removed EVNTDEST and USERTO from Attributes of the Behavior Class on page 128.
Chapter 7	7.50	In DRIVEMAP Type Attribute on page 135, added information about the new partition type, Preserve.
Chapter 8	7.20	Updated graphics.
Chapter 9	7.50	Removed chapter OS Manager Support for HP Blades.
Chapter 9	7.50	Chapter 9 is now Multicast and the OS Manager and all chapter numbers below have changed.
Chapter 9	7.50	Removed information indicating that multicast does not support spanned images and that images must be a maximum of 4 GB.
Chapter 9	7.50	Updated `Minref` on page 166.
Chapter 10	7.50	Updated first paragraph and added a note in Restoring Operating Systems on page 194.
Chapter 11	7.80	Added new chapter about Customizing OS Deployment by Using Exit Points and Add-Ons on page 203.
Chapter F	7.50	Updated Building a Custom Windows PE Service OS on page 303.
Chapter F	7.20	Building a Custom Windows PE Service OS on page 303 no longer has separate instructions for earlier versions.
Chapter 12	7.80	Added new chapter about Personality Backup and Restore on page 213.
Chapter 13	7.50	In Setting the System Language Parameter on page 234, updated instructions to use the CSDB Editor

Chapter	Version	Changes
Chapter 13	7.80	In Setting the System Language Parameter on page 234, updated procedure for setting the **Language used for Service OS** attribute (formerly the LANG parameter). The name of this chapter was changed to reflect the broader focus.
Chapter 14	7.20	Updated Troubleshooting on page 237.
Appendix A	7.20	Updated AppEvents table on page 251.
Appendix B	7.50	Updated introduction to User Messages on page 257.

Support

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 support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Contents

1 Introduction

This chapter includes the following topics:

Abbreviations and Variables

Abbreviations Used in this Guide

Abbreviation	Definition
HPCA	HP Client Automation
Core and Satellite	HPCA Enterprise environment consisting of one Core server and zero or more Satellite servers. All features are installed as part of the Core or Satellite server installation.
Classic	Traditional HPCA Enterprise environment installed from individual server components (not Core and Satellite)
CSDB	Configuration Server Database
Portal	HPCA Portal, formerly known as the Management Portal

Variables Used in this Guide

Variable	Description	Default Value

`InstallDir`	Location where the OS Manager server is installed	Core and Satellite installation:
		`C:\Program Files\Hewlett-Packard\HPCA`
		Classic HPCA Enterprise installation:
		`C:\Program Files\Hewlett-Packard\CM`

`SystemDrive`	Drive label for the drive where the OS Manager server is installed	`C:`

This guide assumes that you have an HPCA Core and Satellite installation.

If you have an HPCA Classic (traditional component-based) installation where the OS Manager is installed separately, the paths to various files and folders used by the OS Manager will be different.

Overview

Use the HP Client Automation(HPCA) OS Manager to configure and deploy operating systems. 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.

You must be very familiar with the Client Automation product suite as many of these products are used to create, prepare and deploy images.

Any time that you are prompted for the OS Manager Server's IP address and port number, you must now specify the port number (by default 3466).

This does not apply to HPCA Classic environments, where the OS Manager port is 3469 by default.

This guide provides an introduction to OS management terminology, requirements and installation instructions, information on capturing, preparing and publishing images. Once you have operating system images, you can use the Enterprise Manager to deploy them to target devices.

If you are a more advanced user, you may want to review additional sections in this guide, including how to prepare content, gain a better understanding of booting from the network versus booting locally, and many other features supported by the OS Manager.

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

Be sure to first read the *HPCA Core and Satellite Getting Started and Concepts Guide* for information about installing and configuring HPCA.

Support for SSL

OS Manager uses SSL when the Core and Satellite environment is configured for SSL.

Product Architecture

The 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 Tools

HP provides two tools with which to capture the image of your operating system and a third tool to publish the captured image to the Configuration Server database (CSDB).

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
InstallDir\Data\OSManagerServer\upload

Then, use the HPCA Administrator Publisher to promote the image to the Configuration Server DB.

HP Client Automation Windows Native Install Packager

Use the HPCA 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 following directory:

InstallDir\Data\OSManagerServer\upload

Then, use the HPCA Administrator 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 67 for additional information.

When you have an image file, use the HPCA Administrator Publisher to store the image in the Configuration Server database (CSDB).

HP Client Automation Administrator Publisher

Use the HPCA Administrator Publisher to store the image and its associated files in the CSDB. 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 CSDB.

See Publishing on page 97 for additional information.

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

Image Deployment Infrastructure

The image deployment infrastructure consists of a set of servers designed to manage and deploy operating systems to target devices based on a set of criteria.

- DHCP Server

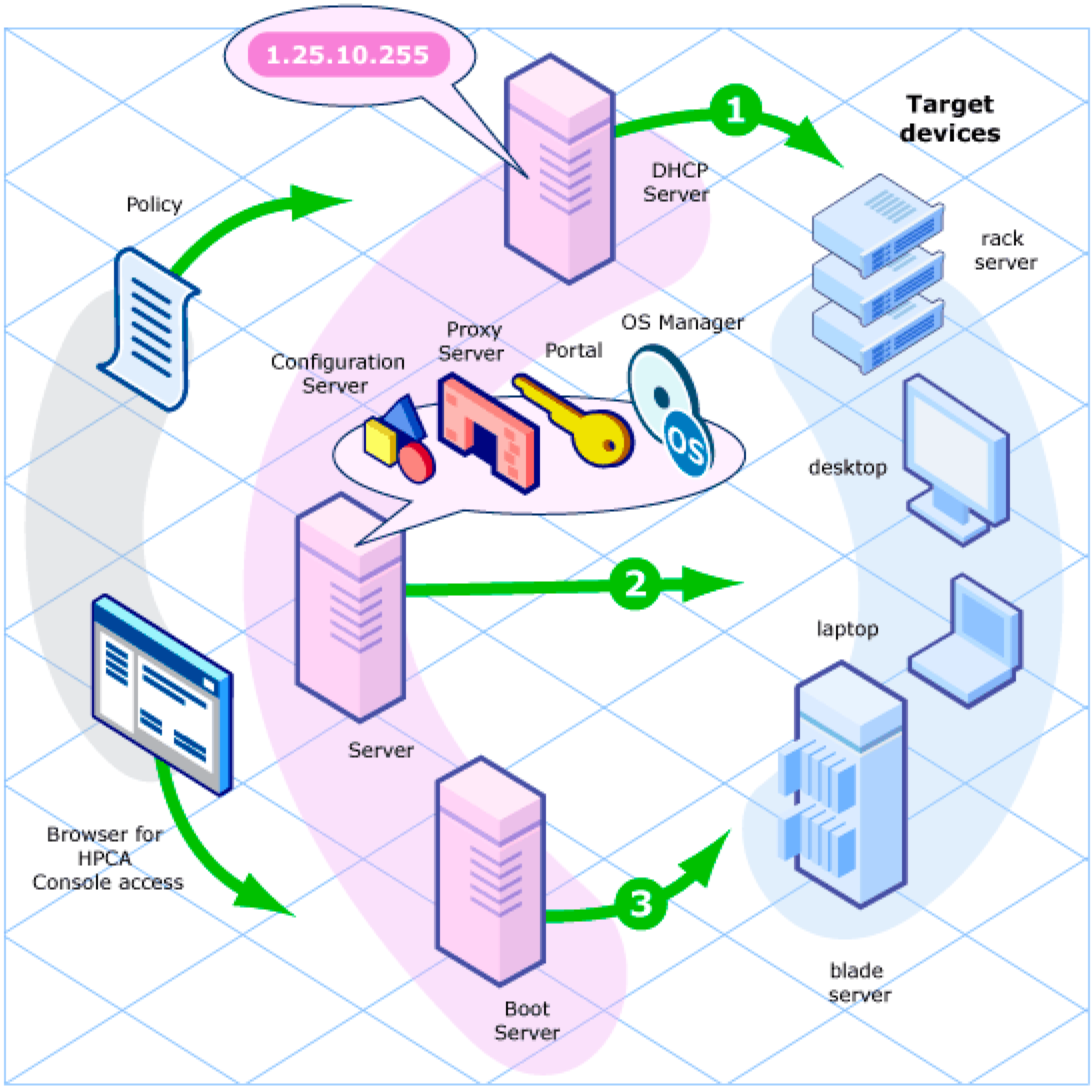
  The target device uses a DHCP server to obtain an IP address. You can easily implement OS Manager in an existing DHCP-enabled network. There is no need to install additional DHCP servers.

- OS Manager Server
- HP Client Automation Configuration Server
- HP Client Automation Proxy Server
- HP Client Automation Portal
- HP Client Automation Enterprise Manager
- HP Client Automation Administrator, which includes the Configuration Server Database Editor and the Publisher.
- Boot Server (PXE/TFTP servers)

Figure 1 on page 27 illustrates the deployment architecture.

See Installing and Configuring the Server on page 45 for more information.

Figure 1 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 67.

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 (CSDB). See Publishing on page 97.

5 Use the Enterprise Manager (the HPCA console in a Core and Satellite installation) to assign operating systems to target devices.

  Alternatively, you can use the CSDB Editor to create, modify, and prepare content for use in production deployments. This is an advanced scenario and should only be used by experienced HPCA administrators.

6 Use the Enterprise Manager (the HPCA console in a Core and Satellite installation) to deploy images to target devices and review the state of your OS deployment.

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.

- **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.
- **HPCA Console** is the web interface console used to manage devices, software, operating systems and patches as well as create and view reports and dashboards based on those managed devices.
- **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

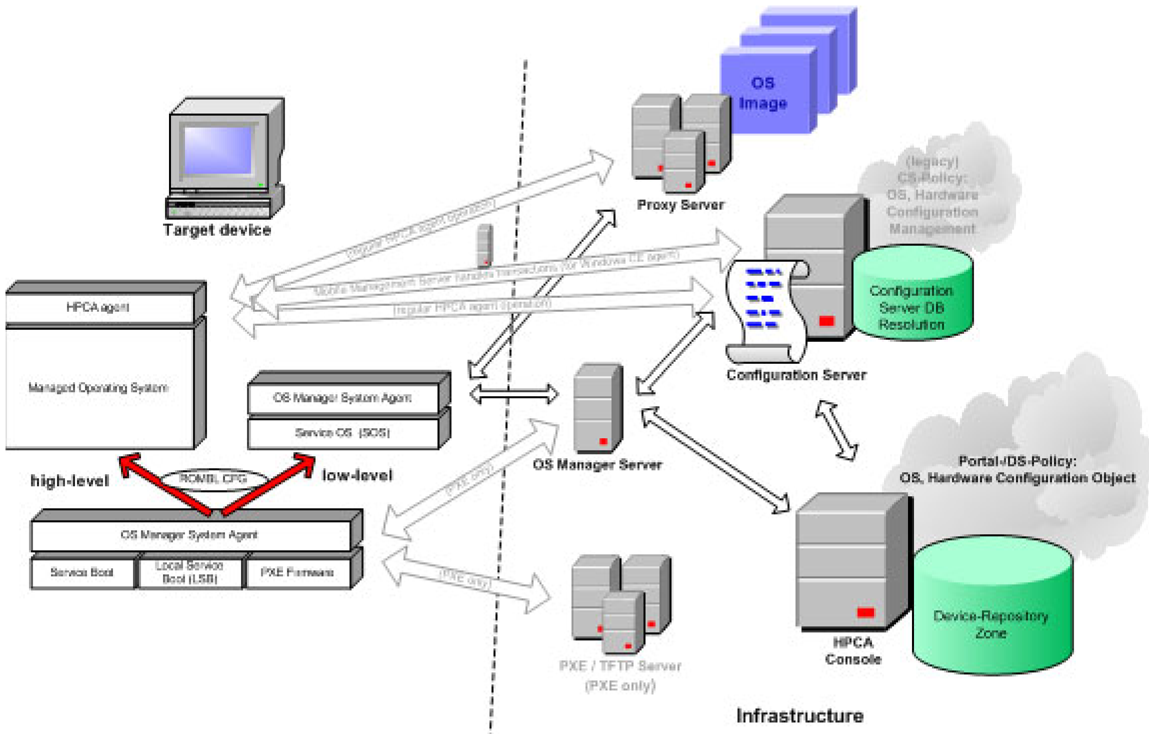
device's system drive or it can continue the boot procedure by loading the HP Client Automation OS Manager System Agent from the Boot Server's TFTP server.

- **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. It 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.
- **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*.
- **HP Configuration Server Database Editor** (CSDB Editor) is a tool that enables you to view and manipulate the contents of the Configuration Server Database. For the OS Manager, this tool is used to create, modify and prepare content for use in production environments. See the *HP Configuration Management Administrator User Guide* for more information.
- **ImageDeploy.ISO** is used to initiate 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.

- **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.

The following figure illustrates the OS Manager components.

Figure 2   OS Manager Components



Terminology

This section provides a description of generic and HPCA-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 connect

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 objectt

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 a device in the HPCA device repository—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 of the following:

- A target device has been discovered by the OS Manager, but policy has not been assigned to this device.
- Policy has been assigned to a target device, but you are not yet ready to overwrite the existing OS on that device.

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

Product Media

In order to install the product, you must use the OS Manager 7.80 media. Before you begin, you may want to create two additional CD/DVDs:

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

Related Documents

HP Client Automation OS Manager Hardware Configuration Management System Administrator Guide

HP Client Automatiion Enterprise Manager User Guide

HP Client Automatiion Administrator User Guide

2 System Requirements

This chapter includes the following topics:

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.
- 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.
- 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 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 deployments 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, or a Linux-based OS installed. Also see Symantec Endpoint Protection Agent Settings for Windows XPE and WES on page 42.
- If you are using VMware as the target device, change your target device's `.vmx` file to contain the following:

  `ethernet0.virtualDev="e1000"`

- If both reference and target devices are virtual machines, and if you are capturing and deploying legacy images of Windows XP and/or Windows 2003, make sure that the virtual hardware of the target virtual machine matches that of the reference virtual machine. Failure to do so may result in a Stop Error (BSOD, blue screen of death) during the installation and/or specialization phase of the Windows deployment.
- 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.
- Target devices can have one CPU or multiple CPUs. The 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.

    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.

  - — Target devices must 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.
- Target devices must match the reference device's ACPI characteristics (that is, ACPI vs. non-ACPI, which is represented in the HAL) and boot drive interface.
- Target devices must be compatible with the programmable interrupt controller capabilities that are represented in the HAL that is captured on the reference machine.

  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.
- Target devices must support NTFS and FAT32 file systems.

- Target devices must have compatible drivers based on the Deployment method being used in the Service OS. If you are using WinPE and the drivers are not available, see Adding Drivers to the Windows PE Service OS on page 308. If you are using a Linux SOS, HP will provide periodic updates of the Linux SOS.

Symantec Endpoint Protection Agent Settings for Windows XPE and WES

Windows XP Embedded (XPE) and Windows Embedded Standard (WES) thin client devices ship with the Symantec Endpoint Protection Agent pre-installed. Two separate rules, one for the HPCA executables and one for the ports, must be created to allow HPCA to operate.

To create the HPCA executables rule

1. Log on to the Windows XPE or WES device as **`Administrator`**.
2. Right-click the Symantec icon in the system tray and select **Advanced Rules**.
3. Click **Add**.
4. On the General tab:
   a. Add description **Allow HPCA Agent**.
   b. Select **Allow this traffic**.
5. On the Applications tab, click **Browse** to add the following applications from *`InstallDir`*`\Agent`.
   — `Nvdkit`
   — `Radconct`
   — `Radpinit`
   — `Radexecd`
   — `Radstgrq`
   — `Radsched`
   — `Radgetproxy`
   — `Radntfyc`
   — `Radidgrp`
   — `Ralf`
6. Click **OK** to save the new rule.
7. Click **OK** to exit.

To create the HPCA Ports rule

1. Right-click the Symantec icon again and select **Advanced Rules**.
2. Click **Add**.
3. On the General tab:
   a. Add description **Allow HPCA Ports**.
   b. Select **Allow this traffic**.
4. On the Ports and Protocols tab, select Protocol: **TCP** and add Local: **3463** and **3465**.
5. Click **OK** to save the new rule.
6. Click **OK** to exit.

When you have created both rules, right-click the **Enhanced Write Filter (EWF)** icon in the system tray, and select **Commit**. You are prompted to reboot. This will write your changes to the flash memory.

After reboot, confirm that both rules are available in the Symantec Endpoint Protection utility and that they are enabled (**Allow this traffic** is selected for both).

Additional Configuration for Windows Thin Client OS Images

The following information pertains to these thin client operating systems:

- Windows XP Embedded (XPE)
- Windows Embedded Standard (WES)
- Windows Embedded Compact (Windows CE)

If you will be capturing any of these OS images, you will also need to allow access to the Image Preparation Wizard executable (`prepwiz.exe`). Note that `prepwiz.exe` is only available from the HPCA Image Capture CD (which is created from the Image Capture ISO on the HPCA media).

Insert the HPCA Image Capture CD, and modify the HPCA Agent rule that you created above to include `prepwiz.exe`. The file is located here:

CD Drive:`\image_preparation_wizard\win32\prepwiz.exe`

Memory Considerations for Windows CE Captures

When you deploy an OS to a Windows CE device using Local Service Boot (LSB), there must be sufficient space available on the device to install and extract the LSB service. If the device reboots but fails to boot the Linux Service OS (SOS), the amount of “storage memory” allocated on the device may be insufficient—at least 10 MByte is required.

Follow these steps on the Windows CE device:

1. Click **Start**.
2. Select **Settings** > **Control Panel**.
3. Click the **System** icon.
4. Select the **Memory** tab.
5. Use the slider on the left to increase the **Storage Memory** to 10 MByte or more.

3 Installing and Configuring the Server

This chapter includes the following topics:

This chapter describes how to install and configure the 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 and Concepts Guide*, as the installation, configuration, and troubleshooting information in that guide may override the information in this guide.

IP Networking Support

HPCA supports Internet Protocal version 6 (**IPv6**)—the latest version of the internet protocol addressing structure—in its Windows-based Core and Satellite servers. The Core and Satellite servers can now use either IPv4 or IPv6 for server-to-server communication. HPCA agent communications, however, are currently limited to IPv4. For details, refer to the “IPv6 Networking Support” appendix in the *HPCA Core and Satellite Enterprise Edition User Guide*.

HP Client Automation “classic” environments that use the traditional, component-based, HPCA server installations will continue to support IPv4 only.

Prerequisites

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

- HP Client Automation Configuration Server, version 7.80 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 (CSDB), version 7.80 or higher.

  To check the version of your CSDB, 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 7.80 or higher.
- HP Client Automation Proxy Server, version 7.80 or higher.
- HP Client Automation Portal, version 7.80 or higher.
- HP Enterprise Manager, version 7.80 or higher
- Microsoft Internet Explorer with the security level set no higher than Medium.

Installation Checklist

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

1. Install and configure the OS Manager Server.
2. Install the Boot Server.
3. Configure the Portal.
4. Configure the Proxy Server.
5. *Optional*: Install the Mini Management Server.
6. *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 the 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.

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 section.

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 located in `*InstallDir*\OSManagerServer\modules`.

> To check that your license string is valid, open the following file:
>
> *InstallDir*\OSManagerServer\logs\httpd-osm-port.log
>
> Search for "License is expired". If you find this string, you must update your license file. See OS Manager Server Logs on page 238 for information about this log.

6 Click **Next**.

7 Type the User ID and Password for the Portal. The default User ID is `romadmin` and the default Password is `secret`. This information is encrypted and stored in the following file.

InstallDir\OSManagerServer\etc\roms.cfg

If you want to change the User ID (PORTAL_UID) and Password (PORTAL_PASS), you must change these values in `roms.cfg`.

See Enabling Communication between the OS Manager and the Configuration Server on page 51 for encryption information.

8 If necessary, type the port for the OS Manager Server and click **Next**.

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

10 Click **Next**.

11 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.

12 Click **Next**.

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

14 Click **Next**.

15 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.

16 Click **Next**.

17 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 is stored in the Portal and can be viewed under a device in the Enterprise Manager.

> 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.

18 Click **Next**.

The Summary window opens.

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

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

> If you are installing the OS Manager Server on Microsoft Windows Server 2003, when you open the Enterprise Manager 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.

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

a Copy `bootsect.exe` from this directory:

`C:\Program Files\Windows AIK\Tools\PETools\x86\`

to this directory:

InstallDir`\OSManagerServer\OSM\SOS\winpe\utilities\Program Files`

b Copy `imagex.exe` from this directory:

`C:\Program Files\Windows AIK\Tools\x86`

to this directory:

InstallDir`\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 or Windows 7 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 (*InstallDir*`\OSManagerServer`).

3 Type **nvdkit** and press **ENTER**.

4 Type the following command:

password encrypt *yourPassword* **aes**

Here, *yourPassword* represents your existing password for the 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 *InstallDir*\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.

Enabling SSL Communication

The OS Manager can be used as an SSL client when communicating with the Configuration Server and Portal. See the *HP Client Automation SSL Implementation Guide* for information about configuring the Configuration Server and Portal.

> These steps apply only when using OS Manager in a Classic HPCA environment. If you are using OS Manager in a Core and Satellite environment, SSL should be configured using the Core console. Refer to the *HPCA Core and Satellite User Guide* for details.

To enable SSL communications between the OS Manager and the Configuration Server/Portal:

1 In *InstallDir*\OSManagerServer\etc\roms.cfg change:

```
PORTAL_USE_SSL   0
RCS_USE_SSL      0
```

to

```
PORTAL_USE_SSL   1
RCS_USE_SSL      1
```

2 Also in *InstallDir*\OSManagerServer\etc\roms.cfg, change the port in the RCS_ADDRESS and the RIBPORT to match the SSL port being used.

3 In the Configuration Server's bin directory, open the edmprof.dat file, and add the following line in the [MGR_ROM] section:

```
PORTAL_USE_SSL   1
```

About the Boot Server

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 section.

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 servers 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.
- 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 250.

- 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 a 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 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 `*InstallDir*\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`.

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 127.

To configure the default Behaviors instance

1 Log on to the CSDB Editor.

See Logging On on page 124 for more information.

2 Go to PRIMARY.OS.BEHAVIOR.DEFAULT_BEHAVIOR.

3 In the RUNPARAM (RunOnce Parameter String) change IP=RCSSERVER to reference the appropriate Configuration Server for your environment.

   If your Configuration Server is running on a non-default port, also add the following string immediately after the server name:

   `,port=`*`<Configuration Server port number>`*

   The default port for Configuration Server is 3464.

4 Click **OK**.

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 *`InstallDir`*`\IntegrationServer\etc`.

1 Stop the HPCA Integration Server service.

2 Open *`InstallDir`*`\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`.

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
```

5 Save the file.

6 Restart the HPCA Integration Server service.

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`

2 Double-click `setup.exe`.

The Client Automation Mini Management Server Install window opens.

3 Click **Next**.

The End User License Agreement window opens.

4 Click **Accept**.

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

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

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

8 Click **Install**.

9 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 7.50 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 Opening the Boot Server's default file. This is typically located in `InstallDir\BootServer\X86PC\UNDI\boot\linux.cfg`.

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.

2 Modify the settings for PXE:

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

b Save and close the file.

3 Modify the setting for LSB by opening the Client Automation Administrator CSDB Editor and going to PRIMARY, OS, Operating Systems (ZSERVICE), Local Service Boot. In the right pane, scroll to the Service OS List (ELGBLSOS) attribute.

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

b Save, and close the Admin CSDB Editor.

4 Modify your deployment CD-ROM as instructed in Building a Custom Windows PE Service OS on page 303.

4 Disk Encryption

This chapter includes the following topics:

In previous versions of the OS Manager, a partition that could not be read was determined to contain no meaningful data and would trigger automated disaster recovery.

As of version 7.5, the OS Manager can detect when a partition has been encrypted using the following products:

- WinMagic SecureDoc
- PGP Whole Disk Encryption
- Check Point PointSec Full Disk Encryption
- McAfee Safeboot

Encrypted drive support changes some behaviors of the system.

1. Partition data that cannot be read is assumed to be valid if an encryption product is detected.
2. Automated disaster recovery is not possible using the Behavior setting, Disaster Recover y (PMDISRCV on page 130). If you want to perform disaster recovery, you must use the OS Management Wizard with the Emergency Mode option selected in the HPCA Console to reinstall the OS.

   After recovering your operating system you must deploy the encryption product components and initiate the encryption process.

3. For kiosk-type machines booting from a CD/DVD, the CD/DVD must be removed following the deployment to prevent the machine being booted from the CD repeatedly.

Prerequisites

Set the BIOS to boot from the local drive first.

Do not capture an image from an encrypted hard drive.

Encryption Support Mode Parameter (ENCMODE)

By default, the OS Manager will automatically detect the supported encryption products listed above and adjust its behavior to ensure that the system does not perform an unwanted re-installation.

- For network (PXE) boots, the ENCMODE attribute is set to AUTO in the [OS Manager] section of the default file.
- For CD/DVD boots, the ENCMODE attribute is set to AUTO in the [OS Manager] section of `rombl.cfg` which resides in the root of the deployment CD.

You can change how encryption is handled using this ENCMODE parameter.

If ENCMODE is not present, the default value AUTO, is used. To change the value, you may need to add the ENCMODE attribute and the desired value.

The following table describes the values that can be assigned to ENCMODE in the format ENCMODE=*`value`*.

Table 1 ENCMODE Attribute Values

Value	Definition
NONE	Do not support encryption. Use this value to enforce the behavior of the OS Manager 7.2 and below, where a partition that could not be read was determined to contain no meaningful data and treated as an automated disaster recovery situation (depending on the behavior settings).
AUTO (default)	Automatically detect supported encryption products.
ENC	Assume all partitions are encrypted. Use this for unsupported encryption products because the auto detection feature is not used.

➤ It is recommended that you use a Client Automation service (ZSERVICE) to deploy the encryption product components and initiate the encryption process. It is also recommended that you prioritize the service to ensure that the encryption service is installed first to keep the amount of time the system runs unencrypted to a minimum.

Using Microsoft BitLocker

Microsoft BitLocker encryption technology is significantly different than other 3rd-party encryption products supported by the OS Manager. BitLocker is an integral part of Vista and newer Microsoft OS deliverables. It is based on a split partition layout that contains a system partition (typically drive S:) and the operating system partition (drive C:). The system partition is always unencrypted.

When using BitLocker, you must prepare your systems at the partition level so that it is ready to be enabled with BitLocker.

Using the OS Manager's new Reserved Space attribute in the DRIVEMAP class you can install and prepare systems with the assurance that the Microsoft BitLocker enablement and subsequent encryption will succeed. Next, you must enable BitLocker. See Microsoft's documentation for enablement instructions.

For Hardware Configuration Operations triggered by policy changes that are sensed during an OS Connect, the OS Manager will temporarily disable BitLocker. After the Hardware Configuration Operations have been completed, Bitlocker will be re-enabled ensuring that the preboot integrity trust chain has not been compromised.

For Hardware Configuration Operations triggered using the OS Management Wizard with the Emergency Mode option selected in the Enterprise Manager, you (the administrator) must handle any potential trust chain issues. See the *HP Client Automation Enterprise OS Manager Hardware Configuration Management Guide* for more information about the Repair Device task.

Reserved Space – RSVDSPCE in DRIVEMAP class

The Reserved Space attribute (RSVDSPCE) in the DRIVEMAP class must contain a value expressed in MB.

If you specify this value for its intended use, use a value equal to or greater than 1500. This is the size that Microsoft recommends for the BitLocker S: partition.

A value of 0 (default) will cause OS Manager to not leave any gap. Non-fatal warnings will be issued in the OS deployment log when the value is smaller than 1500 and greater than 4000.

When OS Manager partitions the disk it will leave un-partitioned space on the disk equal to the size in MB specified in the RSVDSPCE attribute. This space can then be used later by the BDEHDCFG.EXE to prepare the system for BitLocker. This step is not included and has to be done separately. Consult the Microsoft documentation for how to enable BitLocker on a deployed system.

The RVSDSPCE attribute is not supported on pre-Vista operating systems. Any value specified will be reset to 0 during deployment, a warning will be issued and no space will be reserved.

Local Service Boot and OSM Client Method Updates

The Local Service Boot service and the OS Manager Application Manager agent have both been updated to recognize and support a BitLocker prepared and/or enabled dual partition scheme.

Partitioning Notes (DRIVEMAP class)

In case of a Merge DRIVEMAP scenario in a Bitlocker prepared or encrypted system, the OS Manager service OS agent has been updated to correctly identify both the system and the operating system partition and leave the other partitions intact. When re-creating the OS partition, space will be left unallocated for the system partition. Only the OS partition will be recreated.

The Preserve DRIVEMAP type cannot be used with the BitLocker dual partition scheme.

5 Preparing and Capturing OS Images

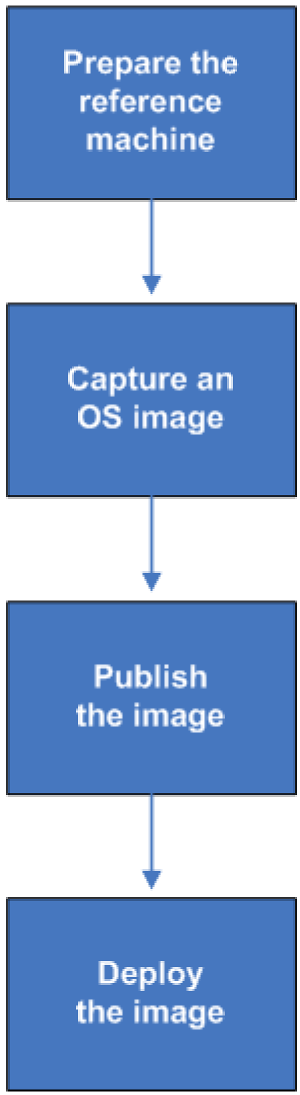
This chapter includes the following topics:

Make sure that the Windows Automated Installation Kit (AIK) is installed on the HPCA Core server *before* you attempt to capture OS images.

Refer to “Using HPCA to Manage Windows Operating Systems” in the *HPCA Core & Satellite Getting Started and Concepts Guide* for more information.

Process Overview

In HPCA, the process of managing operating systems has four steps:



The reference machine is the system that you use to create the “gold” OS image that can be deployed to the managed devices in your environment.

See Preparing the Reference Machine on page 74.

HPCA provides interactive OS image capture tools that enable you to easily capture an OS image on a reference machine.

See Capture the OS Image on page 77.

After you capture an OS image, you must publish it to the HPCA database. HPCA provides an interactive Publisher tool that helps you do this.

See Publishing Operating System Images on page 99.

You can then use the HPCA console to deploy operating system images to groups of managed client devices in your environment.

See Managing Operating Systems on page 208.

The focus of this chapter is preparing and capturing OS images. Publishing and deployment are discussed in the chapters noted above.

Introduction

In this chapter, you will learn how to prepare and capture the following operating system images for deployment to managed client devices in your environment:

- Windows 7
- Windows Server 2008 R2 (x64)
- Windows Vista
- Windows Server 2008

To capture images of older operating systems, see Capturing Windows XP and Windows Server 2003 OS Images on page 277.

In an HPCA Core and Satellite installation, any time that you are prompted for the OS Manager Server's IP address and port number, you must specify the port number (by default 3466).

In an HPCA Classic environment, the port is 3469 by default.

If you are using an existing OS WIM image (this includes the OS `.WIM` files on the Microsoft Windows OS installation media) or have created an OS WIM image using the Microsoft Windows Automated Installation Kit (AIK), you do not need to prepare or capture the image, and you and can skip to the next chapter.

Preparing and Capturing Desktop OS Images

The information in this section pertains to desktop, laptop, notebook, netbook, and workstation client devices. For information about Thin Client devices, see Preparing and Capturing Thin Client OS Images on page 80.

Prerequisites

Before you attempt to capture an OS image using the HPCA OS Image Capture tool, make sure that the Microsoft Windows Automated Installation Kit (AIK) is installed on the HPCA Core server.

- If the Windows AIK was installed *before* the HPCA Core server was installed, no further action is required.
- If the Windows AIK was installed *after* the HPCA Core was installed, you must restart the HPCA Core.

The Windows AIK is available for download from the Microsoft Download Center (`http://www.microsoft.com/downloads`). It is not included as part of a normal Windows installation.

Be sure to install the appropriate version for your operating system, and install it in the default location:

`C:\Program Files\Windows AIK`

Refer to the *HPCA Core and Satellite Getting Started and Concepts Guide* for information.

Make sure that the Microsoft .NET Framework version 2.0 (or later) is installed on the reference machine. The .NET Framework is available at the Microsoft download center:

http://www.microsoft.com/downloads

To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:

`%SYSTEMROOT%/Microsoft.NET/Framework`

Deployment Methods

There are two methods that you can use to deploy an image using the OS Manager:

- Use **ImageX** to capture an image in `.WIM` format that will be deployed using Windows PE and the ImageX utility.
- Use **Windows Setup** to capture an image in `.WIM` format that will be deployed using Windows PE and Windows Setup.

Windows Setup provides greater control over the installation. ImageX is more comparable to a simple file extraction. You can perform unattended installations or upgrades with images captured using either method.

To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GByte image, you will need 50-60 GByte of free disk space.

Table 2 provides a summary of each deployment method. The OS image preparation and capture steps that you perform will vary slightly based on the operating system and deployment method that you choose.

Table 2 Deployment Methods

Method	Service OS Type*	Resulting Files**	Supported Platforms
Microsoft ImageX	WinPE	`ImageName.WIM` `ImageName.EDM`	Windows XP SP2 (or later) Professional x86 or x64 Windows Vista Enterprise, Business and Ultimate Edition x86 or x64 Windows 7 Windows Server 2008 Standard and Business edition x86 or x64 Windows 2003 Server SP1 and Advanced Server x86 or x64 Windows Server 2008 Release 2 (R2) x64
Microsoft Windows Setup	WinPE	`ImageName.WIM` `ImageName.EDM`	Windows Vista Enterprise, Business and Ultimate Edition x86 Windows 7 Windows Server 2008 Standard and Business edition x86 Windows Server 2008 Release 2 (R2) x64

*You must have the compatible drivers for the target device in the SOS. If you are using Windows PE, and the drivers are not available, see Building a Custom Windows PE Service OS on page 303. If you are using a Linux SOS, HP will provide periodic updates of the Linux SOS.

**Resulting files are stored in the following directory on the OS Manager Server after the image is captured:

InstallDir\Data\OSManagerServer\upload

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

About the OS Image Capture Tool

The HPCA OS Image Capture tool performs the following tasks:

1. Collects and stores information (including hardware and OS information capabilities) about the reference machine.
2. Executes the exit points that are available for your use as needed. `PRE.CMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.CMD` is executed after Sysprep has sealed the image. See Image Preparation Wizard Exit Points on page 279 for details.

   Image Capture exit points are only supported for ImageX and Windows Setup capture types.

3. Runs Microsoft Sysprep.
4. 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.
5. Creates and copies files to the following directory on the OS Manager Server:

   InstallDir\Data\OSManagerServer\upload

   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.

The OS Image Capture tool requires the Microsoft .NET Framework version 2.0 (or later), which is available at the Microsoft download center:

http://www.microsoft.com/downloads

To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:

```
%SYSTEMROOT%/Microsoft.NET/Framework
```

Preparing the Reference Machine

The process of preparing the reference machine is slightly different depending on the operating system that you are capturing. See the following topics for detailed instructions:

- Windows 7 or Windows Server 2008 R2 x64 on page 74
- Windows Vista or Windows Server 2008 on page 76

Windows 7 or Windows Server 2008 R2 x64

You can capture from either a single or dual-partition OS setup. In case of a dual-partition OS setup, the System Reserved partition will contain the boot manager and HPCA Service OS (SOS) files. The OS partition will contain the boot loader and the OS itself.

1. Install the operating system from the original product media. The reference machine must be capable of running the operating system that you are installing. Make sure the reference machine is using DHCP.
   - When you are prompted for the type of installation, select the **Custom (advanced)** option.
   - When you are prompted for where to install Windows 7, click **Drive Options (advanced)**.
2. Click **New** to create a new partition that will hold Windows 7.
3. In the **Size** box, select the maximum value.
4. Click **Apply**. A dialog box opens to warn you that Windows may create additional partitions. Click **OK** to close this dialog box and proceed.
5. To create a **single partition** installation, follow these steps:
   a. Select the small System Reserved partition, and click **Delete**. A dialog box opens to warn you that any data stored on this partition will be lost.
   b. Click **OK** to close the dialog box and proceed.
   c. Select the remaining partition, and click **Next**. The Windows 7 installation then proceeds.

   To create a **dual-partition** installation, follow these steps:

a. Select the partition that you created in step 4, and click **Delete**. A dialog box opens to warn you that if you delete this partition, any data stored on it will be lost.
b. Click **OK** to close the dialog box and proceed.
c. Select the System Reserved partition, and click **Extend**.
d. In the **Size** box, specify 1024 MB.
e. Click **Apply**. Once again, a dialog box opens to warn you that extending a partition is not a reversible action.
f. Click **OK** to close this dialog box and proceed.
g. Select the partition that you created in step 4 again, and click **New**.
h. In the **Size** box, select the maximum value.
i. Click **Apply**. Once again, a dialog box opens to warn you that Windows may create additional partitions.
j. Click **OK** to close this dialog box and proceed.
k. Click **Next**. The Windows 7 installation then proceeds.

6. When you are prompted to select your computer's location, select **Work Network**.
7. 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.

   Installing the HPCA agent on the reference machine is not recommended. When the OS is deployed, the HPCA agent will be installed (or upgraded, if it is already installed).

8. 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 HPCA Server is finished.
9. Using the Control Panel, set the User Access Control level to **Never notify**.

10 Keep the file system as small as possible (this will minimize the size of the `.WIM` file).

> To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GByte image, you will need 50-60 GByte of free disk space.

a Delete unnecessary files and directories from the files system.

b Turn off System Restore.

11 As part of the capturing process for Windows 7 and Windows Server 2008 R2 x64, the system will be set up to boot into Capture mode if it reboots from the local disk. There is no need to have Image Capture media present on CD or network.

Windows Vista or Windows Server 2008

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. It is the only drive that 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.

> Installing the HPCA agent on the reference machine is not recommended. When the OS is deployed, the HPCA agent will be installed (or upgraded, if it is already installed).

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 HPCA 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.

> For Windows operating system prior to Windows 7, HP supports deploying the image to the primary boot partition of the primary boot drive.

> To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GByte image, you will need 50-60 GByte of free disk space.

a Delete unnecessary files and directories from the files system.

b Turn off System Restore.

5 As part of the capturing process for Vista and Windows Server 2008, the system will be set up to boot into Capture mode if it reboots from the local disk. There is no need to have ImageCapture media present on CD/DVD or the network.

Capture the OS Image

You can use the OS Image Capture tool to capture an image of a reference machine and upload that image to the HPCA server. You can then publish that image and deploy it to managed devices in your environment.

The Image Capture tool can be used with the following operating systems:

- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2 (64-bit)

> The OS Image Capture tool supports Windows Preinstallation Environment (Windows PE) based captures only. To perform Thin Client captures, see Preparing and Capturing Thin Client OS Images on page 80. To capture older OS images, see Capturing Windows XP and Windows Server 2003 OS Images on page 277.

To access the OS Image Capture Tool

1. Log on to the reference machine using an account with administrator privileges.
2. Insert the ImageCapture media CD into the reference machine.

   See "Product Media" in the *HPCA OS Manager System Administrator User Guide* if you need more information about where to get this media.
3. On the ImageCapture CD, browse to the following folder:

   `image_preparation_wizard\win32`
4. Run `oscapture.exe`.

   The OS Image Capture tool opens. The Welcome page provides information about the reference machine hardware and operating system.

   > If the operating system on the reference machine is older than those listed above, the HPCA Image Preparation Wizard opens instead. See Capturing Windows XP and Windows Server 2003 OS Images on page 277 for more information.
5. Click **Next** to proceed. The Imaging Options page opens.

Imaging Options

Use the Imaging Options page to specify the following information:

- **Imaging Method** – Select ImageX or Windows Setup.
  - ImageX captures an image in `.WIM` format that will be deployed using Windows PE and the ImageX utility.
  - Windows Setup captures an image in `.WIM` format that will be deployed using Windows PE and Windows Setup.

  Windows Setup provides greater control over the installation. ImageX is more comparable to a simple file extraction. You can perform unattended installations or upgrades with images captured using either method.

  For more information about ImageX and Windows Setup, refer to the Windows documentation available at **http://technet.microsoft.com**.
- **Image Name** – A name that you choose for this image. The files that are uploaded to the HPCA server and used to deploy this image will use this name.

The image name can be up to eight characters long. It is not case-sensitive.

- **Image Description** – Any descriptive information that you want to provide. When this image is published, this information will be displayed in the list of available operating system images on the HPCA server.

  The image description can be up to 80 characters long.

- **Destination Server** – Host name or IP address of the HPCA server to which this image will be uploaded after it is captured.

  The Image Capture Tool will attempt to contact the HPCA server to ensure that the image can be uploaded after the capture. If it cannot connect, you will see an error message. Be sure that the system proxy and firewall settings on the reference machine will allow it to communicate with the server.

- **Port** – Port number on which the HPCA server specified above is listening. The default port is 3466.

Click **Next** to proceed to the Summary page.

Summary

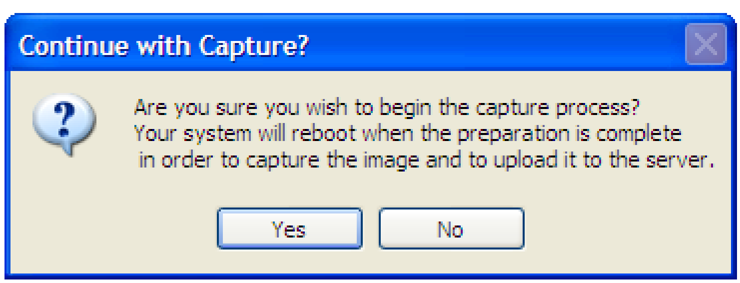
The Summary page shows you information about the image that you are about to capture, including the name that you specified and the estimated size of the image.

To change any of the parameters that you have specified for this capture, click the **Back** button to return to the Imaging Options page.

To capture the image and upload it to the specified HPCA server, click **Capture**.

The following things happen...

1 This dialog box appears:



2 Click **Yes** to prepare the machine, reboot, and capture the image.

   The capture can take 15-20 minutes to complete, depending on the size of the image. During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 93 for more information.

3 After the image is captured, the OS Image Capture tool connects to the network and stores the image in the following directory on the HPCA server:

   `InstallDir\Data\OSManagerServer\upload`

4 When the upload process is complete, you will be asked to reboot the machine.

Next, you will want to publish your image to the HPCA database. Refer to "Publishing" in the HPCA console online help.

Preparing and Capturing Thin Client OS Images

The following sections explain how to prepare and capture supported thin client operating system images:

- Windows XPe and WES OS Images on page 80
- Windows CE OS images on page 85
- Embedded Linux OS Images on page 88

Windows XPe and WES OS Images

The following sections explain how to prepare and capture a Windows XPe and Windows Embedded Standard (WES) thin client operating system image:

- Prepare the Windows XPe or WES Reference Machine on page 81
- Install the Application Manager on Windows XPe or WES (for HPCA Classic only) on page 81

- Run the Image Preparation Wizard on page 82

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

Task 1: Prepare the Windows XPe or WES Reference Machine

To prepare a Windows XPe or WES thin client for image capture, you will need the following:

- HPCA media
- XP Embedded Feature Pack 2007 media
- Image Preparation CD-ROM

Before you can capture a Windows XPe or WES image, you must do the following:

1. Log into Windows XPe or WES as Administrator.
2. From the XP Embedded Feature Pack 2007 media, copy `etprep.exe` to `C:\Windows`.
3. From the XP Embedded Feature Pack 2007 media, copy `fbreseal.exe` to `C:\Windows\fba`.
4. Before you capture the image, you must install the HPCA agent on the Windows XPe or WES device. Refer to "Installing the HPCA Agent on HP Thin Clients" in the *HPCA Core and Satellite User Guide,* or refer to the *HPCA Application and Application Self-service Manager Guide* for details.

Task 2: Install the Application Manager on Windows XPe or WES (for HPCA Classic only)

1. Access the product media from the Windows XPe or WES 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 HPCA Configuration Server.

   The Application Manager is installed.

Task 3: Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1 Checks if there is enough free disk space on the machine and verifies that the Application Manager is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.

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

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

4 Creates and copies the following files to *`InstallDir`*`\Data\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 or WES 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.

   A comprehensive log (*`machineID`*`.log`) is available in *`InstallDir`*`\Data\OSManagerServer\upload` after the image is deployed.

To use the Image Preparation Wizard

1 Insert the Image Preparation Wizard CD-ROM that you created into the CD-ROM drive of the reference machine. (Thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA media.

2 If autorun is enabled, the HPCA OS Preparation and Capture CD window opens.

3 Browse to the `\image_preparation_wizard\win32` directory.

4 Double-click **prepwiz.exe**.

The Image Preparation Wizard verifies that `etprep.exe` and `fbreseal.exe` are available before continuing. The Welcome window opens.

5 Click **Next**.

The End User Licensing Agreement window opens.

6 Click **Accept**.

7 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 used for OS imaging and deployment in an HPCA Core and Satellite installation is 3466. In an HPCA Classic installation, port 3469 is reserved for this purpose.

If the Image Preparation Wizard cannot connect to the OS Manager Server 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.

8 Click **Next**.

The Image Name window opens.

9 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.

10 Click **Next**.

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

11 Type a description for the image file.

12 Click **Next.**

The Options window opens.

13 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 that the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.

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

The Summary window opens.

15 Click **Start**.

16 Click **Finish.**

The wizard prepares the image.

17 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 from Prepare the Windows XPe or WES Reference Machine on page 81.

The upload of the image may seem to take a long time. Transfer speeds will 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.

During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 93 for more information.

18 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
```

19 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 HPCA database. See Publishing on page 97.

Windows CE OS images

The following sections explain how to prepare and capture a Windows CE thin client operating system image:

- Prepare the CE Reference Machine on page 85
- Install the Application Manager on the CE Reference Machine on page 85
- Run the Image Preparation Wizard on page 86

Task 1: Prepare the CE Reference Machine

- Product media
- Image Preparation CD-ROM

Before you capture the image, you must install the HPCA agent on the Windows CE device. Refer to "Installing the HPCA Agent on HP Thin Clients" in the *HPCA Core and Satellite User Guide,* or refer to the *HPCA Application and Application Self-service Manager Guide* for details.

When you deploy an OS to a Windows CE device using Local Service Boot (LSB), there must be sufficient space available on the device to install and extract the LSB service. If the device reboots but fails to boot the Linux Service OS (SOS), the amount of "storage memory" allocated on the device may be insufficient—at least 10 MByte is required.

Follow these steps on the Windows CE device:

1. Click **Start**.
2. Select **Settings** > **Control Panel**.
3. Click the **System** icon.
4. Select the **Memory** tab.
5. Use the slider on the left to increase the **Storage Memory** to 10 MByte or more.

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 HPCA Configuration Server and click **OK**.

The Application Manager is installed.

Task 3: Run the 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 Image Preparation Wizard runs to collect the image and its associated files.

3 Creates and copies the following files to *InstallDir*`\Data\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.

A comprehensive log (*machineID*`.log`) is available in *InstallDir*`\Data\OSManagerServer\upload` after the image is deployed.

To use the Image Preparation Wizard

1 Insert the Image Preparation Wizard CD-ROM that you created into the CD-ROM drive of the reference machine (thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA media.

2 If autorun is enabled, the HPCA OS Preparation and Capture CD window opens.

3 On the CD, browse to the `\image_preparation_wizard\WinCE` directory.

4 Double-click **prepwiz.exe**. The Image Preparation Wizard opens.

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

   The OS Manager Server port used for OS imaging and deployment in an HPCA Core and Satellite installation is 3466. In an HPCA Classic installation, port 3469 is reserved for this purpose.

   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 **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 from Prepare the CE Reference Machine on page 85.

   The upload of the image may seem to take a long time. Transfer speeds will 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

   During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 93 for more information.

7 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
```

8 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 Publishing on page 97.

Embedded Linux OS Images

The following sections explain how to prepare and capture an Embedded Linux operating system image:

- Prepare the Embedded Linux Reference Machine on page 88
- Install the HPCA Agent on the Embedded Linux thin client on page 89
- Run the Image Preparation Wizard on page 90

Task 1: Prepare the Embedded Linux Reference Machine

To prepare an Embedded Linux thin client for image capture, you will need the following:

- HPCA media
- Image Preparation CD-ROM

Before you capture the image, you must install the HPCA agent on the embedded Linux device. Refer to "Installing the HPCA Agent on HP Thin Clients" in the *HPCA Core and Satellite User Guide,* or refer to the *HPCA Application and Application Self-Service Manager Guide* for details.

Task 2: Install the HPCA Agent on the Embedded Linux thin client

➤ If the HPCA Registration and Loading Facility (RALF) is not pre-installed on the reference machine, it should be installed after the HPCA agent is installed.

The best way to install the HPCA Agent on a managed client device is to deploy it from the HPCA Console. You can also install it manually, if you prefer, by following these steps:

1. Login to the target HP thin client device as root. If you are running ThinPro, you may have to create a custom connection for xterm. See To create a custom connection for xterm.
2. Create a new directory called `/opt/hpca`.
3. Copy the install media from the appropriate Linux thin client subdirectory on the HPCA media to a temporary directory on the `/tmp` filesystem.
4. Change the working directory to the new temporary directory.
5. Run the installation by typing:

   `./install -i HPCA_Configuration_Server`

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

   The Application Manager is installed.

To create a custom connection for xterm

If you are using the ThinPro operating system, you may need to create a custom connection to create an xterm connection.

1. From the HP menu in the lower left corner, select **Shutdown**.
2. From the Thin Client Action drop down, select **switch to admin mode** and specify the Administrator password (default password is root).

   Note: Control Center background will change from blue to red.
3. From the Control Center, click the **Add** drop down list and select the **custom** option.
4. Set Name to **xterm**.
5. Set Command to run to:

sudo xterm -e bash &.

6. Click **Finish**.

You now have a connection you can use to open an xterm session.

Task 3: Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

1. Checks if there is enough free disk space on the machine and verifies that the Application Manager is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
2. Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
3. 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.
4. Creates and copies the following files to `*InstallDir*\Data\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.

   A comprehensive log (*machineID*`.log`) is available in *InstallDir*`\Data\OSManagerServer\upload` after the image is deployed.

To use the Image Preparation Wizard

1. Insert the Image Preparation Wizard CD-ROM you created into the CD-ROM drive of the reference machine (thin client devices require a USB CD-ROM drive). This CD is created using the `ImageCapture.iso` found within the `Media\iso\roms` directory on your HPCA 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`

   The OS Manager Server port used for OS imaging and deployment in an HPCA Core and Satellite installation is 3466. In an HPCA Classic installation, port 3469 is reserved for this purpose.

   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 from Prepare the Embedded Linux Reference Machine on page 88.

The upload of the image may seem to take a long time. Transfer speeds will 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 HPCA database for distribution to managed devices. See Publishing on page 97.

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the HPCA database. For instructions, see Publishing on page 97.

After you publish an OS image to HPCA, refresh the OS Library page on the Operations tab to view the new image. Use the HPCA Console toolbar to deploy the image to selected devices.

About the Windows PE Service OS Screen

A Service OS is a pre-installation environment that is based on a lightweight operating system such as Linux or Windows PE. The Service OS does the following things:

1. Boots into the target hardware
2. Loads all the drivers that are needed in order for that hardware to function correctly
3. Downloads and runs HPCA programs which, in turn, download and install OS images

The Service OS is used to perform the following types of operations:

- Operations to hardware on a target device (for example, a BIOS update or hardware configuration)
- Provisioning target devices (for example, deploying an OS)
- Capturing an OS image

Whenever a Service OS starts, the Service OS screen appears on the pertinent device. When an OS image is being captured, for example, the Service OS screen appears on the reference machine. When an OS is being deployed, the Service OS screen appears on the target device.

The Windows PE Service OS screen shows you the status of the operation. Figure 3 is an example of the screen during an image capture operation.

Figure 3 Windows PE Service OS Screen Example

The right side of Windows PE Service OS screen shows you a scrolling log of the steps that are being performed.

- A green checkmark icon indicates that a particular step either is in progress or has been successfully completed.
- A yellow triangle icon is a warning that something may be wrong.

- A red X icon indicates that this step in the capture or deployment has failed.
- A blue question mark (?) icon indicates that input is required.

Information about the current step always appears at the bottom of the list of messages. A scroll bar appears on the far right if there is not enough room to list all of the messages.

If the operation is successful, a green check mark appears on the left side of the Service OS screen with further instructions. If the operation is not successful, a red X appears there with information about the nature of the failure.

If the operation fails, you can use the scroll bar to view information about the hardware detected and determine where in the process the failure occurred.

6 Publishing

This chapter includes the following topics:

Publishing Overview

After you have created your OS image, you must use the Publisher to publish it to the HPCA Database (CSDB).

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

For more information about the Publisher, see the *HP Client Automation Core and Satellite Administrator User Guide*.

After you publish images, they can be entitled and deployed to managed devices in your environment.

To start the Publisher

1. Go to **Start** → **All Programs** → **HP Client Automation Administrator** → **HP Client Automation Administrator Publisher**
2. To log in to the Publisher use your HPCA Administrator user name and password. By default, the user name is **`admin`** and the password is **`secret`**.

Publishing options vary based on the intended target devices and the HPCA license you have installed.

Table 3 on page 98 shows which publishing options are available for each of the three license levels.

Table 3 Publishing Options Available with Each HPCA license

Publishing Option	Starter	Standard	Enterprise
Component Select	No	Yes	Yes
Hardware Configuration	No	No	Yes
HP BIOS Configuration	Yes	Yes	No
HP Softpaqs	Yes	Yes	No
OS Add-ons/extra POS drivers	No	Yes	Yes

Table 3 Publishing Options Available with Each HPCA license

Publishing Option	Starter	Standard	Enterprise
OS Image	No	Yes	Yes
Windows Installer	No	Yes	Yes
Thin Client Component Select	Yes	Yes	Yes
Thin Client OS Image	Yes	Yes	Yes

- The following sections explain how to use the Publisher for the publishing options for your license. Publishing BIOS Settings on page 108

Publishing Operating System Images

Operating system images created using the Image Preparation wizard are stored on the HPCA server in the following directory:

`InstallDir\Data\OSManagerServer\upload`

You can use the Publisher to publish operating system image files for distribution to managed devices. The specific files that you will need depends on the deployment method that you intend to use (see Table 4 on page 100).

If you captured an OS image from a reference machine, you will need the files that resulted from that capture process. For more information, see Preparing and Capturing OS Images on page 67.

If you will be publishing `.WIM` images, see Prerequisites for Publishing .WIM images on page 101 before you begin the publishing process.

Table 4 Files Needed to Publish OS Images

Deployment Method	Files Required	Refer To
Directly from a DVD	DVD `WIM` file HPCA `unattend-dvd.xml`	Pre-requisites for Publishing Directly from a DVD on page 102

Microsoft ImageX	`ImageName.WIM`
	`ImageName.EDM`
	HPCA `unattend-capture.xml`
		Prerequisites for Publishing .WIM images on page 101

Windows Setup	`ImageName.WIM`
	`ImageName.EDM`
	HPCA `unattend-capture.xml`
		Prerequisites for Publishing .WIM images on page 101

Legacy	`ImageName.IMG`
	`ImageName.MBR`
	`ImageName.EDM`
	`ImageName.PAR`
	For WinXPe or Windows CE:
	`ImageName.IBR`
	`ImageName.EDM`
	For Linux:
	`ImageName.DD`
	`ImageName.EDM`
		Publish OS Images on page 104

The names of the `unattend` files shown in Table 4 refer to the files provided in the Image Capture ISO. You can change the name of this file as you see fit.

For information about customizing the `unattend` file, see Customizing the Windows Answer File on page 263.

Prerequisites for Publishing .WIM images

This information in this section pertains to the following Windows operating systems:

- Windows XP SP2/SP3
- Windows 2003 SP1/SP2
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 Release 2 (R2)

If you are publishing a `.WIM` image of one of these versions of Windows, you must:

- Have access to the `\agent` folder on the HPCA media.

  This folder is only required the first time you publish a `.WIM` file or if you want to publish an updated agent package. The HPCA 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.

- For Windows Vista, Windows Server 2008, or Windows 7:

  If you are deploying using Windows Setup, you must be able to access the `\sources` folder from the Windows installation media (used to obtain or create the `.WIM` file) on the device where you are publishing the image.

  This does not apply to Windows XP or Windows 2003 `.WIM` files.

- Install the Windows Automated Installation Kit (AIK) for Windows 7 on the device where you are publishing the image. The Windows AIK is available for download from the Microsoft web site.

  Be sure to install the Windows 7 version of the Windows AIK. This version works for all the operating systems listed above.

  Install the Windows AIK in its default location:

  `C:\Program Files\Windows AIK`

- If you are using an existing *`filename`*`.wim`, 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 (*`InstallDir`*`\Data\OSManagerServer\upload`) to the device where you are publishing the image.

  If your file was spanned, copy `filename.swm`, `filename2.swm`, etc. from the `\upload` directory. These files will be published as *`filename`*`.wim`, *`filename`*`.002`, *`filename`*`.003`, and so on.

- HPCA provides a Windows Setup answer file that you can use for unattended installations. When you run the Publisher, you can choose to either use the answer file that HPCA provides (preferred method) or create your own. See Specifying the Windows Setup Answer File on page 103 for more information

  The answer file that HPCA provides is called `unattend.xml`. Each operating system and architecture (for example, 32-bit or 64-bit) has its own `unattend.xml` file. The files are located in subdirectories of:

  `InstallDir``\Data\OSManagerServer\capture-conf`

  If you want to use the `unattend.xml` file that HP provides, you must modify it for your environment before you run the Publisher. At a minimum, you must specify the ProductKey for the image that you are publishing. You may also want to modify other settings in this file—for example, the TimeZone and the RegisteredOrganization. See Customizing the Windows Answer File on page 263 for details.

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.

Pre-requisites for Publishing Directly from a DVD

Publishing an OS image directly from a DVD is the easiest method to use. This implies that the deployment will be done using Windows Setup. If you want to use straight image deployment, you must use the Image Preparation Wizard and select ImageX as the deployment method.

To prepare to publish an OS image directly from a DVD

1. Copy the `install.wim` file from the DVD to a local folder on the device where you are publishing the image.

2 Mount the image capture ISO.

Specifying the Windows Setup Answer File

Prior to HPCA version 7.90, it was necessary to manually modify and rename files used by HPCA to support unattended installation of a particular OS image.

Now, you can specify the source of this information when you run the Publisher. This new method is much simpler and less prone to error than the manual method. It is the preferred method for specifying this information.

For backward compatibility, the old method is described in an appendix to this guide. See Customizing the Windows Answer File on page 263.

Publish OS Images

The following section describes how to use the Publisher to publish operating system images. There are four basic steps:

- Select the OS image
- Select the Windows Answer File for unattended installations (if needed)
- Specify the package options
- Publish

The following procedure provides detailed instructions. Note that the steps vary depending on the options that you choose.

Be sure to satisfy the Prerequisites for Publishing .WIM images or Pre-requisites for Publishing Directly from a DVD on page 102 before you start the Publisher.

To publish operating system images

1. Start the Publisher. See To start the Publisher on page 98.
2. In the Publishing Options area:
   - If you are publishing for thin clients, select **Thin Client Publishing**.
   - From the drop-down menu, select **OS Image**.
3. Click **OK**. The Select OS Image File page opens.
4. Select the OS image file that you want to publish.

   Images created using the Image Preparation Wizard are stored on the OS Manager Server in the following folder:

   `InstallDir\Data\OSManagerServer\upload`

   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 HPCA database. Use HPCA Console 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 either copied the `\agent` folder from the agent media to this device or the agent folder must be available via a network drive or other media. Select the directory that contains the Agent installation media. On the HPCA Core and Satellite media, for example, this directory is:

`<media root>\Media\client\default`

5 Use the **Description** area to verify that you have selected the correct file before you continue. You can also add information to the description if you choose.

6 Click **Next**.

7 If you did NOT select a `.WIM` file in step 4—for example, if you are publishing a thin client image—skip to step 18.

8 If you manually created `*.subs` and `*.xml` files for this image, skip to step 10. This is not recommended. See Customizing the Windows Answer File on page 263 for more information.

9 In the directory tree, select your Unattended Windows Answer File (`unattend.xml`).

See Prerequisites for Publishing .WIM images on page 101 for additional information.

10 Click **Next**.

11 If you selected a `.WIM` file in step 4, perform *either* Action 1 or Action 2:

Action 1: If you selected a `.WIM` file that was created using the Image Preparation Wizard method for ImageX deployment:

a From the **Deployment method** drop-down menu, choose **Microsoft ImageX**.

b Ignore the **Sources Directory** box.

or

Action 2: If you selected a `.WIM` file in step 4 that was created using the Image Preparation Wizard for Windows Setup deployment OR you are publishing a `.WIM` file from DVD media:

a From the **Deployment method** drop-down menu, choose **Microsoft Setup**.

b. In the **Sources Directory** box, use the **Browse** button to select the `\sources` directory from the Windows installation media DVD that was used to set up the reference machine that you captured using the Image Preparation Wizard.

Always use the `\sources` directory from 32-bit Windows installation media DVD, even if you are publishing a 64-bit image file.

12. In the Client media location, browse to the correct path for the HPCA Agent media (this is in the `Media\client\default` folder on the HPCA media).

    Select the appropriate subdirectory, depending on the target platform that you are publishing for (either a regular machine or thin client).

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

13. Click **Next**.
14. Use the **Package Information** section to enter the details about this package. Note that the **Limit package to systems with** section is not available when publishing OS images.
15. Click **Next**.
16. In the **Service Information** section, select **Create new**.

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

17. Enter the appropriate Application Information in the remaining fields.

    In the **Assignment type** group box, select **Mandatory**.

18. Click **Next**. The Summary window opens.
19. Review the **Summary** information to verify the package and service information that you provided during the previous steps. When you are satisfied, click **Publish**.
20. Click **Finish** to exit the Publisher when the publishing process is complete.

The service is now ready for distribution to managed devices in your enterprise.

You can view the published operating system image service in the OS Library on the Operations tab.

Publishing OS Add-Ons and Extra Production OS (POS) Drivers

For a detailed discussion of this process, see Customizing OS Deployment by Using Exit Points and Add-Ons on page 203.

You can add drivers to previously prepared images by creating **delta packages** that are deployed after the image is installed on a new local partition. This is limited to the Microsoft Windows Setup and ImageX deployment methods.

Prerequisites

- Publish your OS service. The Publisher automatically creates a connection, OS.ADDON.ServiceName_*, under this service.
- If you are publishing OS drivers:
  - — Create the following directory:

    `C:\MyDrivers\osmgr.hlp\drivers`
  - — Store the individual drivers that you want to publish in this directory.

To publish delta packages

1. Go to **Start→All Programs→HP Client Automation Administrator→HP Client Automation Administrator Publisher**. The Logon screen opens.
2. Type your HPCA Administrator user ID and password (by default, **`admin`** and **`secret`**).
3. In the Publishing Options windows select **OS Add-ons/extra POS drivers** from the drop-down list.
4. Click **OK**.
5. Use the Select Drivers Directory window, specify the following:
   a. In the directory tree, select the `C:\MyDrivers` directory.

      Everything below this directory will be recursively scanned, included, and published.
   b. From the **Add-on type** drop-down list, select **OS Driver** file.

c. From the **Select Target Service** drop down list, select the OS service to which you want to add these drivers or add-ons.

d. In the optional **Suffix** text box, you can type a number that can be used to track packages. For example, if the instance is called VISTA_PDD and you type 0 in this text box, then the new ADDON instance name will be VISTA_PDD_0.

   In the **ADDON Instance Name** text box, the instance name will be prepopulated based on the OS service name you selected. It is recommended that you leave this as is.

   It is recommended that you leave this name as is. If you modify this name, there will be no connection between the OS service and the ADDON instance unless you create the connection yourself.

6. Click **Next**.
7. Review the summary screen and click **Publish**.

You can use the CSDB Editor to review the new ADDON instance in PRIMARY.OS.ADDON. The next time the operating system service is deployed, the delta packages will automatically be deployed with it.

When this operating system service is deployed to a target device, the OS drivers are stored in the `C:\OSMGR.HLP\Drivers` directory on the target device.

Publishing BIOS Settings

Use the Publisher to publish a BIOS settings file as a service for distribution to client devices. You can use the settings file to update or modify BIOS settings (for example, boot order) or to change the BIOS password on the client device.

A sample BIOS settings file (`Common HP BIOS Settings.xml`) is included with the Publisher installation and located by default in: `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS`. Use this file to modify BIOS settings on target devices.

If the sample BIOS settings file does not include the options you require, or you would like to create a settings file for a specific device, see Creating a BIOS Settings File on page 110.

To publish BIOS settings

1. Start the Publisher (see To start the Publisher on page 98).
2. At the Logon window, type your administrator User ID and password and click **OK**.

   > Log in to the Publisher using the HPCA user name and password. By default, the user name is **`admin`** and the password is **`secret`**.

3. In the Publishing Options area, select **HP BIOS Configuration** and click **OK**. The Select window opens.
4. Select the BIOS settings file to publish. The sample BIOS settings file (`Common HP BIOS Settings.xml`) is located by default in: `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS`.
5. In the **Current BIOS Admin Password** area, type and then confirm a BIOS password if required. This is required to change any settings if the target devices have a BIOS password.
6. If you want to change the current BIOS password, select, **Change BIOS Password**, then type and confirm the new password. This is required only if you want to change the BIOS password on a client device.
7. Click **Next**. The BIOS Options window opens.
8. To select the BIOS settings to publish click the check box to the left of the BIOS setting name.
9. If you need to change the value of a BIOS setting, click the setting name and adjust the available options as necessary.
10. Click **Next**. The Application Information window opens.
11. View, and if necessary, modify the application information. Application information is pre-determined based on what is available from the settings file.
12. Click **Next**. The Summary window opens.
13. Review the summary information and when satisfied, click **Publish**.
14. When the publishing process is complete, click **Finish** to close the Publisher.

The BIOS settings service is available in the Software library of the HPCA console.

Creating a BIOS Settings File

If you would like to use a BIOS settings file other than the file included with HPCA, you can use the HP System Software Manager (SSM) BIOS Configuration Utility to generate your own settings file.

SSM is installed with the HPCA Agent (`C:\Program Files\Hewlett-Packard\SSM`) or can be downloaded from the HP support site.

To create a BIOS settings file

1 Open a command prompt and change to the directory where the SSM BIOS Configuration Utility is located (`C:\Program Files\Hewlett-Packard\SSM`, by default).

2 Type the following:

```
BiosConfigUtility.exe /
GetConfig:"C:\tmp\MyBIOSconfig.xml" /Format:XML
```

This command will generate an XML file called `MyBIOSconfig.xml` and store it in `C:\tmp`.

If you want to create a text file instead of XML, type:

```
BiosConfigUtility.exe /
GetConfig:"C:\tmp\MyBIOSconfig.txt" /Format:REPSET
```

This command will generate a text file called `MyBIOSconfig.txt` and store it in `C:\tmp`.

3 When you are ready to publish BIOS settings, select this file in step 6 of To publish BIOS settings on page 109.

Viewing Published Services

View published software in the Management tab, Software Management area.

Published operating systems are stored in the Operating System area.

HP Client Automation Administrator Agent Explorer

Installed with the Publisher as part of the HP Client Automation Administrator, the Agent Explorer is available to aid with troubleshooting and problem resolution and should not be used without direct instructions from HP Support.

7 Preparing Content

This chapter includes the following topics:

This chapter provides information on how to use the OS Manager and CSDB Editor 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`, deploying OSs from CD or DVD, and Sysprep are not supported on thin clients. It is important to be aware of this because the interface for these features has 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 Enterprise Manager to view the ROM object, which is stored below the device. 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 5 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. NOTE: In a Core and Satellite environment, the default behavior will no longer prompt the user for the target device role. 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.

Table 5 Expected Results on Target Device

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 upon reboot of the machine 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. The behavior settings will determine how and when the installation will take place—for example, whether the resolved OS is installed or not or whether a user is prompted or not.
has no recognizable partitioning and the Encryption Support Mode parameter, `ENCMODE`, is set to it's default value of `AUTO` – which means that supported encryption products are detected	A new operating system will not be installed unless you use the OS Management Wizard in the Enterprise Manager to reinstall the operating system.
has a corrupted partition table and the Encryption Support Mode parameter, `ENCMODE`, is set to `NONE`	If the disaster recovery behavior setting `PMDISRCV=_CONFIRM_` then the target device shuts down so the administrator can recover data from the target device. This works only if the OSSTATE attribute in the ROM object is not _INVALID_. You can view the ROM object attributes in the HPCA console. If the disaster recovery behavior setting `PMDISRCV=_AUTO_` then the appropriate OS is reinstalled.

Table 5 Expected Results on Target Device

If the target device...	then...
has no recognizable partitioning and the Encryption Support Mode parameter, `ENCMODE`, is set to `ENC`	A new operating system will not be installed unless you use the OS Management Wizard in the Enterprise Manager to reinstall the operating system.

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.

  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 using the Enterprise Manager.
  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 Advanced Topic: Assigning OSs by Using Policy on page 118 for important information about implementing policy.

When using the Machine ROLE, be aware that setting a ROLE value in the device's ROM object must be done through a custom script, as this is not currently exposed in the HPCA console.

Assigning OSs to Devices and Groups

Use the OS Management feature in the Enterprise Manager (the HPCA console in a Core and Satellite installation) to assign operating systems to individual devices or groups of devices. For instructions, refer to the appropriate topic for your license and installation type:

Installation Type	License Type	Topic
Core and Satellite	Enterprise	"Managing Operating Systems" in the HPCA Enterprise Console online help and the *HP Client Automation Enterprise Edition Core and Satellite User Guide*
	Standard	"OS Management" in the HPCA Standard console online help and the *HP Client Automation Standard Edition Core and Satellite User Guide*
Classic (component-based)	Enterprise	"Managing Operating Systems" in the Enterprise Manager online help and the *HP Client Automation Enterprise Manager Guide*

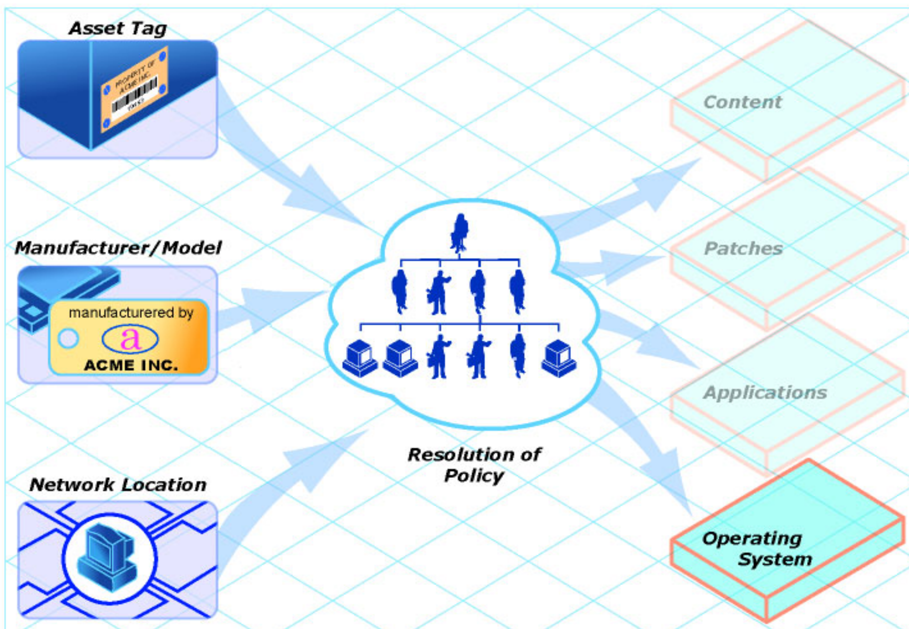
Manufacturer, model, and subnet are based on attributes related to a device. Role is *not* based on a device's attributes. It is simply a grouping of devices, similar to how you might assign policy based on departments. You can set policy based on a device's assigned role—such as server or workstation.

Advanced Topic: Assigning OSs by Using Policy

As an alternative to using the HPCA console to assign operating systems to managed devices (or groups of devices), you can use policy assignments to determine which OS is installed on a particular device. This is much more difficult than using the console method, however, and should only be attempted by experienced HPCA administrators.

We recommend that you select a single criterion for policy.

Figure 4 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.

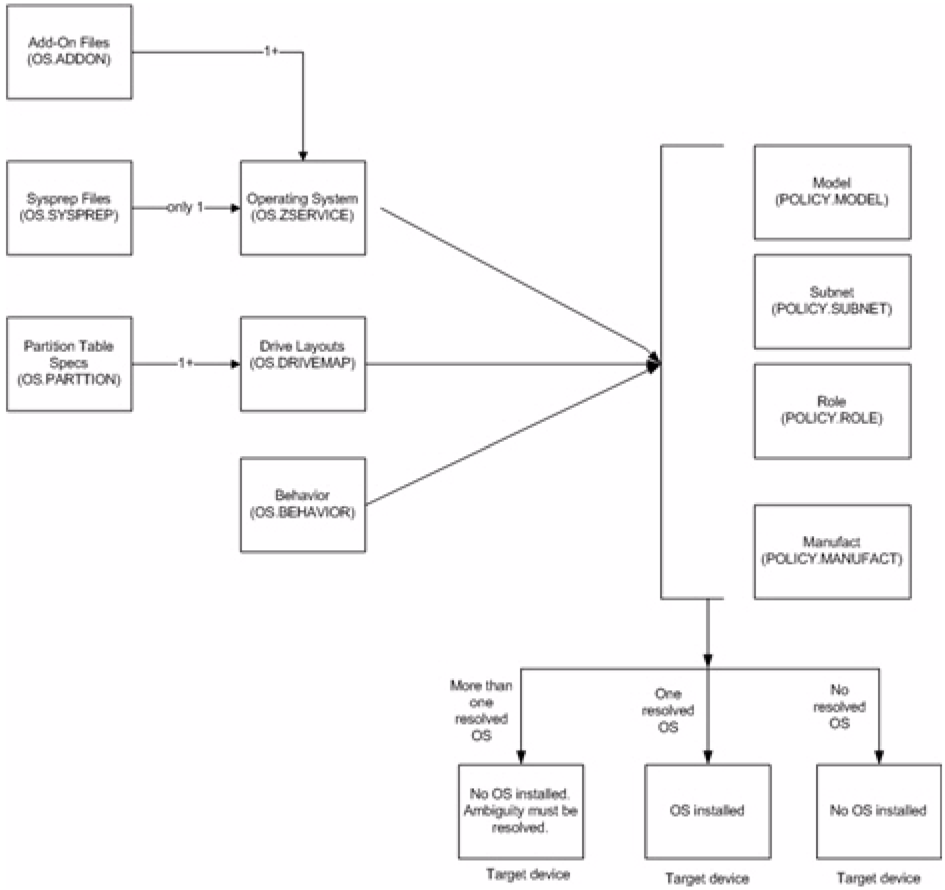
- If your environment is divided by subnets, you may choose to use the SUBNET criterion. For example, server farms are typically defined by subnets.

- If your environment is 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.

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

If more than one criterion was used to determine policy and the machine is a bare metal machine, the user of the target device will be given a list of operating systems from which to choose.

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



Advanced Topic: Preparing Content Using the CSDB Editor

Typically, you will use the Enterprise Manager (the HPCA console in a Core and Satellite installation) to simply assign an operating system to a set of target devices and initiate the deployment. See

In some cases, however, you may need to make use of advanced capabilities to handle customer needs. To do this, you will use the CSDB Editor to create, modify, and prepare content in production environments. You must be familiar with the CSDB Editor to complete these tasks.

Before you begin preparing content, 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 operations to learn how to use the CSDB Editor to complete the operations.

> To use the following scenarios, you must be logged into the CSDB Editor as an administrator.

Table 6 Advanced Administrative Procedures

If you want to...	Then...
Install an OS on a bare metal machine Note: This does not apply to Local Service Boot implementations.	1 Use the Enterprise Manager (the HPCA Console in a Core and Satellite installation) to create any necessary policy instances. If you are creating a manufacturer or model policy instance, see Creating a Manufacturer or Model Instance on page 132. 2 Use the Enterprise Manager (the HPCA Console in a Core and Satellite installation) to connect the OS service to the policy instances. 3 If you do not want to use the default behavior (the Undefined instance in the Behavior class or in a Core and Satellite environment, DEFAULT_BEHAVIOR), you can modify the behaviors. See Setting Behaviors on page 127. 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. 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 Chosen OS are Unmanaged. 2 Use the OS Management Wizard in the Enterprise Manager.
Force a re-installation of the current OS without retaining any existing data.	Use the OS Management Wizard in the Enterprise Manager (the HPCA Console in a Core and Satellite installation). Be sure to check the **Emergency** check box on the Deployment Options page when executing the OS management wizard.

Table 6 Advanced Administrative Procedures

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. 2 Use the OS Management Wizard in the Enterprise Manager (the HPCA Console in a Core and Satellite installation. Be sure to check the **Emergency** check box on the Deployment Options page when executing the OS management wizard
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 127. 2 Assign policy so that the new OS that you want to install is the *only* OS connected to policy. 3 Use the OS Management Wizard in the Enterprise Manager to re-evaluate the state of the OS and install a new one based on policy. Note that if you do not set the Behavior to NEVER, the user of the target device 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. 2 Set the PMSLCTOS behavior to _LOCAL_. See Setting Behaviors on page 127. 3 Use the OS Management Wizard in the Enterprise Manager to re-evaluate the state of the OS and install a new one based on policy.
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 Using an Override Sysprep File on page 149. 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

Table 6 Advanced Administrative Procedures

If you want to...	Then...
Add partitions.	1 Use the Drive Layouts Class to specify the type of partition. See Defining Drive Layouts on page 133. 2 Add a partition. See Adding Partitions on page 147. *All existing data will be lost.* 3 Assign the appropriate drive layouts to your target devices. See Assigning Drive Layouts on page 149.
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 133. 2 Assign the appropriate drive layouts to your target devices. See Assigning Drive Layouts on page 149.

Logging On

To log on to the Client Automation Administrator CSDB Editor

1. Go to **Start**→**All Programs**→**HP Client Automation Administrator**→ **HP Client Automation Administrator CSDB Editor.**
2. In the **User ID** text box, type **`admin`**.
3. In the **Password** text box, type a password. Passwords are case sensitive.

   The pre-defined password is **`secret`**.

   ⚠ Be sure to change your password before moving the CSDB Editor into your production environment.
4. Click **OK**.

About the OS Manager Classes

The following are the classes you may need to use when preparing operating system content.

The CSDB Editor is an open system. You must have a comprehensive understanding of how to use the CSDB Editor and the tasks that you want to perform in order to prevent unintended consequences.

Except for specific instance attributes detailed in this guide, do not change, edit, or delete any of the classes in the OS domain.

- Do not change any of the _BASE_INSTANCE_ wiring.
- Do not change (or otherwise add) _NULL_INSTANCE_.
- Do not change ZxxxPRI attribute values.
- Do not re-order the connections in any of the instances.
- Do not change any of the expressions in any of the instances.

Part of the implementation of the OS Manager is contained in the classes and instances of the OS domain. Any change to anything other than the instance attributes detailed in this guide may render the system unusable and void support.

To view the OS Manager classes

1. Open the CSDB Editor and go to PRIMARY.OS.
2. In the list view, the following classes appear.
   - Behavior (BEHAVIOR)
     Lists the settings for how the OS Manager behaves. You can assign different system behaviors to different target devices. See Setting Behaviors on page 127.
   - Drive Layouts (DRIVEMAP)
     This class lists the types of partitions that you can add or copy, and also allows you to configure new partitions. See Defining Drive Layouts on page 133.
   - HW Config (LDS)
     Stores instances 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 (LME)
Stores instances 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*.

— AddOn Resources (ADDON)
If you use the option **OS Add-ons/Extra POS drivers** in the HPCA Admin Publisher, the directories or files that you select will be published to the ADDON class. There is no need (nor any support) to edit these instances directly.

> OS services published to the CSDB with HPCA 7.5x or 7.8x will have a generic connection pointing to the ADDON class. Any directories or files published using the **OS Add-ons/Extra POS drivers** option in the HPCA Publisher will be included automatically in the OS deployment.
>
> If you migrated from HPCA version 5.11 or 7.2x, you will need to manually add the connection to the OS.ZSERVICE instance:
>
> OS.ADDON.<InstanceNameOfOSService>_*
>
> For example:
>
> OS.ADDON.WIN7X86_*
>
> Place the value in the 6th _ALWAYS_ connection field.

— Mobile File Resource (RMMFILE)
File resources for mobile devices.

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

— OS Packages (PACKAGE)
Used to combine multiple files into packages.

— OS Path (OSPATH)
A controlling class used by HPCA. Do not edit.

— ELIGIBLE (ELIGIBLE)
A controlling class used by HPCA. Do not edit.

— OS Resources (FILE)
OS resources, such as `WIN7.WIM`.

— Partition Table Spec (PARTTION)
Lists the specifications for the partitions that you may add in addition to theh OS boot partition. See Adding Partitions on page 147.

— STATE (STATE)
A controlling class used by HPCA. Do not edit.

— Sysprep Files (SYSPREP)
Lists the Sysprep files and `unattend.txt` files stored in your database. See Using an Override Sysprep File on page 149.

— Unix Config Files (UNIXCFG)
UNIX configuration resource class. Refer to the *HP Client Automation OS Manager System Administrator User Guide for SuSE AutoYaST and Red Hat Kickstart*.

Setting Behaviors

You can assign system behaviors to your target devices based on policy. If you do not assign a behavior to policy, the _NULL_ instance is the default (or in a Core and Satellite environment, DEFAULT_BEHAVIOR 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 In the CSDB Editor, go to PRIMARY.OS.BEHAVIOR.

2 Create a new instance or modify an existing instance.

If you do not know how to create or modify instances, refer to the *HP Configuration Management Administrator User Guide*.

Table 7 Attributes of the Behavior Class

Attribute	Description
Name of this instance	Instance Name
PMROLE	Indicates whether the user is allowed to select a machine role. • _LOCAL_ 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. • _CENTRAL_ Disables the ability to select roles. A role selection remains in effect until you (the administrator) void or overrule the selection. Default: _CENTRAL_ (applies to Core and Satellite environments only) This functionality should no longer be used. In a Core and Satellite environment, it cannot be used from the HPCA Console.

Table 7 Attributes of the Behavior Class

Attribute	Description
PMACKOVW	Specifies whether to prompt the user before overwriting or modifying the OS. • _ALWAYS_ (Default) Prompts the user before a reinstallation. • _NEVER_ Does not prompt the user, but installs the OS. Caution: NEVER is designed for use with unattended devices. Use this option with caution, as the user will not be prompted before the OS is overwritten. • _VALID_ This option has been deprecated.
PMINITL	Specifies whether an OS should be installed over an existing file system on a recently discovered, but unmanaged device. 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. • _LOCAL_ (default) Prompts the user. • _KEEP_ Does not prompt the user and keeps the current OS. • _REINSTALL_ Does not prompt the user and reinstalls the operating system, regardless of what exists.

Table 7 Attributes of the Behavior Class

Attribute	Description
PMDISRCV	Specifies the action to be taken when there is no valid bootable partition. • If PMDISRCV = _CONFIRM_, the target device shuts down so that the administrator can recover data from the target device. • If PMDISRCV = _AUTO_, the appropriate OS is reinstalled.
RUNPARAM	Specifies the parameters that are appended to the `radskman` command line. This command line runs 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 Software Support web site. Be sure to specify the IP address or DNS name for your Configuration Server. If you do not modify this parameter, your target device will not be able to successfully run an HPCA OS connect. Do not remove the `cop=y` parameter; it is necessary because COP must be enabled to use the OS Manager. In the RUNPARAM (RunOnce Parameter String), change IP=RCSSERVER to reference the appropriate Configuration Server for your environment. If your Configuration Server is running on a non-default port, also add: `,port=`*`ConfigurationServerPortNumber`*`>` The default port for Configuration Server is 3464.
ROMAPARAM	Typically, use this only if instructed by Technical Support.

Table 7 Attributes of the Behavior Class

Attribute	Description
BANDWITH	The bandwidth throttle used by each target device. For example, 1000K. 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), which means that the download process will run at the maximum speed of the network interface.
KBDMAP	Sets the keyboard mappings: • **en** (default) loads English keyboard mappings • **fr** loads French keyboard mappings • **de** loads German keyboard mappings For OS deployment using the Windows PE service OS, we additionally have the following values: • **it** Italian • **pt** Brazilian Portugese • **es** Spanish
LANG	Specifies the language to be supported. • en_US = English • zh_CN = Simplified Chinese • ja_JP = Japanese • pt_BR = Brazilian Portuguese • fr_FR = French • de_DE = German • it_IT = Italian • es_ES = Spanish

Table 7 Attributes of the Behavior Class

Attribute	Description
ACKTMOUT	Specifies how long ACKTMOUT waits before assigning the default AUTOROLE. • Set ACKTMOUT = 0 to disable the timeout. • Set ACKTMOUT = *number of seconds* to wait the specified length of time before continuing. This functionality should no longer be used. In a Core and Satellite environments, it cannot be used from the HPCA console.
AUTOROLE	The ROLE that is assigned if a timeout occurs. This functionality should no longer be used. In a Core and Satellite environments, it cannot be used from the HPCA console.

3 When you are done making changes, click **OK**.

4 Connect the BEHAVIOR instance to a POLICY instance.

— Connect only one BEHAVIOR instance per POLICY instance.

— If you are using a Core and Satellite environment, you may need to first remove the DEFAULT_BEHAVIOR connection from the ROLE base instance.

Creating a Manufacturer or Model Instance

As you learned earlier, you can assign OS policy based on various criteria. When you want the policy to be dependent on the device manufacturer or the device model, there is a certain naming convention that must be followed.

Use the following steps to create a Manufacturer or Model instance.

To create a manufacturer or model instance

1 In the CSDB Editor go to PRIMARY.POLICY.MODEL or PRIMARY.POLICY.MANUFACT.

2 Right-click the class name, and select **New Instance**.

3 Type the Display name and the Instance name.

> You must use the manufacturer or model information that is stored in the ROM object in the Enterprise Manager. 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.
>
> When naming the model instance, it must be named as nvdmanufact_nvdmodel.
>
> For example, if you have an HP Compaq dc7700 Small Form Factor machine, manufacturer (nvdmanufact) will be displayed as HEWLETT_PA and the model (nvdmodel) will be displayed as COMPAQ_DC7700_SMALL in the ROM object. The name of the Model instance for this machine should be HEWLETT_PA_COMPAQ_DC7700_SMALL.

4 Click **OK**.

Assigning Operating Systems

You must assign the appropriate OSs to your target devices based on policy such as machine type, manufacturer, model, role or subnet.

To assign operating systems

1 In the CSDB Editor, go to PRIMARY.OS.ZSERVICE.

2 Select the appropriate OS service.

3 Connect the OS Service to a PRIMARY.POLICY instance.

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.

For all supported operating systems, you can use the Drive Layouts class to specify the type of partitioning strategy used. For Windows 7 and Windows 2008 R2, you can also specify how much disk space is allocated to each partition. Partitioning is supported for the boot drive only.

For details, see the following topics:

Partitioning Strategies on page 134

Allocating Disk Space for Partitions on page 138

Special Considerations for Dual-Partition Installations on page 143

Specify the Drive Layout on page 146

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.

Partitioning Strategies

You can use the following attributes in the DRIVEMAP class to specify how HPCA should partition the hard disk prior to installing an operating system on a target device:

Table 8 DRIVEMAP Attributes for Partitioning

Attributes Name	Core and Satellite Default	Classic Default
Type	Merge	Replace
Reserved Space Size	0	0
System Partition Size	1024	1024

These attributes cannot be edited in HPCA Standard Edition.

Table 9 describes the possible values for the DRIVEMAP Types attribute.

Table 9 DRIVEMAP Type Attribute

Type	Description
REPLACE (default in Classic environments)	Replaces the current partitioning on the target device with a single or dual-partition installation as defined for, or included with, the OS image being installed. If there are no DRIVEMAP instances connected to the OS being installed, this is the default method. IMPORTANT: If you use REPLACE, *all existing data will be lost*.
ADD	Same as REPLACE, and this option additionally creates one or more data partitions in an extended partition at the end of the hard disk. See Adding Partitions on page 147 for more information. IMPORTANT: If you use ADD, *all existing data will be lost*.
MERGE (default in Core and Satellite environments)	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 “System Reserved” (if applicable) and OS partition and will not touch data on any other partitions. • If the partitions to be installed are larger than the space already defined for these partitions, the installation will fail. • If the target drive does not contain existing partitions (bare metal, for example), then MERGE will auto-switch into REPLACE mode. See REPLACE on page 135 for behavior. See Special Considerations for Dual-Partition Installations on page 143 for additional information about using MERGE with Windows 7 and Windows Server 2008 R2.

Table 9 DRIVEMAP Type Attribute

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. IMPORTANT: If you use CACHE, *all existing data will be lost*. See Restoring Operating Systems on page 194 for information about restoring this image.

Table 9 DRIVEMAP Type Attribute

Type	Description
PRES	Allows you to preserve a set of files and folders on a target device during the installation of a new operating system and restore them after the OS installation. NOTE: This requires the ImageX method of OS deployment. Any attempt to use any other deployment method will result in an error. To do this: • Before the target device is rebooted to install the new OS, the files and folders to be preserved must be placed in the folder `C:\OSMGR.PRESERVE`. It is recommended that you use `NOVAPDC` to do this. However, any method (including manual) that results in the desired files and folders being placed in the named folder is acceptable. • During the resolution and deployment process, if this Partition Type is resolved for the target device, no disk repartitioning is performed. The existing (NTFS) root file system is kept intact, and all contents of the file system except for the contents of `C:\OSMGR.PRESERVE` are removed. • The new OS image is deployed to the (preserved) file system. • After the machine reboots into the newly deployed OS, the files and folders in `C:\OSMGR.PRESERVE` are available to be restored. It is recommended that you use `NOVAPDR` to do this. However, any method (including manual) that results in the desired files and folders being restored properly is acceptable. Note that all data in `C:\OSMGR.PRESERVE` remains until explicitly removed by the (user-defined) restore process. • If the target drive does not contain existing partitions (bare metal for example) then PRES will auto-switch into REPLACE mode. See REPLACE on page 135 for behavior. NOTE: You cannot use this PRES if your target device has a “System Reserved” partition in addition to the OS partition.

Allocating Disk Space for Partitions

The following information applies only to OS installations using ImageX and Windows Setup deployment methods (Windows PE Service OS only).

You can use the RSVDSPCE and SYSPSPCE attributes of the DRIVEMAP class to control how the hard disk is partitioned on a target device before the OS is deployed:

- CSDB:OS.DRIVEMAP.RSVDSPCE

  Leave un-partitioned free space in the beginning of the drive selected for deployment. This free space can be used later for Microsoft BitLocker enablement (Windows Vista, Windows 2008) or for other purposes such as a recovery partition.

- CSDB:OS.DRIVEMAP.SYSPSPCE

  Create a "System Reserved" partition of the specified size when installing Windows 7 or Windows 2008 R2. If the value of this attribute is greater than zero, Windows 7 or Windows 2008 R2 will be installed in a dual-partition setup including a "System Reserved" partition of the specified size plus the operating system partition itself.

➤ You must specify the values of these attributes in Megabytes. For example: specifying 2000 means 2 GByte.

RSVDSPCE and SYSPSPCE work differently depending on the DRIVEMAP Type and the OS being deployed. The following sections provide the details:

- Windows 7 and Windows Server 2008 R2 on page 138
- Pre-Windows 7 Operating Systems on page 141

Windows 7 and Windows Server 2008 R2

For Windows 7 and Windows Server 2008 R2 installations, you can specify the size of the System partition and unallocated reserved space using the RSVDSPCE and SYSPSPCE attributes.

Table 10 Partitioning in Windows 7 and Windows Server 2008 R2

<table>
<tr><th>DRIVEMAP Attribute</th><th>Description</th></tr>
<tr><td>SYSPSPCE</td><td>The SYSPSPCE attribute specifies the size of the System partition in MBytes.
If no value is specified for SYSPSPCE, the System partition will be 1 GByte.
If SYSPSPCE = 0 (zero), the System partion will not be created.
If the value of SYSPSPCE specified is less than 1000 (1 GByte), a warning is generated.</td></tr>
<tr><td>RSVDSPCE</td><td>The RSVDSPACE attribute specifies how much unallocated disk space should be set aside before the OS partition in a single-partition scenario or before the System and OS partitions in a dual-partition scenario.

This free space can be used for two purposes. It can be used for BitLocker encryption, or it can be used to create a RECOVERY partition at a later time.

When deploying Windows Vista, RSVDSPCE can be used to reserve space on the hard disk to make the system BitLocker-ready without creating a System partition (see Using Microsoft BitLocker on page 64). When deploying Windows 7 or Windows Server 2008 R2, the System partition defined by the SYSPSPCE attribute is used for BitLocker.

If you use RSVDSPCE to set aside space for a RECOVERY partition, that partition can subsequently be created, initialized, and populated in one of two ways:
Using an OS Manager exit-point routine
Using a separate HPCA Service installed through the HPCA agent after the production OS is up and running</td></tr>
</table>

Table 11 RSVDSPCE and SYSPSPCE Behavior for Windows 7 and Windows Server 2008 R2

Type	RSVDSPCE Reserved Space Size	SYSPSPCE System Partition Size	Comments
REPLACE	Honored	Honored	
MERGE	Honored	Honored	See also Special Considerations for Dual-Partition Installations on page 143.
ADD	Honored	Honored	
CACHE	Honored	Not Applicable	OS installed in a single partition setup (no “System Reserved” partition).
PRES	Not Applicable	Not Applicable	No repartitioning done at all. Operating system partition is cleared with the exception of the Preserve directory.
Deploy CD Install OS from Cache	Not Applicable	Not Applicable	Requires prior OS deployment with DRIVEMAP type CACHE. OS is redeployed to the active OS partition.
Deploy CD Install OS from CD	Not applicable	Not Applicable	Wipes all partitions and installs the OS on a single partition.

Example 1 – Default values for HPCA Standard

RSVDSPCE = 0 SYSPSPCE = 1024

1 GByte System Partion	OS Partition (Windows 7)

Example 2 – Reserve 2 GByte for a RECOVERY Partition in a Dual-Partition Scenario

RSVDSPCE = 2048 SYSPSPCE = 1024

2 GByte Reserved Space	1 GByte System Partion	OS Partition (Windows 7)

Pre-Windows 7 Operating Systems

The following information pertains to the following operating systems:

- Windows XP
- Windows 2003
- Windows Vista
- Windows 2008

This information applies only to OS installations using ImageX and Windows Setup deployment methods (Windows PE Service OS only).

Table 12 RSVDSPCE and SYSPSPCE Behavior for Pre-Windows 7 OSs

Type	RSVDSPCE Reserved Space Size	SYSPSPCE System Partition Size	Comments
REPLACE	Honored (see Comments)	Not Applicable	RSVDSPCE is only honored for Windows Vista and Windows Server 2008. It is not applicable to Windows XP and Windows Server 2003.

Table 12 RSVDSPCE and SYSPSPCE Behavior for Pre-Windows 7 OSs

Type	RSVDSPCE Reserved Space Size	SYSPSPCE System Partition Size	Comments
MERGE	Honored (see Comments)	Not Applicable	RSVDSPCE is only honored for Windows Vista and Windows Server 2008. It is not applicable to Windows XP or Windows Server 2003.
ADD	Honored (see Comments)	Not Applicable	RSVDSPCE is only honored for Windows Vista and Windows Server 2008. It is not applicable to Windows XP or Windows Server 2003.
CACHE	Honored (see Comments)	Not Applicable	RSVDSPCE is only honored for Windows Vista and Windows Server 2008. It is not applicable to Windows XP or Windows Server 2003.
PRES	Not Applicable	Not Applicable	No repartitioning done at all. Operating system partition is cleared with exception of Preserve directory.
Deploy CD Install OS from Cache	Not Applicable	Not Applicable	Requires prior OS deployment with DRIVEMAP type CACHE. OS is redeployed to the active OS partition.

Table 12 RSVDSPCE and SYSPSPCE Behavior for Pre-Windows 7 OSs

Type	RSVDSPCE Reserved Space Size	SYSPSPCE System Partition Size	Comments
Deploy CD Install OS from CD	Not Applicable	Not Applicable	Wipes all partitions and installs OS on single partition.

Example 3 – Reserve 2 GByte in a Single Partition Scenario for Pre-Windows 7 OS

RSVDSPCE = 2048 SYSPSPCE = 1024

2 GByte Reserved Space	OS Partition (Windows Vista)

Special Considerations for Dual-Partition Installations

The OS Manager can install Windows 7 and Windows 2008 R2 (and later) operating systems using dual partitions or a single partition. The MERGE strategy works differently, however, depending on the values of the RSVDSPCE and SYSPSPCE attributes and the number of partition table slots available:

- If SYSPSPCE is greater than zero, one empty partition table slot is needed to create the System partition.
- Similarly, if RSVDSPCE is greater than zero, one empty partition table slot is needed to set aside the unallocated disk space.
- If both SYSPSPCE and RSVDSPCE are greater than zero, two empty partition table slots are needed to create the specified layout.
  - If no empty slots are available, neither the System partition nor the unallocated space will be created.
  - If only one empty slot is available, the unallocated space will be set aside, but the System partition will not be created.

For example, a single-partition Windows XP installation will be upgraded to a dual-partition Windows 7 installation with a 1 GByte System partition under the following conditions:

Example 1 – Single Partition Windows XP to Dual Partition Windows 7

RSVDSPCE = 0 SYSPSPCE = 1024 Empty partition table slots = 1

Original Layout:

OS Partition (Windows XP)	Data 1

New Layout:

1 GByte System Partition	OS Partition (Windows 7)	Data 1

If an empty partition table slot is not available, the OS Manager will create a single partition Windows 7 installation:

Example 2 – Same Upgrade, No Free Partition Table Slots

RSVDSPCE = 0 SYSPSPCE = 1024 Empty partition table slots = 0

Original Layout:

OS Partition (Windows XP)	Data 1	Data 2	Data 3

New Layout:

OS Partition (Windows 7)	Data 1	Data 2	Data 3

Example 3 – Single Partition Windows XP to Dual Partition Windows 7 with Unallocated Space

RSVDSPCE = 1024 SYSPSPCE = 1024 Empty partition table slots = 2

Original Layout:

OS Partition (Windows XP)	Data 1

New Layout:

1 GByte Reserved Space	1 GByte System Partition	OS Partition (Windows 7)	Data 1

If only one empty partition table slot is available, however, only the unallocated space will be set aside:

Example 4 – Same Upgrade, Only 1 Empty Partition Table Slot

RSVDSPCE = 1024 SYSPSPCE = 1024 Empty partition table slots = 1

Original Layout:

OS Partition (Windows XP)	Data 1

New Layout:

1 GByte Reserved Space	OS Partition (Windows 7)	Data 1

If no empty partition table slots are available, a single partition installation is implemented:

Example 5 – Same Upgrade, No Empty Partition Table Slots

RSVDSPCE = 1024   SYSPSPCE = 1024   Empty partition table slots = 0

Original Layout:

OS Partition (Windows XP)	Data 1

New Layout:

OS Partition (Windows XP)	Data 1

Specify the Drive Layout

Follow these instructions to specify your Drive Layout settings.

To specify a drive layout

1. In the CSDB Editor, go to PRIMARY.OS.DRIVEMAP.
2. Create a new instance.
3. Open the instance, and double-click **Type** to specify the type of partition that you want to create. The Editing window opens.
4. In the text box, type ADD, REPLACE, CACHE, MERGE, or PRESERVE (see Partitioning Strategies on page 134).
5. In the Editing window, click **RSVDSPCE**. Specify a value in MBytes.
6. Still in the Editing window, click **SYSPSPCE**. Specify a value in MBytes.
7. Click **OK**.

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

If you then add a second hard drive, the drive letter mappings are reassigned so that the primary partitions are in alphabetical sequence. For example:

Drive 1

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. In the CSDB Editor, go to PRIMARY.OS.PARTTION.
2. Create a new instance.
3. Open the instance.
4. Set the PARTTION class attributes as needed.

Table 13 PARTTION Class Attributes

Attribute	Description
PARINFO	Identifies the name of the partition.
SIZE	Specifies the partition size specified as a percentage of the hard drive or in MB. These values equal the total hard drive space.
UNITS	Indicates whether the partition size is being specified as a percentage or in megabytes.
FORMAT	Specifies whether to format the drive.
PARTYPE	Indicates the type of partition: NTFS, FAT32, EXT2, EXT3, or QNTFS. EXT2 and EXT3 are not supported under the WinPE Service OS. Note that QNTFS performs a quick format without zeroing out the partition.

5. Connect the PARTTION instance to the corresponding DRIVEMAP instance.

Assigning Drive Layouts

Once you have created your Drive Layout (DRIVEMAP), you must assign the appropriate drive layouts to your target devices based on policy such as machine manufacturer, model, role, or subnet.

To assign drive layouts

1. In the CSDB Editor, go to the appropriate POLICY instance, such as a SUBNET instance.
2. Connect the appropriate DRIVEMAP instance to the POLICY instance.

   In Core and Satellite environments, you will need to remove the DEFAULT_DRIVEMAP from the ROLE base instance. Only one connection is allowed.

   Remember that you can add, merge, replace, *or* cache partitions. You cannot do more than one of these things.

Using an Override Sysprep File

You can 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`. During the merge, the values in the override `Sysprep.inf` take priority. If a value is not specified in the override `Sysprep.inf`, the keyword will be removed.

In the [GUIRUNONCE] section of the `Sysprep.inf`, the lines in the file are merged based on their position in the file. Two edit functions are supported in this section. If you type a + in the override `Sysprep.inf`, it will keep the corresponding line from the embedded `Sysprep.inf`. If you type a - in the override `Sysprep.inf`, it will remove the corresponding line from the embedded `Sysprep.inf`.

Here is an example of a sysprep file that has been embedded in the image, an override sysprep file, and the result of the merge of these files using the edit functions.

Table 14 Example of Resulting Sysprep File Using Edit Functions

Sample of sysprep file in the image	Override sysprep file	Sample of resulting sysprep file

`[Unattended]`
`OemSkipEula = No`
`ExtendOemPartition = 0`
 	
`[Identification]`
`JoinWorkgroup = "WORKGROUP"`
 	
`[guirunonce]`
`C:\TEMP\KEEPRUNNINGTHIS.CMD`
`C:\TEMP\ANDRUNTHIS.CMD`
`C:\TEMP\STOPRUNNINGTHIS.CMD`
	`[Unattended]`
	`OemSkipEula = Yes`
	`ExtendOemPartition = 1`
	
	`[Identification]`
	`JoinWorkgroup =`
	`JoinDomain = "TESTDOM1"`
	
	`[guirunonce]`
	`+`
	`C:\TEMP\RUNTHISONETOO.CMD`
	`-`
	`C:\TEMP\STOPRUNNINGTHIS.CMD`
		`[Unattended]`
		`oemskipeula=Yes`
		`extendoempartition=1`
		
		`[Identification]`
		`joindomain="TESTDOM1"`
		
		`[guirunonce]`
		`C:\TEMP\KEEPRUNNINGTHIS.CMD`
		`C:\TEMP\ANDRUNTHIS.CMD`
		`C:\TEMP\RUNTHISONETOO.CMD`

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 Publishing on page 97.

3 Use the CSDB Editor to connect the PRIMARY.OS.SYSPREP instance to the appropriate OS (PRIMARY.OS.ZSERVICE instance). 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 displayed in the Enterprise Manager 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.

8 Implementing the OS Manager Server

This chapter includes the following topics:

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

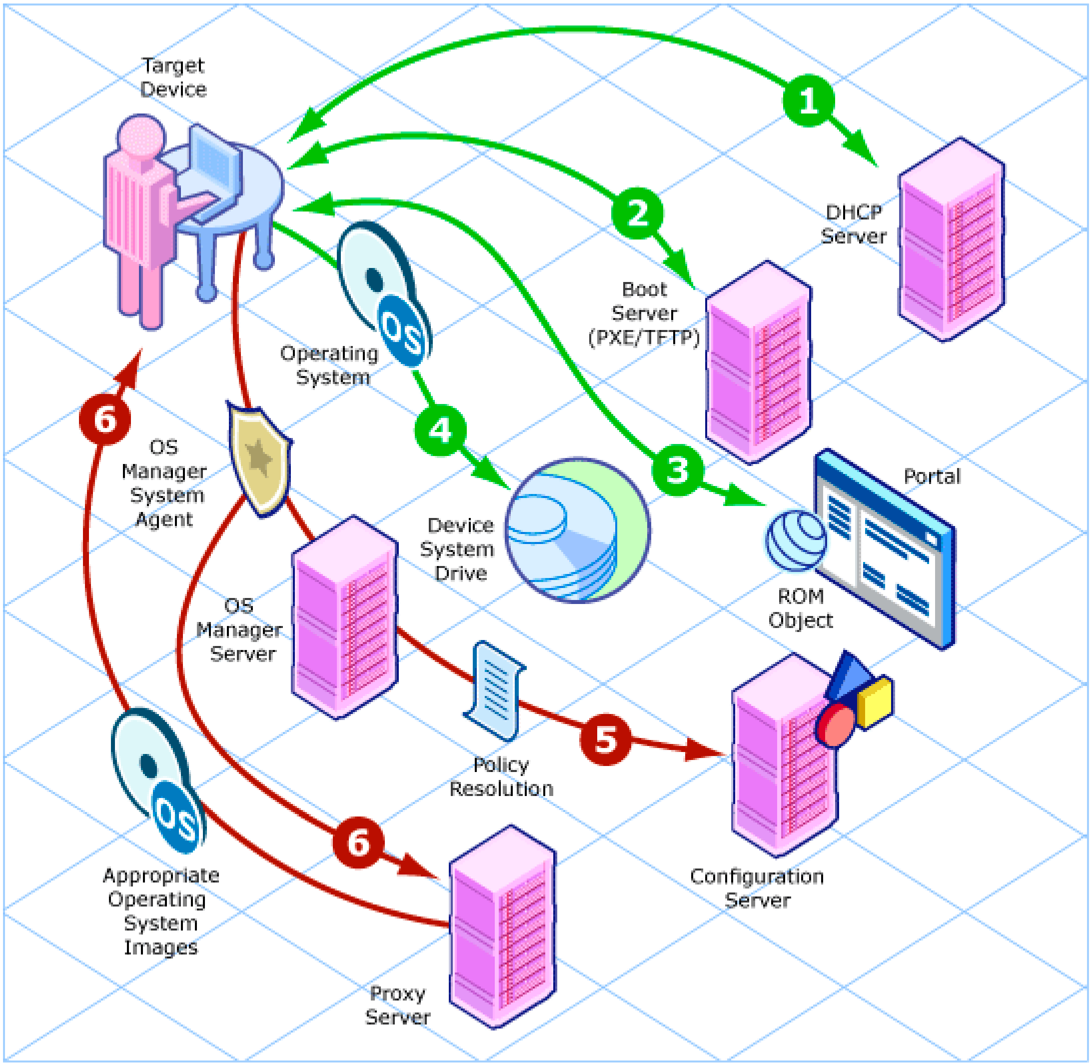
If you already have Client Automation implemented in your environment and want to use a PXE-based environment for the OS Manager, we recommend the following:

1 Install the OS Manager Server infrastructure before making any changes to your target devices. See Installing and Configuring the Server on page 45.

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



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 Software Support web site for product updates and release notes. See Support on page 10.

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 COP with OS Manager on page 199.

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 Installing and Configuring the Server on page 45.
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:3466`

The OS Manager Server port used for OS imaging and deployment in an HPCA Core and Satellite installation is 3466. In an HPCA Classic installation, port 3469 is reserved for this purpose.

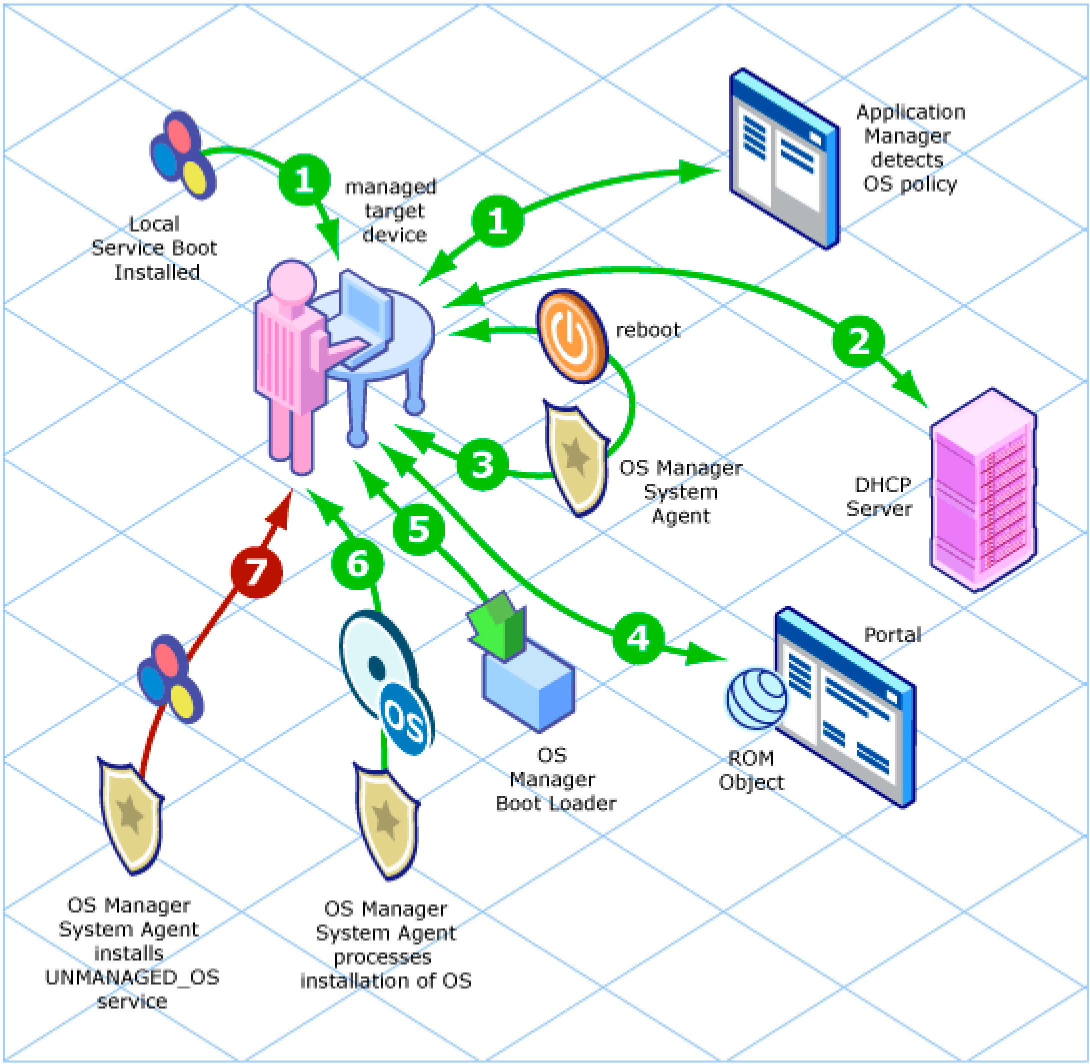
The value of the URL must be in lowercase text; otherwise the Local Service Boot will fail.

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



Booting with Local Service Boot – Process Flow:

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 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 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 Software Support web site for product updates and release notes. See Support on page 10.

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 on the Enterprise Manager, use the OS Deployment Wizard.

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 HP Professional Services to determine what is best for your environment.

9 Multicast and the OS Manager

This chapter includes the following topics:

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.

Prerequisites

- An understanding of the Multicast Server.
- A basic understanding of the OS Manager.

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.

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 15 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 the following file as needed:

```
SystemDrive:\Program Files\Hewlett-Packard\CM\
MulticastServer\etc\mcast.cfg
```

— `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. You may want to set `minref=1` for debugging purposes.

— `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 this folder:
>
> `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 16 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
`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. 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. A block contains a number of packets. The size of a block is defined by the `numpktblks` parameter described below.	4098

Table 16 Multicast Parameters

Parameter	Used By	Definition	Default Value
`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
`pktsperblk`	Sender or Receiver	Specifies the number of packets within a resend block. 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. 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. Specifies how often to check to see if the inter-packet delay should be adjusted.	8
`throthighth`	Sender	Throttle high threshold. The number of average resends per block that will trigger an increment of the inter-packet delay.	-1 (disabled) Note: To enable this, set it to a positive integer.

Table 16 Multicast Parameters

Parameter	Used By	Definition	Default Value
`throtincr`	Sender	Throttle increment. The value, in milliseconds, that is automatically added to (or subtracted from) the current inter-packet delay each time the throttle is adjusted. See Auto Throttle on page 175 for more information.	0.01
`throtlowth`	Sender	Throttle low threshold. The number of average resends per block that will trigger a decrement of the inter-packet delay.	-1 (disabled) Note: To enable this, set it to a positive integer.
`throtmax`	Sender	Throttle maximum. The maximum inter-packet delay, in milliseconds, that can be set by the throttle.	0.5
`throtmin`	Sender	Throttle minimum. The minimum inter-packet delay, in milliseconds, that can be set by the throttle.	0.0
`ttl`	Sender	Time to live. The number of subnets that the packet will reach. 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. 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 file, `gdmcsend.log`, is typically stored here:

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.

b. 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.

c. 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:

- **Total image transfer time-out** occurs when the total time it takes to transfer the image exceeds the value of the recvtimeout parameter.
- **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 176, can be used to identify and resolve the problem.

Network Inactivity Time-Out

A log file message in the following form is indicative of a network inactivity time-out:

```
Inactivity timeout has been exceeded.
```

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.

In the following folder on the installation media, there is a script called `gdmsend.cmd` that can be used for testing:

```
Infrastructure\extended_infrastructure\multicast_server\
multicast_test_modules\
```

To start the multicast test sender module

1. Copy the multicast test send modules (`gdmcsend.exe`, `gdmcsend.cmd`, and `TESTDATA0004`) from the following directory on the infrastructure CD to a temporary directory:

   `extended_infrastructure\multicast_server\multicast_test_module`

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 191.

When setting values for parameters that apply to both `gdmcsend` and `gdmrecv`, the values must match.

The following 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 17 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

Table 17 gdmcsend Command Options

Option	Corresponding parameter in mcast.cfg	Description	Default
-lc *n*	`lingercount`	Linger count. The number of times to check for resend requests (NACKs), after the last packet has been sent.	256
-lf *log_file*	N/A	The name of the log file. The log file is stored in the directory where you execute the command. 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

Table 17 gdmcsend Command Options

Option	Corresponding parameter in mcast.cfg	Description	Default
-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
-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. 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

Table 17 gdmcsend Command Options

Option	Corresponding parameter in mcast.cfg	Description	Default
-rm F|B|D	N/A	Resend mode. **F = fixed** Each packet block is resent a fixed number of times (as specified by the **-nr** option). **B = backup** Resend all blocks from the lowest number requested to the current block (last block sent by the sender). **D = discrete** Resend only requested blocks.	B
-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

Table 17 gdmcsend Command Options

Option	Corresponding parameter in mcast.cfg	Description	Default
-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. 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 191.

When setting values for parameters that apply to both gdmcsend and gdmrecv, the values must match.

The following are two sample commands. 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 18 gdmcrecv Command Options

Option	Corresponding Parameter in meast.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
-lf *log_file*	N/A	Name of log file. The log file is stored in the directory where you execute the command. 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

Table 18 gdmcrecv Command Options

Option	Corresponding Parameter in meast.cfg	Description	Default
-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
-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

Table 18 gdmcrecv Command Options

Option	Corresponding Parameter in meast.cfg	Description	Default
`-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).	

Table 18 gdmcrecv Command Options

Option	Corresponding Parameter in meast.cfg	Description	Default
`-rm F|B|D`	N/A	Resend mode. **F = fixed** Each packet block is resent a fixed number of times (as specified by the -nr option). **B = backup** Resend all blocks from the lowest requested to the current. The receiver will only send resend requests (NACKs) for the lowest block needed. **D = discrete** 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

This chapter includes the following topics:

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-requisites

- The ImageDeploy media. See Product Media on page 34 for 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 is 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 Partitioning Strategies on page 134), 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 created a CD or DVD (using either the `osm-deployment.tcl` script or the **Create CD Deployment** task in the HPCA console), 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, you can use the HPCA Personality Backup and Restore utility or command-line interface. Refer to “Personality Backup and Restore” in the *HPCA Core and Satellite Enterprise Edition User Guide* (or the HPCA console online help).

In addition, HP provides the ROM Client method (`romclimth.tkd`), which has two exit points. This method is stored in *`InstallDir`*`\Agent`.

The exit points call two optional scripts:

- `Novapdc.cmd` (data capture)
- `Novapdr.cmd` (data restore)

These scripts must also be stored in *InstallDir*\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 *InstallDir*\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.

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 19 HP Exit Point Return Codes

<table>
<tr><th>Code</th><th>Description</th></tr>
<tr><td>0</td><td>Sucessful</td></tr>
<tr><td>1</td><td>An error occurred and will be logged, but processing will continue. The log is located in:
<code>SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log</code>.</td></tr>
<tr><td>2</td><td>For <code>Novapdc.cmd</code> (capture):
A fatal error has occurred and will be logged here:
<code>SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log</code>.
Processing of the service has ended.
For <code>Novapdr.cmd</code> (restore):
An error has occurred and will be logged here:
<code>SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log</code>.
The service is flagged, but at the next HPCA OS connect, the Application Manager will attempt to install the service again.</td></tr>
</table>

Using COP with OS Manager

HP Client Automation Client Operations Profiles (COP) 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 Profiles (SAPs) so that managed devices can access alternate sources for image download is an 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 Customizing OS Deployment by Using Exit Points and Add-Ons

This chapter contains the following topics:

HPCA provides two features that you can use to dynamically customize your OS deployments:

- **Add-On Packages** enable you to deploy arbitrary sets of data during image deployment.
- **User Exit Points** enable you to execute custom code at various stages of the deployment

These feature can be used in both ImageX and Windows Setup deployments. They enable you to build a more flexible and controlled OS deployment environment, where static OS images can be transformed during deployment to meet the complex requirements of your enterprise.

For example, you can use these features to inject drivers during the OS deployment. To do this, you must:

1. Publish the drivers as described in Publishing OS Add-Ons and Extra Production OS (POS) Drivers on page 107.
2. Use either Windows Setup or ImageX for deployment.
3. For Windows Setup deployments, use an `unattend.xml` file that contains a reference to `C:\osmgr.hlp\drivers`. The sample `unattend.xml` files provided by HPCA contain this reference.

   For ImageX deployments, a reference to `C:\osmgr.hlp\drivers` is added to the registry on the reference machine before the OS image is captured.

User Exit Points

Although exit points provide a way to customize OS deployments, extreme caution needs to be exercised when implementing such exit points. You must take care not to interfere with the HPCA OS deployment. Thorough testing of such custom solutions is mandatory

In addition to the existing Personality and Data Capture exit points, the OS Manager has enabled several new, formal exit points to allow customization of the OS deployment process. These exit points are defined for the following purposes, but could be used for alternative processing. The following table details when they are run:

- Before disk partitioning occurs

- Before the OS and its resource files are downloaded
- Before the OS will be installed
- After the OS has been installed but before the reboot occurs

Add-On Methods

HPCA also allows for methods and/or data to be downloaded to the service OS RAM drive or to the production OS during image installation. This data is called Add-On. Any number of Add-On methods can be run during the deployment.

Add-Ons are typically used to dynamically inject non-critical device drivers into a Vista, Windows 2008 Server or later OS image prior to its deployment, but they are not limited to such use. They are enabled by simply publishing one or more files using a new ADD-ON publish feature in the Publisher.

Drivers (or other methods) must be published. After publishing, the Add-On package is connected to a Service. Formal exit-point command files are also published as an Add-On and connected to the appropriate Service. The Publisher has been extended to allow a formal publishing session to the OS Manager ADDON class. Refer to Publishing OS Add-Ons and Extra Production OS (POS) Drivers on page 107.

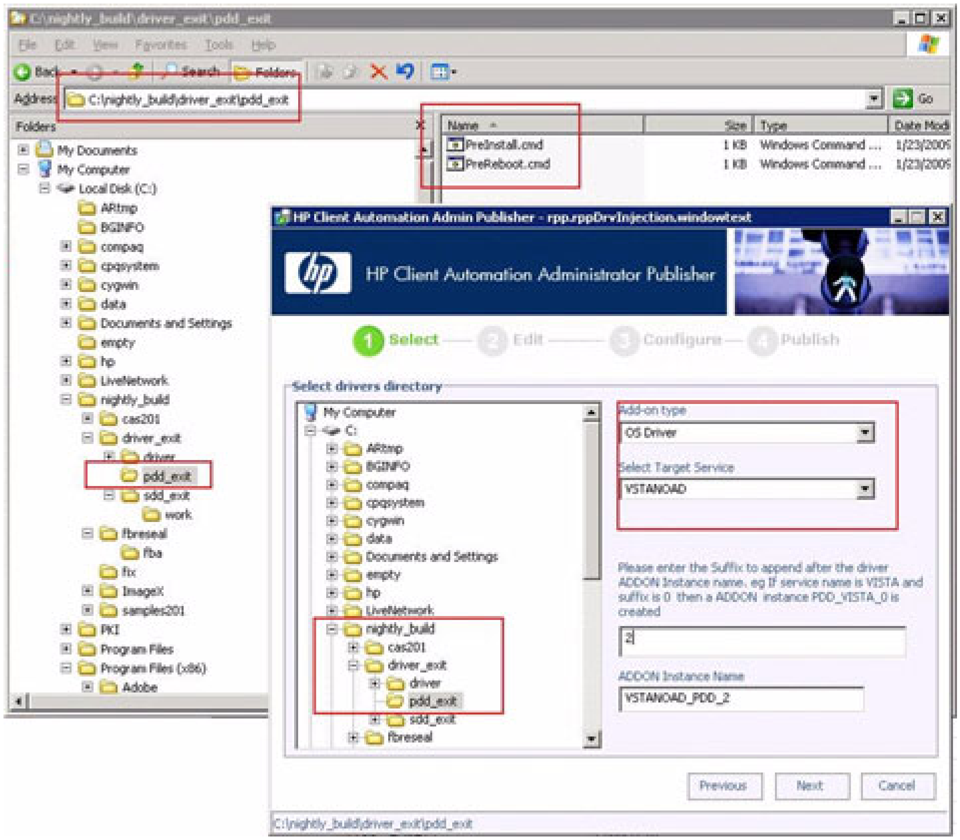
The Add-Ons feature is integrated with the normal image deployment process. Published Add-Ons are downloaded as needed along with the Service's resources. The Service OS Add-Ons are downloaded before Production OS Add-Ons.

Add-Ons that run in the Service OS have the extension `.sdd` (Service aDD-on), and Add-Ons that run under the Production OS use the `.pdd` extension (Production aDD-on). Both `.pdd` and `.sdd` files are created as TAR files (compressed archive in `.tar` format with path-information).

Exit Point and Add-On processing can be used with ImageX and Windows Setup deployment methods.

Publishing Add-On Methods

The HPCA Publisher now has a drop-down option to publish an OS ADDON. Choose this option when publishing Service OS or Production OS methods and any associated data, like device drivers.



Add-Ons are published to the Configuration Server Database (CSDB) into the OS.ADDON class as new instances that are connected to an OS ZSERVICE. Publishing always occurs for a specific OS service. The wiring is done automatically.

For new installations of HPCA version 7.50 and later, the wiring setup is done as part of the creation of a new OS service. For migrated environments, administrators will need to connect the service and any associated ADD-ONs manually.

Deployment of the OS is triggered by launching an OS Deployment job.

- In a classic installation, jobs are managed through the Enterprise Manager. Refer to "Managing Operating Systems" the *HPCA Enterprise Manager User Guide* for more information.
- In a Core and Satellite installation, jobs are managed using the HPCA Console. Refer to "OS Management" in the *HPCA Core and Satellite Enterprise Edition User Guide*.

Add-Ons and user exits points are processed during the OS deployment process.

Agent Execution of Add-On Methods

Service OS Add-On (`.sdd`) files are downloaded and extracted into the root of `X:\` (typically the local RAM drive in the Windows PE service OS) as the first step of the install WIM phase. The OS Manager Agent aborts if the available free-space on this drive drops below 20 MB while downloading and extracting any `.sdd` files.

Production OS Add-On (`.pdd`) files—for example, device driver files—are downloaded and extracted into the root of the new OS partition, always `c:\`, after downloading the `.WIM`. When computing the size for the new OS partition, the OS Manager Agent will take into consideration the uncompressed size of all resolved `.pdd` archives (from the ADDON resource meta-data attribute ZRSCSIZE). Each `.pdd` file is stored and named after its object-ID and not the original name it was published as. The agent executes user-provided exit-point scripts during its normal flow of operation if well-known exit-point specific script files exist after `.sdd`/`.pdd` extraction.

The processing sequence for a typical OS Management deployment follows the sequence below when installing an OS. Note that if an exit point is defined to reside in both the `X:\work` and `C:\`, then the exit method will be called twice. Be certain to publish a directory structure that contains a `\work` subdirectory (see examples above).

Add-Ons are extracted in the order they are resolved by the Configuration Server. There is no sequencing. All exit-point scripts are first being searched for in `X:\Work` and executed if available.

- Service OS methods, `.sdd` extensions, run from the `x:\` drive

- Production OS methods, `.pdd` extensions, run from the `c:\` drive

➤ Exit points and any associated data is NOT deleted automatically.

Agent Execution of Add-On Methods – Important Information

- Exit-point execution and error-handling is similar to LME Apply-method execution.
- After looking for and executing either the `PreInstall.cmd` and `PreReboot.cmd` exit points in the `X:\Work` directory, the agent will also look under `C:\osmgr.hlp` directory and executes exit points found in this directory in addition to the exit points in the `X:/Work` directory.
- The agent does a drive-/partition re-synch after having run `PrePartition.cmd` and `PreDownload.cmd`.
- The HPCA Publisher is extended to create new OS.ZSERVICE instances of deployment-types ImageX and Windows Setup with a connection to OS.ADDON.PDD_<Servicename>_* by default
- The tar archive(s) published as PDD_<Servicename>_<Suffix> will be used as Production OS Add-On(s) (for example, for additional drivers) without the need to use the CSDB Editor for standard cases. The <Suffix> should be used to classify Add-Ons.
- Using the CSDB Editor, there can be more `.pdd` and/or `.sdd` ADDON connections and the standard OS.ADDON.PDD_<Servicename>_* connection can be replaced by something more selective (for example, leveraging model information)
- For publishing type Production OS add-ons, optionally ask for a corresponding service name/suffix and create an instance name in the form of PDD_<Servicename>_<Suffix>.
- The directory `C:\osmgr.hlp\drivers` is the suggested additional driver library location. Each driver .pdd ADDON needs to extract its contents into one driver-/driver-and-version specific subdirectory under `C:\osmgr.hlp\drivers`.

  The current `unattend.xml` template will be changed to always include the `C:\osmgr.hlp\drivers` directory in the search-path for Plug-and-Play drivers.

For captured images, the `C:\osmgr.hlp\drivers` directory will have been added to the registry before capturing (in HPCA version 7.9 and later).

Subdirectories below `C:\osmgr.hlp\drivers` must not contain multiple dots in their names!

- Older, pre-existing OS services need to re-publish their `unattend.xml` template (to add the driver path) and add the OS.ADDON.PDD_<Servicename>_* connection to leverage driver-injection.

  As an alternative to re-publishing the modified `unattend.xml` template, a sample `PreInstall.cmd` script could be provided (and added to any `.pdd` package) to extend the PnP search-path for `C:\osmgr.hlp\drivers` by modifying the xml file on the fly.

OS Deployment Processing Using User Exits

There are 3 phases during a normal deployment process:

- Pre-OS deployment phase where pertinent information is extracted from the device prior to its being provisioned
- OS deployment phase
- Post-OS deployment phase where the machine may be added to a directory and any extracted information is restored

Pre-OS Deployment Phase

You can use the HPCA Personality Backup and Restore feature to capture user files and settings for later restoration after the device has had its OS provisioned. See Personality Backup and Restore on page 213 for more information.

OS Deployment Phase

1 Start Service OS

2 User exit: `PrePartition.cmd`

- Runs before partitioning is completed (ImageX or Windows Setup only)
- `PrePartition.cmd` can be defined as a Service OS Add-On (`.sdd`). It cannot be defined as a Production OS Add-On (`.pdd`).
- Typically used to partition disk drive(s). Agent does a drive-/partition re-synch after having run PrePartition.cmd user exit.
- OS is not available
- Network is available
- RAM drive of the WinPE service OS is available

  You can use the environment variable SystemDrive to find the drive letter of the Windows PE RAM drive.

3 Partition Disk Drive(s)

4 User exit: `PreDownload.cmd`

- Runs after partitioning, before downloading/extracting OS and other resource files
- `PreDownload.cmd` can be defined as a Service OS Device Driver (`.sdd`) Add-On. It cannot be defined as a Production OS Device Driver (`.pdd`) Add-On.
- May be used to modify the environment after the disk has been partitioned
- Agent does a drive-/partition re-synch after running PreDownload.cmd user exit.
- OS is not available
- Network is available
- RAM drive of the WinPE service OS is available

5 Download OS and other resource files

6 User exit: `PreInstall.cmd`

- Runs after downloading/extracting resource files and before running Windows Setup or ImageX extract that installs the OS
- `PreInstall.cmd` can be defined as a Service OS Add-On (`.sdd`) or a Production OS Add-On (`.pdd`).
- May be used to customize the environment before the OS has been installed (for example, Customize OS install configuration files or add or replace OS files)
  - Could be used to replace the `install.wim` file from the Configuration Server with one from another location, if desired
- OS is not available
- Network is available
- RAM drive of the WinPE service OS is available

7. Install OS using ImageX or Windows Setup
8. User exit: `PreReboot.cmd`
   - Runs after Windows Setup returned or ImageX extract and before triggering reboot
   - `PreReboot.cmd` can be defined as a Service OS Add-On (`.sdd`) or a Production OS Add-On (`.pdd`).
   - May be used to modify the environment after the OS has been installed and to prepare for methods to be run immediately or after the reboot has occurred (for example, Registry run or runonce keys)
   - WinPE OS is available and is the running OS
     - Facilities and interfaces limited to what is provided by the WinPE service OS. Refer to the Windows AIK for WinPE features and limitations.
     - Native OS is installed, but not yet actively running
     - SYSPREP has not yet run
   - Network is available
   - RAM drive of the WinPE service OS is available
9. Reboot device
10. Post-reboot device start-up
    - Completes native OS installation

    - Runs SYSPREP
    - Install HP Client Automation Agent (runsync)
    - HPCA Agent runs first connect to Configuration Server
        - Metadata download
        - OS Manager client methods are run
        - OS state set to _DESIRED_
        - Runs User exit: `novapdr.cmd` - Optional
            - Typically used to restore user files and personality captured before the device was provisioned.
- Full native OS is available (for example, Vista)
- Network is available

12 Personality Backup and Restore

The HPCA Personality Backup and Restore solution enables you to back up and restore user files and settings for applications and operating systems on individual managed devices. Files and settings are stored on the HPCA Core server and are available for restoration to the original device or a new device. Alternatively, you can back up and restore files and settings locally on a managed device.

You can use the HPCA Personality Backup and Restore solution to migrate files and settings as part of an operating system deployment.

The HPCA Personality Backup and Restore solution is based on the Microsoft User State Migration Tool (USMT). It enhances USMT by providing both remote and local management of the migration store created by USMT. It also downloads the required USMT control files to eliminate the need to deploy those separately. HPCA supports USMT versions 3.0.1 and 4.0.

➤ Backups created with versions of HPCA prior to HPCA 7.5 cannot be restored, because they were based on a different backup technology.

The following sections explain how to implement the HPCA Personality Backup and Restore solution in your environment.

- Requirements on page 213
- About USMT on page 215
- Using Personality Backup and Restore on page 220
- Troubleshooting on page 228

Requirements

Before you implement the Personality Backup and Restore solution, make sure that your environment meets the following requirements.

- Operating System on page 214
- Disk Space on page 214
- Software on page 215

Operating System

You can create backups from source computers with the following operating systems:

- Windows 2000 Professional Service Pack 4 or later
- Windows XP
- Windows Vista
- Windows 7

You can restore files and settings to destination computers with the following operating systems:

- Windows XP
- Windows Vista
- Windows 7

Disk Space

Before you begin, you must make sure that your source computer, destination computer, and the HPCA Core server have adequate disk space to store the files and settings that will be backed up. To estimate the disk space that will be needed for the backup, refer to "Determine Where to Store Data" on the Microsoft TechNet web site at the following URL:

http://technet.microsoft.com/en-us/library/cc722431.aspx.

Note that the storage location is automatically set by HPCA, and each of the source computer, destination computer, and HPCA Core server must have adequate disk space available for the files and settings being migrated.

Also note that the destination computer needs to have twice the disk space required by the files and settings being migrated.

If you use the HPCA Personality Backup and Restore Utility, the HPCA Core server stores the archived user files and settings that were created during the backup. During a restore, the archived files and settings are downloaded to a temporary location on the destination computer and then restored to their original location. After a successful restore, the archived files and settings are deleted from the destination computer.

If you use the `pbr.exe` command with the `/localstore` option, backups are stored locally on the disk under `C:/OSMGR.PRESERVE/PBR.work`. The backups are not deleted, because they are the only copy of those files.

Software

You need the following applications:

- **Microsoft USMT version 3.0.1 or 4.0**
  This application must be installed in the default location on the source and destination devices. See the About USMT.

  This solution requires that you use Microsoft USMT version 3.0.1 or version 4.0. No other versions of USMT are supported.

- **HP Client Automation Personality Backup and Restore**
  This application must be installed on both the source and destination devices. It is installed automatically when the HPCA agent is installed on a managed device.

About USMT

Because the HPCA Personality Backup and Restore solution is based on the Microsoft User State Migration Tool (USMT), you should become familiar with this tool and its capabilities by reviewing its documentation on the Microsoft Technet web site at the following URL:

http://technet.microsoft.com/en-us/library/cc722032.aspx.

This section describes Microsoft USMT; how to obtain it, install it, and how to use its migration files. For a description of the Hewlett-Packard user interface provided with the Personality Backup and Restore solution, which invokes USMT automatically during a backup and restore, see Using the HPCA Personality Backup and Restore Utility on page 221.

Supported Files, Applications, and Settings

USMT migrates a wide variety of data including user files and folders (e.g., the My Documents folder on XP or the Documents folder on Vista), operating system settings (e.g., folder options and wallpaper settings), and application settings (e.g., Microsoft Word settings). For a comprehensive list see "What does USMT 3.0 Migrate?" on the Microsoft TechNet web site at the following URL:

http://technet.microsoft.com/en-us/library/cc722387.aspx

Also see "What's New in USMT 4.0?" at the following URL:

http://technet.microsoft.com/en-us/library/dd560752(WS.10).aspx

➤ For application settings to migrate successfully, the version of an application should be identical on the source and destination computers. There is one exception. You can migrate Microsoft Office settings from an older version on a source computer to a newer version on a destination computer.

➤ USMT only migrates application settings that have been accessed or modified by the user. Application settings that have not been accessed by the user on the source computer may not migrate.

➤ Some operating system settings, such as fonts, wallpaper, and screen saver settings, are not applied until after a reboot on the destination computer.

Obtaining and Installing Microsoft USMT 3.0.1 or 4.0

You might want to install USMT for one or both of the following reasons:

- As an administrator, you want to become familiar with the capabilities of USMT and to learn how to customize the migration rules for your personalized solution.
- As an end user, you want to be able to back up and restore files and settings on managed devices.

If you want to implement Personality Backup and Restore, you must install Microsoft USMT 3.0.1 or 4.0 on the source computer for backup, and on the destination computer for restore. This section explains where you can obtain this application, and how to install it.

You must use Microsoft User State Migration Tool, version 3.0.1 or 4.0. No other versions of USMT are supported.

Obtaining Microsoft USMT 3.0.1

USMT 3.0.1 is available at the Microsoft Download Center:

http://www.microsoft.com/downloads

There are two versions: 32-bit and 64-bit. Select the appropriate version for your environment.

Obtaining Microsoft USMT 4.0

USMT 4.0 is part of the Windows Automated Installer Kit (AIK) for Windows 7, which is available at the Microsoft Download Center:

http://www.microsoft.com/downloads

There are two versions: 32-bit and 64-bit. Select the appropriate version for your environment.

Installing Microsoft USMT on Managed Devices

You can install USMT on managed devices in two ways. You can install it manually, or you can package it into a service using the HPCA Administrator Publisher (see Publishing on page 97) and then entitle or deploy it to managed devices. USMT must be installed in the default location on both the source and destination client devices:

Table 20 Default USMT Installation Locations

USMT Version	Default Location
3.0.1	`C:\Program Files\USMT301`
4.0	`C:\Program Files\Windows AIK\Tools\USMT`

Be certain to install the appropriate version (32-bit or 64-bit) based on the operating system of the managed device.

Migration Files

The Personality Backup and Restore solution uses the following three USMT migration files to specify the components to include in the migration.

- `MigSys.xml` – migrates operating system settings
- `MigApp.xml` – migrates application settings
- `MigUser.xml` – migrates user folders and files

Before you implement this solution in your environment you must obtain these files and store them on the HPCA Core Server (see Storing the Migration Rules on the Core Server on page 218).

To obtain these files you must install USMT on one of its supported platforms (see Obtaining and Installing Microsoft USMT 3.0.1 or 4.0 on page 216). The installation places these files in the directories shown in Installing Microsoft USMT on Managed Devices on page 217.

You can then edit these files (see Editing the Rules on page 218) or use them as is.

Editing the Rules

In some instances you may want to edit the default migration rules. For example, you may not wish to migrate settings for a particular application or may want to exclude a particular file type. To modify the default migration behavior, you need to edit the migration XML files. Refer to the following document to learn how to customize these files:

http://technet.microsoft.com/en-us/library/cc766203.aspx

Storing the Migration Rules on the Core Server

When you are finished editing the migration files—or even if you choose not to edit them—save the files in the following folder on the HPCA Core server:

`DataDir\PersonalityBackupAndRestore\conf`

Here, *DataDir* is the user-configurable data directory specified during the HPCA Core installation.

The migration files must have the same file names as the original files obtained from the Microsoft USMT 3.0.1 or 4.0 installation: `MigSys.xml`, `MigApp.xml`, and `MigUser.xml`.

ScanState and LoadState Command Lines

The migration rules are downloaded from the Core Server by the Personality Backup and Restore Utility and are used by the USMT executables ScanState and LoadState that collect and restore the personality data. `ScanState.exe` is the executable that collects personality data on the source computer. Here is the ScanState command line that is used by the Personality Backup and Restore Utility:

```
ScanState.exe /i:MigApp.xml /i:MigUser.xml /i:MigSys.xml /o
/l:ScanState.log /localonly “Agent\Lib\PBR\work\store”
```

where *Agent* is the agent's installation directory.

LoadState is the executable that restores the personality data to the destination computer. Here is the LoadState command line that is used by the Personality Backup and Restore Utility:

```
LoadState.exe /i:MigApp.xml /i:MigUser.xml /i:MigSys.xml /
l:LoadState.log /lac:password /lae
“Agent\Lib\PBR\work\store”
```

Here, *Agent* is the agent's installation directory.

These command lines are not customizable, but are provided here to facilitate your understanding of what is being backed up and restored. Note that these ScanState and LoadState command line arguments automatically migrate all user accounts on a system, including local user accounts. If, when the restore is performed, a local user account does not exist on the destination computer, LoadState will create it with a password of `password` (see command line above). Therefore, after the restore, you should change the password of any restored local user accounts.

Using Personality Backup and Restore

There are three ways that you can access the HPCA Personality Backup and Restore feature:

- Using the HPCA Personality Backup and Restore Utility on page 221
- Using the Personality Backup and Restore Services on page 226
- Using the Command Line Interface on page 225

All three methods invoke the same HPCA application, which is called `pbr.exe`. Each time that `pbr.exe` runs, it downloads the three migration XML files (see Migration Files on page 218) from the HPCA Core server to the managed device and uses these files to perform the backup or restore.

By default, `pbr.exe` stores the backup files on—and restore them from—the following location on the HPCA Core server:

`DataDir``\PersonalityBackupAndRestore\backups`

Here, *`DataDir`* is the data directory specified during the installation of the HPCA Core. A subdirectory is created under the `backups` folder for each managed device that is backed up, and it contains all of the information that is required for a restore.

If you want to store the backup files on the local hard disk of the managed device instead of on the HPCA Core server, you can use the `pbr.exe` command with the `/localstore` option. In this case, the files are stored on the local disk in the following location:

`C:/OSMGR.PRESERVE/PBR.work`

All of the information that is required for a restore is stored in this location.

See Using the Command Line Interface on page 225 for details.

Whether the backup files are stored on the HPCA Core server or the local hard disk of a managed device, they are never automatically deleted. If backup data for a particular device is no longer needed, that backup data can be deleted manually by the HPCA administrator

Using the HPCA Personality Backup and Restore Utility

The HPCA Personality Backup and Restore Utility is a user interface that simplifies the usage of USMT. The Utility is deployed to managed devices when the HPCA agent is installed.

Before you begin, make sure you have enough disk space available on the HPCA Core server and on both the source and destination computers (see Disk Space on page 214.)

To start the Personality Backup and Restore Utility:

On the managed client device, use the Start menu, and go to:

All Programs > **HP Client Automation Personality Backup and Restore** > **Client Automation Personality Backup and Restore Utility**

The following sections explain how to use the Utility:

- Personality Backup on page 221
- Personality Restore on page 223

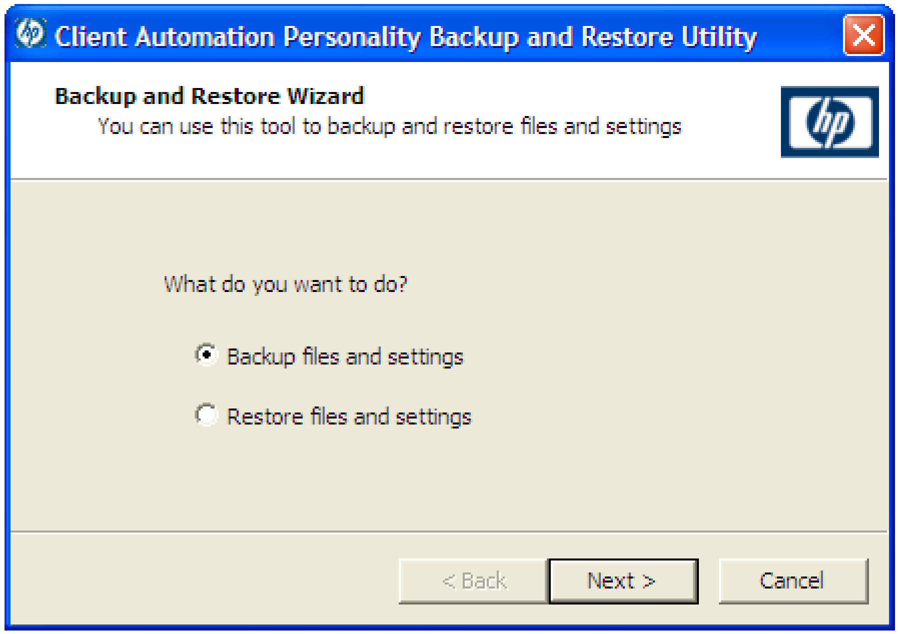
Personality Backup

You must run the Personality Backup and Restore Utility from a user account with administrator privileges.

To help ensure a successful backup, close as many open files and running applications as possible before you run the backup . Do not launch new applications or open files while the backup is running, as this can cause the backup to fail.

To back up files and settings:

1 On the managed device, start the Personality Backup and Restore Utility (see page 221).



2 Select **Backup files and settings**, and click **Next**. The Backup dialog box opens.

3 Enter the computer name of the device that you want to back up.

4 Enter a password that is at least 7 but no more than 15 characters long, and click **Next**. The summary dialog box opens.

5 Review the summary information. Make a note of the computer name and password that you use, as you will need this information to restore your files and settings.

6 Click **Finish** to begin the backup process. Depending on the amount of data to be backed up, this process can take from a few minutes to several hours to complete. Wait for the Personality Backup and Restore Utility to indicate that the backup has completed before you close the application.

Personality Restore

You must run the Personality Backup and Restore Utility from a user account with administrator privileges.

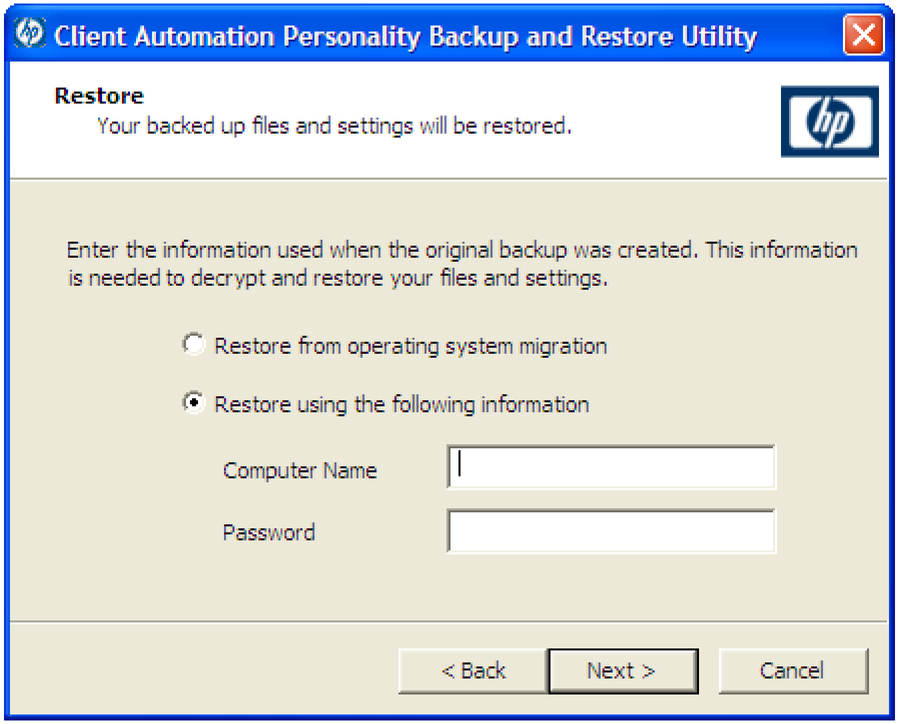
To help ensure a successful restore, close as many open files and running applications as is possible before you run the restore. Do not launch new applications or open files while the restore is running, as this can cause the restore to fail.

Before you begin the restore procedure, you must install (on the destination computer) all applications that have settings to be migrated. Note that for all applications other than Microsoft Office (where a newer version is allowed), the same application version must be installed on the destination computer as was installed on the source computer.

You should do a restore to a computer on the same Windows domain that was used for the backup. You should also do a restore to the same locale (for example, US English) that was used for the backup.

To restore files and settings

1. On the destination computer, start the Personality Backup and Restore Utility (see page 221 for instructions).
2. Select **Restore files and settings** and click **Next**. The Restore dialog box opens.



3 Perform one of the following actions:

— To restore files and settings that were backed up using the Personality Backup and Restore Utility, follow these steps:

a Select **Restore using the following information**.

b Type the **Computer Name** and **Password** that were used during the backup.

— To restore files and settings that were stored during the last operating system deployment for which migration was enabled, select **Restore from operating system migration**.

4 Click **Next**. The Summary dialog box opens.

5 Click **Finish** to begin the restore process. Depending on the amount of data to be restored, this process can take from a few minutes to several hours to complete. Wait for the Personality Backup and Restore Utility to indicate that the restore has completed before you close the applcation.

6 Since some operating system settings, such as fonts, wallpaper, and screen saver settings, are not applied until after a reboot on the destination computer, you should now perform a reboot to ensure that all these settings are successfully applied.

Using the Command Line Interface

You can use the HPCA Personality Backup and Restore command line interface to backup and restore files and settings for a managed device.

The syntax is as follows:

`InstallDir\Agent\pbr.exe /B|/R [/localstore]`

Here, `InstallDir` is the location where the HPCA agent is installed. By default, this is `C:\Program Files\Hewlett-Packard\HPCA`.

Use the `/B` option to perform a backup and the `/R` option to perform a restore.

Example 1: Backup your files and settings on the HPCA Core server

`InstallDir\Agent\pbr.exe /B`

Example 2: Restore from the HPCA Core server

`InstallDir\Agent\pbr.exe /R`

You can use the `/localstore` option to perform a local backup or restore operation. In this case, the user data is stored on and restored from the local hard disk of the managed device instead of the HPCA Core server.

Example 3: Backup your files and settings locally

`InstallDir\Agent\pbr.exe /B /localstore`

Example 4: Restore after a local backup

`InstallDir\Agent\pbr.exe /R /localstore`

Using the Personality Backup and Restore Services

There are two built-in services that HPCA provides to help you automate the process of backing up and restoring user files and settings:

- HPCA Personality Backup (HPCA_PBR)
- HPCA Personality Restore (HPCA_RESTORE)

Both services invoke the `pbr.exe` application. These services are particulary helpful in the context of operating system deployment. The process works slightly differently depending on your HPCA license type.

You can only use the HPCA Personality Restore service to restore user data if the HPCA Personality Backup service (or `pbr.exe /B`) was used to perform the backup. If the Utility was used to perform the backup, the Utility must also be used to perform the restore.

To migrate user data as part of an OS deployment in HPCA Standard

1. On the Deployment Behavior page in the OS Deployment Wizard, specify **Yes** for the **Migrate User Data & Settings** option.

   When this option is selected, HPCA will use the HPCA Personality Backup service to back up the user data and settings for each managed device in the group prior to deploying the operating system. By default, the backup files are stored on the HPCA Core server.

2. Deploy the OS to the specified group of managed devices.
3. After the OS deployment is completed, make sure that USMT is installed in the default location on each managed device in the group (see Installing Microsoft USMT on Managed Devices on page 217).
4. Deploy the HPCA Personality Restore service (HPCA_RESTORE) in the Software Library to each managed device in the group.

   The service will run once on each device to restore the user data. The service first checks the `C:/OSMGR.PRESERVE` folder on the device to see if a local backup was performed. If it does not find local backup files, it restores the user data from the HPCA Core server.

To migrate user data as part of an OS deployment in HPCA Enterprise

1. Make sure that the following items are installed on all managed devices that will be part of this OS deployment:

— The HPCA agent

— USMT

2. Make sure that the OS image that you will deploy includes USMT installed in the default location and configured properly for your environment.

   An alternative is to install and configure USMT on your managed devices immediately after the OS deployment (see About USMT on page 215).

   If HPCA does not find USMT installed in the default location, neither the backup nor the restore will work.

3. Using the HPCA Policy Wizard, entitle the managed devices to the HPCA Personality Backup (HPCA_PBR) service.

4. Deploy the OS. The HPCA Personality Backup service will run on each managed device prior to the installation of the new OS. The backup files are stored on the HPCA Core server.

5. After the OS deployment is completed, entitle each managed device to the HPCA Personality Restore (HPCA_Restore) service.

6. Create a Notify job to deploy the HPCA Personality Restore service to each managed device.

   The service will run once on each device to restore the user data. The service first checks the `C:/OSMGR.PRESERVE` folder to see if a local backup was performed. If it does not find local backup files, it restores the user data from the HPCA Core server.

Troubleshooting

This section describes troubleshooting actions you can perform in the event that a backup or restore does not complete successfully.

Backup or Restore Did Not Complete Successfully

If the backup or restore did not complete successfully, check the `pbr.log` under the agent's `Log` directory for any errors that may have occurred during the backup or restore. The default `Log` directory is:

`C:\Program Files\Hewlett-Packard\HPCA\Agent\Log`

If you are using the `/localstore` option with `pbr.exe`, the log files are saved here:

`C:\OSMGR.PRESERVE\PBR.work\log`

You might also check the `ScanState.log` and the `LoadState.log` files that were created during the backup and restore, respectively. These files can be found under the agent's `Lib` directory in the `PBR\work\log` directory. The default `Lib` directory is:

`C:\Program Files\Hewlett-Packard\HPCA\Agent\Lib`

User Forgot Password and Cannot Restore Data

To perform a restore using the Personality Backup and Restore Utility, you need both the computer name and password that the user supplied for the backup. Although there is no method for recovering a lost password, an administrator can create a new password to enable a user to perform a restore. The process is as follows:

1. The administrator locates the backup directory on the HPCA Core server that contains the user files and settings. This directory resides under *DataDir*`\PersonalityBackupAndRestore\backups`, where *DataDir* is the user-configurable data directory specified during the installation of the HPCA Core. The subdirectories are named as follows:

   ComputerName_EncodedComputerNameAndPassword

2. The administrator runs the Personality Backup and Restore Utility to perform a backup. This backup should *not* be performed on the computer where the user forgot his password but can be performed on any other machine—preferably one with little or no user data to ensure a fast backup.

   To do this backup, the administrator must enter the same computer name that was used for the original backup (and which is part of the backup folder name discussed above) and create a password that will be given to the end-user to perform the restore.

3. The administrator locates the new directory created under `Data\PersonalityBackupAndRestore\backups`, deletes the *contents* of that directory, and copies the contents from the original backup directory discussed in step 1.

4. The end user runs the Personality Backup and Restore Utility, entering the original computer name and the password created by the administrator, to restore his files and settings.

Note that if the end user forgets his password but does not need to restore any data from past backups, he can simply enter a new password the next time he runs a backup and use that password to perform a restore.

13 Supported Locales

This chapter includes the following topics:

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.

When you are 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 you do not need the SOS and OS Manager System Agent messaging to be localized, do not make any of the following changes.

Supported Languages

- Brazilian Portuguese
- English
- French
- German
- Italian
- Japanese
- Simplified Chinese
- Spanish

Changing the Locale

To add support for a specific locale in a PXE environment

1 Use a UNIX based text editor to open this file:

   InstallDir\BootServer\X86PC\UNDI\boot\linux.cfg\default

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

   The file looks similar to the following:

```
[OS Manager]
DFLTSVOS=_SVC_LINUX_
ISVR=10.10.10.1:3466

[_SVC_LINUX_]
KERNEL=bzImage
APPEND initrd=rootfs.gz root=/dev/ram0 rw quiet pci=nommconf

[SVC_PEX86]
PEBCD=rombl.bcd
PEAPPEND=initrd=winpe.wim
```

2 For the Linux Service OS (SOS), add the LANG parameter to the end of the APPEND line. For example:

```
APPEND initrd=rootfs.gz root=/dev/ram0 rw quiet pci=nommconf
LANG=zh_CN
```

   For the WinPE SOS, add the LANG parameter to the end of the PEAPPEND line. For example:

```
PEAPPEND=initrd=winpe.wim LANG=zh_CN
```

   The following languages are available:

Language	LANG Value
Brazlian Portuguese	pt_BR
English	en_US
French	fr_FR

Language	**LANG Value**
German	de_DE
Italian	it_IT
Japanese	jp_JP
Simplified Chinese	zh_CN
Spanish	es_ES

3 Save and close the `default` file.

To add support for a specific locale when restoring from the Service CD-ROM

In the ServiceCD section of the `romsinfo.ini` file, specify `LANG=`*`LANGValue`* where *`LANGValue`* is the language code listed in the table above.

For example: `LANG=zh_CN`

> In previous HPCA releases, the `LANG=CJK` option was supported. As of HPCA version 7.80, this is no longer supported.
>
> If you specify `LANG=CJK,` the Linux SOS will start up with English messages until it switches to the locale specified in the pertinent BEHAVIOR instance in the CSDB (see Setting the System Language Parameter on page 234) or the locale specified in the `ROMBL.CFG` file for the LSB case.

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 CSDB Editor.

2 Go to the appropriate PRIMARY.OS.BEHAVIOR instance.

3 Double-click the **Locale used in Service OS** attribute. The Editing dialog box opens.

4 In the **Locale used in Service OS** box, type in the code for the language that you want. See the codes listed in the table on page 232.

5 Click **OK** to save your change and close the dialog box.

6 Drag and drop the BEHAVIOR instance to the appropriate POLICY instance.

Double-Byte Support for Sysprep or unattend.txt files

If you are using double byte characters, the `unattend.txt` file must be encoded in UTF-8 coding. For Sysprep files, follow double-byte character rules as stated by Microsoft.

14 Troubleshooting

This chapter includes the following topics:

If your environment uses Core and Satellite servers, first read the *HPCA Core and Satellite Servers Getting Started Guide* as the 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`

  Main log file, stored by default in *`InstallDir`*`\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-3466.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 *`InstallDir`*`\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 *`InstallDir`*`\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 *`InstallDir`*`\Data\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 here:

- 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 (InstallDir/Agent/Logs) and agent object information (InstallDir/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 InstallDir\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 InstallDir\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 InstallDir\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:
  - *`InstallDir`*`\Data\OSManagerServer\upload\machineID-all.log`
  - *`InstallDir`*`\Data\OSManagerServer\upload\machineID_rnl.log`
  - *`InstallDir`*`\OSManagerServer\logs` directory

    or

    `InstallDir``\OSManagerServer\RomVer.log`

— *InstallDir*\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 *InstallDir*\Data\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 InstallDir\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 *S*InstallDir\ManagementPortal and run Romadver.cmd. The log is created in the same directory.

To determine the versions of the Configuration Server, go to InstallDir\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

See the *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 *InstallDir*\Data\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 *InstallDir*\Data\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 67 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 InstallDir`\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 197.

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 3466, 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.

What if my devices fail to boot into the Service OS from the ImageCapture or ImageDeploy media?

Certain devices will not boot into the Service OS from the standard ImageCapture or ImageDeploy media provided with HPCA. This has been observed on some Dell devices, including the gx620, some Optiplex 745 and 755 models, and the Latitude 62.

If this happens, you must create a custom Service OS ISO for these devices. See Building a Custom Windows PE Service OS on page 303.

When you run the script to build your custom Service OS ISO, be sure to specify option **2** in step h on page 312 (boot load segment = 0x0000).

What should I do if my OS deployment to a Windows CE (Thin Client) device fails?

When you deploy an OS to a Windows CE device using Local Service Boot (LSB), there must be sufficient space available on the device to install and extract the LSB service. If the device reboots but fails to boot the Linux Service OS (SOS), the amount of "storage memory" allocated on the device may be insufficient—at least 10 MByte is required.

Before you deploy the OS, follow these steps on the Thin Client device:

1. Click **Start**.
2. Select **Settings** > **Control Panel**.
3. Click the **System** icon.
4. Select the **Memory** tab.
5. Use the slider on the left to increase the **Storage Memory** to 10 MByte or more.

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 21 App Events

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.

Table 21 App Events

Message	Description
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.
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). 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.

Table 21 App Events

Message	Description
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.
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). 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”. 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.

Table 21 App Events

Message	Description
%1$s %2$s has been selected	%1 = "OS" or "Hardware Configuration" %2 = The name of the OS or LDS Indicates what has been selected based on policy.
%1$s %2$s already installed	%1 = "OS" %2 = "OS name" The OS referenced has previously been installed.
%1$s %2$s was installed	%1 = "OS" %2 = "OS name" 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" %2 = "partition or disk ID" %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.

Table 21 App Events

Message	Description
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). 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. This can occur when multiple OSs resolve and the behaviors are configured for CENTRAL selection. The administrator must arbitrate the OS.
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. OR The OS Manager determined that a selected OS needed to be installed; it installed successfully and the system was set to desired state.

Table 21 App Events

Message	Description
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. Messages remain on screen for 30 seconds and then depending on the situation, the machine will be powered off, rebooted or the failed action will be attempted again.

Table 22 User Messages

Message	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

Table 22 User Messages

Message	User Action
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.
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: ACPI: $::acpi APIC: $::apic Minimum CPU speed: $::cpuspeed Minimum RAM size: $::mem Boot Hard Drive Type: $::boottype Minimum Hard Drive Size: $::hdsize The machine cannot be used and will shut down until an administrator specifies policy and performs a Wake On LAN.	N/A

Table 22 User Messages

Message	User Action
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.
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.

Table 22 User Messages

Message	User Action
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 `InstallDir\IntegrationServer\etc\put.cfg`.

2 Find the following section:

```
namespace eval Put {
    array set cfg [list \
        -ROLLOVER   0   \
        -TYPELIST   ".log"
    ]
}
```

3 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.

D Customizing the Windows Answer File

This appendix contains the following topics:

These topics pertain to the process of capturing and publishing operating system images so that they can be deployed to managed devices in unattended mode (requiring no user interaction on the client devices).

Customizing the unattend.xml File

HPCA provides an answer file that you can use for unattended OS installations. This answer file is called `unattend.xml`.

Each operating system and architecture (for example, 32-bit or 64-bit) has its own `unattend.xml` file. The files are located in subdirectories of:

InstallDir`\Data\OSManagerServer\capture-conf`

The header at the beginning of the file shows you the OS, architecture, and deployment method to which the file applies.

If you want to use the `unattend.xml` file that HP provides, you must modify it for your environment before you publish the OS image. Here are some settings that you will want to customize:

- ProductKey on page 265
- TimeZone on page 267
- RegisteredOwner and RegisteredOrganization on page 268
- JoinDomain on page 268
- MetaData on page 270

At a minimum, you must specify a valid product key (see ProductKey on page 265). Modifying the other settings discussed here is optional.

Use a text editor to modify a copy of the pertinent `unattend.xml` file. You can name this copy anything that you like as long as it has the `.xml` file extension. When you publish the OS image, you will specify where your customized answer file is located.

The Windows Automated Installation Kit (AIK) includes a file called `Unattend.chm`. This is a compiled online help file that contains reference information about the contents of the `unattend.xml` file. Refer to this help file for more detailed information about the settings discussed here and the other settings available that you can customize. To open the file, simply double-click `Unattend.chm`.

ProductKey

The `<ProductKey>` element appears in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using. The `<ProductKey>` is a string with 29 characters that is delimited like this:

```
XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

➤ For all DVD installations, be sure that `/IMAGE/INDEX` is pointing to the correct image on the DVD (see MetaData on page 270).

Retail Editions

For retail editions of Windows (for example, Windows 7 Ultimate), make the following modifications:

- Put a valid product key in the `<Key>` element inside the `<ProductKey>` element. For example:

  ```
  <UserData>
      <AcceptEula>true</AcceptEula>
      <ProductKey>
          <Key>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</Key>
          <WillShowUI>OnError</WillShowUI>
      </ProductKey>
  </UserData>
  ```

  This element is located in the "Microsoft-Windows-Setup" component in the “WindowsPE” in pass.

- Remove the entire `<ProductKey>` element located in the “Microsoft-Windows-Shell-Setup” component in the “specialize” pass:

  ```
  <ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>
  ```

Business Editions

For business editions of Windows (including Business, Enterprise, Professional, or Server editions), make the following modifications:

- Remove all characters in the <Key> element located in the located in the "Microsoft-Windows-Setup" component in the “WindowsPE” in pass (see example above):

  `<Key></Key>`

- Put a valid product key in the <ProductKey> element located in the “Microsoft-Windows-Shell-Setup” component in the “specialize” pass:

  `<ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>`

  If you are using a Volume License Multiple Activation Key (MAK), use that in the <ProductKey> element.

In the Windows AIK, the <Key></Key> element supports an empty value, but the <ProductKey> element does not—hence <ProductKey> element must be deleted if it is not being used (see Retail Editions on page 265).

64-Bit Platforms

When you are using a DVD with the Windows Setup deployment method on some 64-bit architectures, be sure to make the following modifications:

- Remove all characters in the <Key> element located in the located in the "Microsoft-Windows-Setup" component in the “WindowsPE” in pass (see example above):

  `<Key></Key>`

- Put a valid product key in the <ProductKey> element located in the “Microsoft-Windows-Shell-Setup” component in the “specialize” pass:

  `<ProductKey>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</ProductKey>`

- Make sure that /IMAGE/INDEX points to the correct image on the media (see MetaData on page 270).
- Change "amd64" to "x86" in the following component specifications in the “WindowsPE” pass:

```
<component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="amd64" ...
```

```
<component name="Microsoft-Windows-Setup"
processorArchitecture="amd64" ...
```

- During publishing, when you are prompted for the source directory, specify the one from the 32-bit media for the same operating system.

- Special instructions for Windows 2008 R2 x64:
  - Use the Windows 7 Enterprise Edition 32-bit installation media.
  - Before you publish the OS image, follow these steps:
    a. From the Windows 7 32-bit installation media, copy the `mediaDrive:\sources` folder to `c:\temp`
    b. Remove the Windows 7 media, and load the Windows 2008 R2 x64 media.
    c. From the Windows 2008 R2 x64 installation media, copy the `mediaDrive:\sources\license` folder to `c:\temp\sources`

    If prompted to overwrite existing files, do so.

    This ensures that the Windows 2008 Server R2 EULAs are available from the Windows 7 installation folder.

For more information, refer to the "ProductKey" topic in the `Unattend.chm` help file included in the Windows AIK.

HPCA does not currently support image capture for Windows Setup deployment on 64-bit platforms.

TimeZone

The `<TimeZone>` element appears in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using.

For example, in the `unattend.xml` file for a captured Windows 7 (x86) image, there are two places where the `<TimeZone>` element appears:

- In the `Microsoft-Windows-Shell-Setup` component under

  `<settings pass="oobeSystem">`
- In the `Microsoft-Windows-Shell-Setup` component under

  `<settings pass="specialize">`

Change the `<TimeZone>` to match the target devices to which the OS will be deployed. For example:

```
<TimeZone>Eastern Standard Time</TimeZone>
```

It is important that the spelling of the time zone exactly match the spelling used in the Windows Registry. For more information, refer to the “Language Pack Default Values” topic in the `Unattend.chm` help file included in the Windows AIK.

➤ Greenwich Mean Time is now known as Coordinated Universal Time.

➤ On a computer running Windows 7 you can use the `tzutil` command to list the time zone for that computer.

RegisteredOwner and RegisteredOrganization

These elements appear in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using.

For example, in the `unattend.xml` file for a captured Windows 7 (x86) image, there are two places where these two elements appear:

- In the `Microsoft-Windows-Shell-Setup` component under

  ```
  <settings pass="oobeSystem">
  ```

- In the `Microsoft-Windows-Shell-Setup` component under

  ```
  <settings pass="specialize">
  ```

Change these elements to the name of your company (or the entity to whom the operating system is registered). For example:

```
<RegisteredOrganization>Hewlett-Packard</RegisteredOrganization>
<RegisteredOwner>Hewlett-Packard</RegisteredOwner>
```

These strings can be up to 256 characters in length.

Refer to the “RegisteredOrganization” and “RegisteredOwner” topics in the `Unattend.chm` help file included in the Windows AIK for more information.

JoinDomain

You can instruct target devices to either join a domain or a workgroup after the OS is installed. Workgroup mode is the default. To instruct targets to join a domain, modify the following element:

```
<component name="Microsoft-Windows-UnattendedJoin" ... >
    <Identification>
        <Credentials>
            <Domain></Domain>
            <Password></Password>
            <Username></Username>
        </Credentials>
        <JoinDomain></JoinDomain>
    </Identification>
</component>
```

For example:

```
<component name="Microsoft-Windows-UnattendedJoin" ...>
    <Identification>
        <Credentials>
            <Domain>lan.mycompany.com.de</Domain>
            <Password>T3ch3d08</Password>
            <Username>administrator</Username>
        </Credentials>
        <JoinDomain>lan.mycompany.com.de</JoinDomain>
    </Identification>
</component>
```

- The user specified must have an access level sufficient to join the domain.
- If any of this information is missing or incorrect, the device will join a workgroup instead of a domain.
- If the target device was previously managed by HPCA, and the device was previously a member of a domain, the stored domain information will override the contents of the `<Domain>` and `<JoinDomain>` elements in the `unattend.xml` file.
- Any information that is set centrally—for example, by using an OS Manager Server script to set the domain—will override information in `unattend.xml`.

Refer to the "JoinDomain" topic in the `Unattend.chm` help file included in the Windows AIK for more information.

MetaData

If you are deploying an operating system image directly from a DVD, you must specify the location of that image within the WIM file on the DVD. In the WIM file, this information is organized like this:

```
<WIM>
   <IMAGE INDEX="2">
      <NAME>MyWIM</NAME>
      <DESCRIPTION>MyCustomWindowsImage</DESCRIPTION>
   </IMAGE>
</WIM>
```

In the `unattend.xml` file, the image information is specfied in the `<MetaData>` element in the `Microsoft-Windows-Setup` component hierarchy under `<settings pass="WindowsPE">`. For example:

```
<MetaData>
   <Key>/IMAGE/INDEX</Key>
   <Value>2</Value>
</MetaData>
```

The `<Key>` element indicates which data item in the WIM file to match. It can be any of the following:

- `IMAGE/INDEX`
- `IMAGE/NAME`
- `IMAGE/DESCRIPTION`

The `<Value>` element indicates what the value of this data item should be. Here, the image to be deployed has an `IMAGE/INDEX` value of `2` in the WIM file.

You can extract a list of the images in a WIM file by using the following command:

```
imagex /info WIMFileName > c:\info.txt
```

Here, *`WIMFileName`* is the name of the WIM file (for example, `install.wim`). Be sure to redirect the output of the command to a text file (as shown here) so that you can easily search through the results.

For more information, refer to the "MetaData" topic in the `Unattend.chm` help file included in the Windows AIK.

XML File Processing in the HPCA OS Manager

The unattend.xml file that you publish is overlaid on top of any unattend.xml file that is present in the image that was published.

Before HPCA starts the image install, the published XML is combined with the substitutes file to generate the final unattend.xml.

This combining of files is done by HPCA before it starts the actual image installation. The previously exposed substitutes file is now used behind the scenes. Each operating system and architecture (for example, 32-bit or 64-bit) has its own file. The files are located in subdirectories of:

InstallDir\Data\OSManagerServer\capture-conf

The correct file is selected automatically depending on the processor architecture of the image being published.

Table 23 lists the settings in the unattend.xml file that are updated when the substitutes file is published.

The settings in blue (CommandLine, Path, and both instances of PartitionID) are required for HPCA to work. They cannot be removed.

Table 23 Settings Updated Based on the substitutes File

Settings Pass	Component	Path	Setting	Override Value
windowsPE	Microsoft-Windows-Setup	DiskConfiguration/Disk/ModifyPartitions/ModifyPartition	PartitionID	DISKPART volume ID to which HPCA will install the OS
windowsPE	Microsoft-Windows-Setup	ImageInstall/OSImage/InstallTo/	PartitionID	DISKPART volume ID to which HPCA will install the OS
windowsPE	Microsoft-Windows-Setup	ImageInstall/OSImage/InstallFrom/	Path	WIM file to use for installation

Table 23 Settings Updated Based on the `substitutes` File

Settings Pass	Component	Path	Setting	Override Value
`oobeSystem`	`Microsoft-Windows-Shell-Setup`	`AutoLogon/`	`Domain`	Computer name (for auto-logon)
`specialize`	`Microsoft-Windows-Shell-Setup`	`AutoLogon/`	`Domain`	Local computer name (for auto-logon)
`specialize`	`Microsoft-Windows-UnattendedJoin`	`Identification/Credentials/`	`Domain`	Centrally set domain via `getmachinename.tcl` or pre-existing device entry in the HPCA Enterprise console
`specialize`	`Microsoft-Windows-UnattendedJoin`	`Identification/`	`JoinDomain`	Centrally set domain via `getmachinename.tcl` or pre-existing device entry in the HPCA Enterprise console
`specialize`	`Microsoft-Windows-Shell-Setup`		`ComputerName`	Computer name
`oobeSystem`	`Microsoft-Windows-Shell-Setup`	`FirstLogonCommands/SynchronousCommand`	`CommandLine`	Path to agent install media installer

You can, if required, customize the `substitutes` file to disable certain customizations or to add new ones. You cannot however remove or change the `PartitionID` or `CommandLine` settings.

About the .subs and .xml Files

HPCA now enables you to specify the source of this information when you run the Publisher. See Publishing Operating System Images on page 99 for more information.

This topic does not apply to Windows XP or Windows 2003.

The HPCA Publisher is backward compatible. It supports publishing saved OS images that consist of a `.WIM` file, a `.EDM` file, a `.XML` file, and a `.SUBS` file.

If you choose to manually pre-create `*.SUBS` and `*.XML` files, they must have the same prefix as the `*.WIM` file. For example: `vista.WIM`, `vista.SUBS`, and `vista.XML`. All three files must be stored in the same directory.

When you run the HPCA Publisher, if it finds a `*.SUBS` and `*.XML` file in the same directory as the `*.WIM` file, it will not prompt you for an `unattend.xml` file.

HPCA provides samples of these files on the Image Capture media in subdirectories of the following folder:

```
\samples\unattend
```

If you choose to use the sample files, rename them and then modify them as needed—for example, setting the `<TimeZone>` and the `<ProductKey>`.

The `*.XML` file is an answer file that contains standard information as well as placeholders for information that will be included from `*.SUBS`. You can use the Microsoft Windows System Image Manager (SIM) tool to make additions to the `*.XML` file. If you do so, you must first open the corresponding `*.WIM` file before opening `*.XML`.

If you choose to use `*.XML` and `*.SUBS` files, you must specify your Windows installation product key in the `*.XML` file.

Do not delete any XML values from this file! If you modify the `*.XML` 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.

The `*.SUBS` file is the "substitutes" file that lists each XML item to be modified in `*.XML` and what its value should be. The lines in the `*.SUBS` file are called XPATHs.

Information entered in the `*.SUBS` file takes precedence over information in the `*.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 changed from "`anything`" in the *`filename`*`.xml` file to "`VistaTeam`" in the `unattend.xml` file.

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

1. Locate the appropriate `unattend*.xml` and `subsitutes` files for your operating system, target device architecture, and deployment method. These files are located under `samples\` on the ImageCapture CD.
2. Make a copy of the `unattend*.xml` file, and name it *`filename`*`.xml`, where *`filename`* matches the name of your `.WIM` file. Store the copy in the same directory as your `.WIM` file.

3 Make a copy of the `substitutes` file, and name it *`filename`*`.subs`. Store the copy in the same directory as your `.WIM` file.

You should now have the following three files in one directory:

— *`filename`*`.wim`

— *`filename`*`.xml`

— *`filename`*`.subs`

4 Locate the XML element for JoinDomain in the *`filename`*`.xml` file. It should look similar to this example:

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

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

    <settings pass="specialize">

<component name="Microsoft-Windows-UnattendedJoin"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/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#Windows Vista ULTIMATE"
xmlns:cpi="urn:schemas-microsoft-com:cpi"/>

</unattend>
```

5 Modify the following XPATH element in the *`filename`*`.subs` file. Note that this XPATH element appears on a single line in the *`filename`*`.subs` file.

```
//un:settings[@pass='specialize']//
un:component[@name=Microsoft-Windows-UnattendedJoin'][@pr
ocessorArchitecture='x86']/un:Identification/
un:JoinDomain,VistaTeam
```

During deployment of the operating system, the `filename.subs` and `filename.xml` files will be combined to create an `unattend.xml` file that is used to provide information during all phases of the Windows setup. In this example, the JoinDomain attribute will be set to **`VistaTeam`**.

E Capturing Windows XP and Windows Server 2003 OS Images

The information in this appendix pertains only to Windows XP and Windows Server 2003 OS image captures.

For information about capturing Windows Vista, Windows Server 2008, Windows 7, and all supported Thin Client operating systems—as well as important image capture process overview information—see Preparing and Capturing OS Images on page 67.

The OS Manager only supports capturing unencrypted partitions.

This chapter includes the following topics:

About the HPCA Image Preparation Wizard

You can use the HPCA Image Preparation Wizard to capture Windows XP or Windows 2003 Server OS images for ImageX, Windows Setup, or Legacy deployment (see Deployment Methods on page 70 for more information).

The Image Preparation Wizard performs the following tasks:

1. Collects and stores information (including hardware and OS information capabilities) about the reference machine.

2 Executes the exit points that are available for your use as needed. `PRE.CMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.CMD` is executed after Sysprep has sealed the image. See Image Preparation Wizard Exit Points on page 279 for details.

> Image Capture exit points are only supported for ImageX and Windows Setup capture types.

3 Runs Microsoft Sysprep (on supported operating systems).

4 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.

During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 93 for more information.

5 Creates and copies files to the following directory on the OS Manager Server:

InstallDir`\Data\OSManagerServer\upload`

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.

Image Preparation Wizard Exit Points

You can use exit points for the Image Preparation Wizard as needed. For example, you may use them to clean up a device before performing a capture.

Image Capture exit points are only supported for ImageX and Windows Setup capture types.

To use the exit points:

1 Create the files `PRE.CMD` and `POST.CMD`.

2 Save these files and any supporting files in `OSM\PREPWIZ\payload\default\pre` and `OSM\PREPWIZ\payload\default\post` respectively.

The Image Preparation Wizard copies these files to `%temp%\prepwiz\pre` and `%temp%\prepwiz\post` on the reference device and removes them before the capture begins. `PRE.CMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.CMD` is executed after Sysprep has sealed the image.

A non-zero return value from either `PRE.CMD` or `POST.CMD` will cause the Image Preparation Wizard to halt. In interactive mode, you can decide to Stop or Ignore the error and continue. In batch mode, the Image Preparation Wizard will halt.

Prerequisites for Capturing Images

The following steps must be completed prior to performing an OS image capture for ImageX, Windows Setup, or Legacy deployment:

- Prepare the Reference Machine on page 280
- Install the Windows AIK on page 282

- Install and Configure Sysprep on page 282

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. 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 knowledge base article contains information about including OEM drivers for Windows OS installations:

   Article: 314479 - How to Add OEM Plug and Play Drivers to Windows XP

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

3 Make sure that the Microsoft .NET Framework version 2.0 (or later) is installed. The .NET Framework is available at the Microsoft download center:

   http://www.microsoft.com/downloads

   To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:

   `%SYSTEMROOT%/Microsoft.NET/Framework`

4 If you plan to use the Legacy method to deploy this image, you must install the HPCA agent on the reference machine. This is not necessary for Windows Setup or ImageX deployments, because HPCA requires you to publish the agent along with the OS image for Windows Setup or ImageX.

   For Legacy deployment only:

   Install the agent from the HPCA installation media as per your requirements—at a minimum, you must install the Application Manager and OS Manager agents. These are required so that when the OS image is deployed, the device can connect to the OS Manager Server. If you need to update the agents, you must use agent self-maintenance.

5 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 HPCA Server is finished.

6 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.

> For Windows operating system prior to Windows 7, HP supports deploying the image to the primary boot partition of the primary boot drive.

> To successfully capture an image using the Windows Setup deployment method, you must have sufficient free disk space in the OS partition on the reference machine. For example, to capture a 7 GByte image, you will need 50-60 GByte of free disk space.

The following steps help to minimize the size of the `.WIM` 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 `ExtendOemPartition = 1` in the `[Unattended]` section of the `Sysprep.inf` file to allow for the small image to be installed on a target device with a much larger drive.

When `ExtendOemPartition = 1`, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The HPCA agent can then use the free space on the volume for application installations.

b If you are using a laptop, disable hibernation.

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.

Install the Windows AIK

If you will use ImageX or Windows Setup for deployment, the Windows Automated Installation Kit (AIK) must be installed on the HPCA Core—where you will publish OS images to the HPCA database.

If the Windows AIK is not installed, you can download it from the Microsoft Download Center (`www.microsoft.com/downloads`). It is not included as part of a normal Windows installation. Be sure to install the appropriate version for your operating system, and install it in the default location:

```
C:\Program Files\Windows AIK
```

After you install the Windows AIK, be sure to restart the HPCA Core service.

Refer to "Using HPCA to Manage Windows Operating Systems" in the *HPCA Core & Satellite Getting Started and Concepts Guide* for more information.

Install and Configure Sysprep

Microsoft Sysprep is a program that enables you to distribute Microsoft operating systems using cloned images. The HPCA OS Manager Image Preparation Wizard runs Microsoft Sysprep in order to strip out all of the security identifiers and reset the image.

After the operating system image is delivered to the target device, the Microsoft Mini-Wizard runs 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 install Sysprep

1 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` file, and how to set the available parameters.

2 On the Microsoft operating system installation media, locate the `DEPLOY.CAB` file in the `SUPPORT\TOOLS` folder. See Microsoft's documentation for details.

3 Extract the Microsoft Sysprep files from the `Deploy.cab` file. 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 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 Image Preparation Wizard will exit and after you set up the appropriate user rights you will need to run the wizard again.

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

5 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 the `\samples\sysprep\` directory.

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

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 Using an Override Sysprep File on page 149 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 HPCA database and then use the Administrator 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 ROM object in the Portal.

Capturing OS Images

Refer to the instructions for the type of capture you want to perform:

Deployment Method	Instructions
ImageX, Windows Setup, Legacy	Capture Images Using the Image Capture Wizard on page 285 or Capture Images Using the Image Preparation Wizard in Unattended Mode on page 293
Windows Native Install Packager	Capture Images for Deployment using the Windows Native Install Packager on page 295

Capture Images Using the Image Capture Wizard

The following instructions pertain to OS image capture for ImageX, Windows Setup, or Legacy deployment.

To use the HPCA OS Manager Image Preparation Wizard

If you are capturing an image locally, before continuing, set the reference machine to boot from the CD-ROM/DVD 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 34 if you need more information about where to get this media.

2 On the ImageCapture media, go to `\image_preparation_wizard\win32`, and run `oscapture.exe`.

> If the HPCA agent is not installed on the reference machine, 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 HPCA agent before running the Image Preparation Wizard.

> The `oscapture.exe` program requires the Microsoft .NET Framework version 2.0 (or later), which is available at the Microsoft download center:
>
> **http://www.microsoft.com/downloads**
>
> To determine which version of the .NET Framework is present on the reference machine, list the folders in the following directory:
>
> `%SYSTEMROOT%/Microsoft.NET/Framework`

— 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 the 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:\sysprep`.

When you deploy using Windows XP Service Pack 2 using either ImageX or Windows Setup, the HPCA agent will be injected into the image during the deployment process.

If you want to install the agent to a location other than the default location on your target devices, you must edit the `INSTALLDIR` property in `install.ini`. Refer to the *HP Client Automation Enterprise Application Manager and Application Self-service Manager Installation and Configuration Guide* for details on modifying `install.ini`.

It is important to note that if you have already installed the agent to a location other than the default in your image, you must update the `INSTALLDIR` property in `install.ini` as well.

If the agent is installed in the default location, do not make any changes to `install.ini`.

You must edit `install.ini` prior to using the Publisher to publish the image to the HPCA database.

When using the Publisher, you will be given an option to select where to get 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 HPCA database. After you do this, all new `.WIM` deployments will automatically use the latest agent.

If you are using an HPCA Standard license, the agent must already be included on the image that was captured. However, you still must select where to publish the agent from when running the Publisher.

3 Click **Next**.

The End User License Agreement window opens.

4 Click **Accept**.

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 Windows PE and the ImageX utility.

— **Windows Setup** captures an image in `.WIM` format that will be deployed using Windows PE and Windows Setup.

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

5 Select the deployment method that you want to use, and click **Next**.

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 used for OS imaging and deployment in an HPCA Core and Satellite installation is 3466. In an HPCA Classic installation, port 3469 is reserved for this purpose.

7 Click **Next**.

8 Type a name for the image file. This is the image name that will be stored in the *InstallDir*`\Data\OSManagerServer\upload` directory.

9 Click **Next**.

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 HPCA database.

If this value is set to 0 (zero), and the size of the image resource files exceeds 4GB, the image will be spanned automatically.

11 Click **Next**.

If appropriate, the Additional Sysprep Options window opens. 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. Any additional options that you add or changes that you make are not validated and may result in image capture or deployment failure. Use with caution or when instructed to do so by HP Software Support personnel.

Review Microsoft's documentation for information about additional Sysprep options

12 Click **Next**.

13 If you chose ImageX for the deployment method, the Select Image Preparation Wizard payload window opens with the default option selected.

The payload contains Local Service Boot (LSB) data to be delivered to target devices.

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. It is important to have this agent installed only 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 or if you are capturing a Windows Vista (or later) 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 (and later) 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, depending on the size of the image.

A message pops up if insufficient space is available on the System Reserve partition to hold the LSB injection files. You can either ignore this message or stop the Image Preparation Wizard. If you ignore the message (and have created enough space on this partition) the Image Preparation Wizard will continue. Otherwise, it will fail indicating that it cannot inject the LSB files.

During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 93 for more information.

Sysprep will reboot the device when complete. You may need to click **OK** to restart the device.

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).

For Legacy capture mode, 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 300 KByte/sec to 1MByte/sec or more 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 HPCA Core in the following directory:

InstallDir\Data\OSManagerServer\upload

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

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

Next, you will want to publish your image to the HPCA database. See Publishing on page 97.

Capture Images Using the Image Preparation Wizard in Unattended Mode

You may use a configuration file to run the Image Preparation Wizard in unattended mode.

To use the Image Preparation Wizard in Unattended Mode

1. Insert the ImageCapture media into the reference machine. See Product Media on page 34 if you need more information about where to get this media.
2. Go to `\samples\prepwiz_unattend` and copy the OS-specific configuration file (`vista.cfg` or `xp.cfg`) to your local machine or a network location.
3. Make the necessary modifications. Table 24 lists the values that you may need to change.

Table 24 Variables in the Configuration File to be Modified

Variable Name	Description	Sample Value
RISHOSTPORT	The OS Manager Server's IP address.	*xxx.xxx.x.x:port*
IMAGENAME	The prefix used to create the uploaded files. This is appended to `.WIM` to create the name of the uploaded image.	Vista
IMAGEDESC	Description of the image that is published to the Database.	“Windows Vista Unattended Test Image”

Table 24 Variables in the Configuration File to be Modified

Variable Name	Description	Sample Value
PREPWIZPAYLOAD (for future releases)	Payload that the administrator wants to use. The payload contains Local Service Boot (LSB) data to be delivered to target devices.	Use the default value "`/OSM/PREPWIZ/payload/default/`"
OSEDITION (required for Vista)	Specifies the edition of Vista used.	"Enterprise"
set ::setup(DEPLOYOS,SELECTED)	Set to 1 or 0 to indicate whether you want to redeploy the OS after the image capture.	"0"
set ::setup(ClientConnect,SELECTED)	Set to 1 or 0 to indicate whether you want the target device to perform an OS a connect after the image is deployed.	"1"

4 On the reference machine, open a command window and change to the CD/DVD directory. Go to `Image_Preparation_Wizard\win32`. Then, run the following command:

```
prepwiz -mode silent -cfg <fully qualified
path>\<config_file>
```

Where <*config_file*> is the operating system-specific configuration file (for example, `setup.cfg`).

The Image Preparation Wizard starts Sysprep; this can take 15-20 minutes to complete. Sysprep reboots the device when complete, connects to the network and stores the image in the `/upload` directory on the OS Manager Server.

Capture Images for Deployment using the Windows Native Install Packager

Capture of Windows XP and Windows 2003 images for this deployment mode is only supported in HPCA Enterprise Edition.

This is the only case 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 HPCA agent. The image is sent to the *InstallDir*`\Data\OSManagerServer\upload` directory on the OS Manager Server, and then you use the Publisher to publish the image to the HPCA database.

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 1: Prepare the Reference Machine on page 295
- Task 2: Create unattend.txt on page 297
- Task 3: Install the HPCA Windows Native Install Package on page 298
- Task 4: Run the HPCA Windows Native Install Package on page 298

Task 1: 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 HPCA media, and that the reference machine meets the following requirements:

1. Connectivity to an 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 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 Task 3: Install the HPCA Windows Native Install Package on page 298.

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 HPCA agent.

— 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 allow you to 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 Server, 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 the `\samples` directory.

Task 2: Create unattend.txt

The `unattend.txt` file 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 HPCA agent setup uses the Windows installer to install the agent on the target device, and `$OEM$\cmdlines.txt` cannot run the Windows Installer.

  The `AutoLogon` and `AutoLogonCount` statements ensure that the agent 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). Then, 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 Publisher to publish these files to the SYSPREP class in the HPCA DB, and then you can connect them to the appropriate OS image. When the image is deployed, the customized `unattend.txt` will be merged with the original file.

  See Publishing on page 97 for details about publishing files. When publishing `unattend.txt` files, follow the instructions as if you were publishing a `Sysprep.inf` file.

Task 3: Install the HPCA Windows Native Install Package

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 4: Run the HPCA Windows Native Install Package

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

   You must complete the information in each of the three areas in 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 HPCA agent.
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` directory 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. 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 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 device, 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/DVD. This refers to the Image Capture media.

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

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

21 Click **Finish**.

22 Reboot the device, and the image is uploaded the `*InstallDir*\Data\OSManagerServer\upload` directory.

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

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the HPCA database. For instructions, see Publishing on page 97.

When you have published the image, refresh the OS Library to view the list of available OS images. Use the HPCA Console toolbar to deploy the image to selected devices.

F Building a Custom Windows PE Service OS

This chapter includes the following topics:

About the Custom Build Script

HP provides a script that enables you to:

- Add font support for Chinese or Japanese.
- Update the Windows Preinstallation Environment (PE) Service OS when a new `winpe.wim` file is made available through an updated Windows Automated Installation Kit (AIK).
- Add extra drivers or packages that do not exist in the Windows PE Service OS provided.
- Use the information in this chapter in conjunction with your knowledge of the Microsoft Windows AIK to rebuild the Windows PE Service OS with the drivers and packages necessary for your environment.
- 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

Before you can use the script provided by HP to build a custom Windows PE Service OS, you must satisfy a number of prerequisites. See the following topics for details:

- Process Knowledge on page 305
- Administrator Machine on page 305
- Media on page 306
- Files and Directories on page 306
- Support for Other Languages on page 307
- Advanced Option on page 307

Do not attempt to run this script on a machine where incompatible software is installed. See the prerequisites for the Administrator Machine.

Process Knowledge

You will need a basic understanding of Microsoft's preinstallation customization process to add drivers and other information to the Windows PE Service OS.

Administrator Machine

To run the script, you will need an "administrator" machine with the 32-bit version of the Windows Automated Installation Kit (AIK) installed. This is the machine that you will use to build the customized Windows PE Service OS.

Do NOT use a machine where any of the following are installed:

- HPCA Boot Server
- HPCA Core or Satellite server
- Cygwin

Versions 1.1 and 2.0 of the Windows AIK are supported. Version 1.1 comes with Windows Vista and Windows Server 2008. Version 2.0 comes with Windows 7 and Windows Server 2008 R2; it is backward compatible. You can download either version from the Microsoft web site.

Be sure to download and install the 32-bit version of the Windows AIK.

Media

You will need the following media (DVD or CD-ROM):

- HPCA product media
- HPCA Image Capture media
- HPCA Image Deploy media

Files and Directories

- You will need the `build_scripts.zip` file from the HPCA product media.
- If you are generating a new `ImageCapture.iso` or `ImageDeploy.iso`, you must do the following to include the updated files required.

  a. Create a build items directory on the Administrator Machine, such as `c:\build_items`.

  b. *Optional*: Copy any updated files that you have received from HP to this build items directory. Create subdirectories as needed, based on the structure of the Image Capture or Image Deploy media.

     If any of the 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*: Include `romsinfo.ini` (see page 195) or `netinfo.ini` (see page 196) in the build items directory for use on the ImageDeploy CD.

  d. *Optional:* Include `rombl_capture.cfg` and `rombl_deploy.cfg` in the build items directory for use on the appropriate ISO. These files contain information such as the menu timeout settings and the default Service OS.

To create these files, copy `rombl.cfg` from the previous `ImageCapture.iso` or `ImageDeploy.iso`, and modify and rename the files as necessary.

If you do not include these files in the build items 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, a standard `rombl.cfg` file will be created automatically.

Support for Other Languages

If you want to add support for Chinese or Japanese 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 Windows PE Service OS on page 309 to run the script.

  To use the Chinese or Japanese enabled `winpe.wim` file without rebuilding the `winpe.wim` file, be sure to type **N** when prompted to recreate the `winpe.wim` file.

- If you are using the ImageDeploy CD to install from CD—or you 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 media to the build items directory. You may remove the `.msg` files that are not needed for your local language.

Advanced Option

The following information is intended for experienced HPCA administrators only. Do not attempt to customize an existing `winpe.wim` file unless you have a strong understanding of both OS Management under HPCA and the Microsoft Windows AIK tools.

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 the Windows AIK that is installed on the machine where you are executing the build scripts.
- The `winpe.wim` file must have the following packages installed:
  - For Windows AIK version 1.1
    - `WinPE-HTA-Package`
    - `WinPE-Scripting-Package`
    - `WinPE-XML-Package`
    - `WinPE-WMI Package`
  - For Windows AIK version 2.0
    - `WinPE-hta.cab`
    - `WinPE-scripting.cab`
    - `WinPE-wmi.cab`
    - `WinPE-setup.cab`
    - `WinPE-legacysetup.cab`
    - `WinPE-setup-client.cab`
    - `WinPE-setup-server.cab`
- If your `winpe.wim` file was prepared using the `peimg /prep` command, refer to the Microsoft documentation for the Windows AIK, peimg, and ImageX for restrictions (only applies to Windows AIK 1.1).

Adding Drivers to the Windows PE Service OS

You can add drivers to the Windows PE Service OS when you run the build scripts. For example, if you have a driver that requires a reboot, you must do it in "offline" mode. This 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 Windows PE while it is running (“online” mode). 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 Windows PE Service OS, any drivers that exist in *InstallDir*\OSManagerServer\SOS\WinPE\drivers will be downloaded and installed using drvload.exe.

Building a Custom Windows PE Service OS

The following topics show you how to obtain and use the script that HPCA provides to build a custom Windows PE Service OS.

- To obtain the script and prepare to run it, see Get the Script on page 309.
- To launch the script and specify the information that it requires, see Run the Script on page 310.
- After you run the script, see Additional Information on page 314.

Be sure to review and satisfy the Prerequisites on page 305 before you invoke the script.

Get the Script

The script that you will need to build a custom Windows PE Service OS is located on the HPCA installation media. Follow the procedure below to obtain the script and prepare to run it on your Administrator Machine.

To obtain the script and make it available on the Administrator Machine

1. Copy *InstallDir*\media\ISO\roms\build_scripts.zip from the installation media to a location on the Administrator Machine (where the Windows AIK is installed).
2. Unzip build_scripts.zip to a directory of your choice (such as C:\Build_scripts).

Run the Script

This procedure assumes that you have satisfied the prerequisites (see Prerequisites on page 305) and obtained the script (see Get the Script on page 309).

To build a custom Windows PE Service OS

1. Go to a Windows command prompt, and change to the directory that you just created (for example, `C:\ Build_scripts`).
2. Type **`run`**
3. Type the number corresponding to the HPCA version that you want to use.
4. 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 you are later prompted to recreate the `winpe.wim` file.

   If you typed **`Y`**, you will be prompted to type the path to your Windows AIK tools directory. For example, `C:\Program Files\Windows AIK\Tools`
5. 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.
6. When asked whether you want to include the local font support packages, type **`Y`** or **`N`**.
7. When asked whether you want to pause the WIM creation process to add extra drivers or packages, type **`Y`** or **`N`**.
8. When asked whether you want to provide a path to a directory containing additional drivers to be added during the WIM creation process, type **`Y`** or **`N`**.

If you typed **`Y`**, you will be asked to enter the fully qualified path to the directory containing the drivers.

9 The next group of questions determines whether you want to create a new Image Capture ISO or Image Deploy ISO and which Service OS to include.

- You should create a new Image Capture ISO (type **`Y`**) if any of the following conditions are true:
  - You have received updated files from HP Software Support.
  - You have rebuilt `winpe.wim`, and you are using the ISO to perform the capture.
  - You need to change the configuration (`rombl.cfg`, `netinfo.ini`, or `rominfo.ini`).
- You should create a new Image Deploy ISO (type **`Y`**) if any of the following conditions are true:
  - You have received updated files from HP Software Support.
  - You have rebuilt `winpe.wim`, and you are booting from the CD during deployment.
  - You need to change the configuration (`rombl.cfg`, `netinfo.ini`, or `rominfo.ini`).

Follow these steps to specify the ISO options:

a When asked whether you want to create a new Image Capture ISO, type **`Y`** or **`N`**.

b When asked whether you want to create a new Image Deploy ISO, type **`Y`** or **`N`**.

c If you answered **`Y`** to question (a) or (b), you will be asked which Service OSs to include on the ISO. Type the appropriate selection. Then, press **Enter**.

d When asked if you want to create a new `rombl.cfg` or use a pre-existing `rombl.cfg` file, choose one of the following actions:

- To create a new `rombl.cfg` file, type **`1`**, and press **Enter**.
- To use a pre-existing `rombl.cfg` file, type **`2`**, press **Enter**, and skip to step (h).

e When asked which Service OS you want to boot by default, type the appropriate selection. Then, press **Enter**.

f Specify how the boot menu should be handled in each ISO that you are creating. There are three choices:

0	Hide the boot menu from the user of the target device. The default service OS that you specified in step (d.e) will be used.
-1	Show the boot menu, and wait for a user response. The response will override the default Service OS setting.
Number greater than zero	Show the boot menu, and wait this number of seconds for a user response before booting into the default service OS specified in step (e).

g When asked if you want to change the port used to connect to the OS Manager infrastructure, type **Y** or **N**. The default port is 3466.

h When asked if want to specify the ISO boot load value that gets included in the ISO boot sector, type **Y** or **N**.

Use this option only if you experience problems using the default value and you have been instructed by HP Software Support to change it.

Certain hardware models require a boot load segment of 0x2000 due to a BIOS issue. Other models cannot boot from the CD when the boot load segment is something other than the default loader segment of the El Torito ISO format: 0x0000.

To specify the boot load segment setting, type **1**, **2** or **3**:

1 HPCA default (0x2000) – works with most BIOSs

2 ISO default (0x0000) – gets translated to 0x07c0 by most BIOSs

3 Manually enter a value

Then press **Enter**. If you typed **3**, specify the boot load segment setting as a hexadecimal string beginning with 0x.

i When prompted for the fully qualified path to the build items, type the directory name (such as `C:\build_items`), and press **Enter**.

This completes the questions pertaining to the Image Capture and Image Deploy ISOs.

10 When prompted for the fully qualified path for the temporary work directory, type a directory name (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.

11 When prompted for the fully qualified path for the output directory, type a directory name such as (`C:\build_output`).

> If you are prompted to create ISOs for CAS, type **N**.

The build process takes some time, as you will see from the on-screen messaging. When it is finished, you will see a message indicating that the Service OS creation process completed successfully and be returned to a command prompt.

Final steps:

After the build is completed, go to the directory where the `Windows PE.wim` was stored, such as `C:\WinPE_output`, and perform the following action:

Table 25

Boot Method for Target Devices	Action Required
PXE	Copy `winpe.wim` from the output directory to *`InstallDir`*`\BootServer\X86PC\UNDI\boot`
LSB	Use the CSDB Editor to replace `winpe.wim` in the LSB package.
CD	Create a new ISO using the Windows PE scripts.

If you chose to create `ImageCapture.iso` or `ImageDeploy.iso`, they will be stored in the same output directory.

Additional Information

After you provide all the information that the custom Windows PE service OS build script requires, the following things happen:

1. 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.
2. The information that you entered is saved, and the Windows PE directory creation begins.
3. If you indicated that you wanted to pause the WIM creation process to add extra drivers or packages, the process will pause after the Windows PE directory is created and the contents of `winpe.wim` are extracted into the WIM directory (for example, `C:\build_work\WIM`). There are two ways to do this:

   Method A: Use a Windows AIK tools to make your modifications.

   If you are using Windows AIK version 1.1, use the `peimg.exe` command. The default location of this executable file is:

   ```
   C:\Program Files\Windows AIK\Tools\PETools\peimg.exe
   ```

   If you are using Windows AIK version 2.0, use the `dism.exe` command. The default location of this executable file is:

   ```
   C:\Program Files\Windows AIK\Tools\Servicing\dism.exe
   ```

   Refer to the Windows AIK documentation for information about how to use these commands (or use the **`/help`** command line option).

   Method B: Add the drivers to a driver list.

   After you see a message indicating that all required information is gathered, the `build.config` file will be created in the `C:\Build_scripts` directory to store the information that is needed to build the `winpe.wim` and the ISOs. You can 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 "
   ```

Because the back-slash (\) is a special character, you must "escape" it by using two back-slashes, as shown in this example.

Note that all lines except the last end with a back-slash. In this case, the back-slash indicates a continuation of the declaration.

If you do not specify a directory, the script will search for the driver in the `<work-dir>\WIM\Windows\inf` directory.

If you prefer, you can provide a fully qualified path that specifies the location and driver, such as `c:\\anydirectory\\mydrivers.inf`

You can also specify 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 finished, 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.

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 various 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` file will be created and used.

Index

D

E

F

G

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **ca-docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: