

# HP Client Automation

## OS Manager

for the Windows® operating system

Software Version: 7.50

---

## System Administrator User Guide

Manufacturing Part Number: None

Document Release Date: May 2009

Software Release Date: May 2009



i n v e n t

## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notices

© Copyright 2003-2009 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER  
Copyright © 1996-1999 Intel Corporation.

TFTP SERVER

Copyright © 1983, 1993

The Regents of the University of California.

OpenLDAP

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.  
Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License

Copyright © 1998-2001 The OpenSSLProject.

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar  
Copyright Mihai Bazon, 2002, 2003

## Documentation Updates

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

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

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

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

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

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

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

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

Table 1 indicates changes made to this document.

**Table 1 Document changes**

<b>Chapter</b>	<b>Version</b>	<b>Changes</b>
All	5.10	General edits. Fixed outdated references.
All	7.20	General edits and rebranding. Removed version number for WinPE. Added cautions regarding Core and Satellite environments.
1	5.11 March 2008	Added note on page 18.
1	7.50	Added <a href="#">Support for SSL</a> on page 19.
1	7.20	Added information about the HP Client Automation Mini Management Server.
1	5.10	Added note on page 20.

<b>Chapter</b>	<b>Version</b>	<b>Changes</b>
1	7.20	Changed the note under Machine 2 in <a href="#">Image Deployment Infrastructure</a> on page 20.
1	5.10	Modified the steps in <a href="#">Using the HP Client Automation OS Manager</a> on page 23 to account for situations where you may use .WIM files.
1	7.20	Updated version number in <a href="#">Product Media</a> on page 27.
1	5.10	Added definition for <a href="#">Service Operating System (Service OS)</a> to <a href="#">Terminology</a> on page 27.
2	5.10	Changed from Target Requirements to Requirements.
2	7.20	Added information about thin clients in <a href="#">Target Devices</a> on page 32.
2	7.20	Removed list of operating systems in <a href="#">Server</a> on page 32.
2	7.20	Added Firewall Settings for Windows XPe Thin Client Devices from page 38.
2	7.50	Removed Firewall Settings for Windows XPe Thin Client Devices from page 38.
2	7.50	Added <a href="#">Symantec Endpoint Protection Agent Settings for Windows XPE</a> on page 34
2	7.50	Removed topic Installing the Application Manager on Thin Client
3	7.20	Updated the <a href="#">Prerequisites</a> on page 38.
3	7.50	Added topic <a href="#">IP Networking Support</a> on page 38.
3	5.10	Updated the <a href="#">Installation Checklist</a> on page 40.
3	5.10	In <a href="#">Installing the OS Manager Server</a> on page 41, added information about utilities necessary to capture images to be deployed by ImageX.
3	7.20	Updated name of log in the note on page 41.
3	7.50	In <a href="#">Installing the OS Manager Server</a> on page 41, added a caution and modified the instructions slightly.
3	7.50	In <a href="#">Enabling SSL Communication</a> on page 44, updated step 3.

<b>Chapter</b>	<b>Version</b>	<b>Changes</b>
3	5.10	In the <a href="#">Prerequisites</a> on page 46 for the Boot Server, added information to a note about the types of editors to use to modify the Boot Server's configuration files.
3	7.50	In <a href="#">About the Boot Server</a> on page 45, added a caution.
3	7.50	Added <a href="#">Enabling SSL Communication</a> on page 44
3	7.50	<a href="#">Configuring the Portal</a> on page 48, removed information about updating modules, adding directory services and modified the instructions for <a href="#">Configuring the Default Behaviors Instance</a> to use the CSDB Editor.
3	7.20	Added <a href="#">Installing the Client Automation Mini Management Server</a> on page 51.
3	5.10	Added <a href="#">Converting the Service OS to WinPE (optional)</a> on page 52.
3	7.50	Removed the section about the Admin Publisher.
4	7.50	Added chapter <a href="#">Disk Encryption</a> .
5	5.11 March 2008	Added information about capturing Windows Server 2008 operating systems.
5	5.11 March 2008	In <a href="#">Deployment Methods</a> on page 60, removed Windows NT 4 x86 as a supported platform. Microsoft no longer supports this product.
5	5.11 March 2008	In <a href="#">Deployment Methods</a> on page 60, updated Vista versions and added Windows Server 2008 versions supported.
5	7.20	Updated <a href="#">Deployment Methods</a> on page 60.
5	7.50	Added note on page 62 related to capturing images when using supported disk encryption products.
5	7.20	In <a href="#">Capturing pre-Windows Vista Operating Systems for Legacy Deployment</a> on page 63, modified the note in task 2.
5	7.20	In <a href="#">Capturing pre-Windows Vista Operating Systems for ImageX Deployment</a> on page 64, modified the note in task 2.
5	7.20	Added a task Copy utilities to the HPCA OS Manager Server to <a href="#">Capturing Windows Vista Operating Systems for ImageX Deployment</a> on page 66 and <a href="#">Capturing Windows Vista Operating Systems for Windows Setup Deployment</a> on page 75.

<b>Chapter</b>	<b>Version</b>	<b>Changes</b>
5	5.11 March 2008	In <a href="#">About the HP Client Automation OS Manager Image Preparation Wizard</a> on page 80, combined the list of files uploaded for both ImageX and WinSetup.
5	7.50	In <a href="#">About the HP Client Automation OS Manager Image Preparation Wizard</a> on page 80, added information about exit points for the Image Preparation Wizard.
5	7.50	Added <a href="#">Using the Image Preparation Wizard Exit Points</a> on page 81.
5	7.50	Added <a href="#">Preparing To Capture Remote Images</a> on page 82.
5	7.20	Updated <a href="#">To use the HPCA OS Manager Image Preparation Wizard</a> on page 83.
5	7.50	Updated note and changed it to a caution on page 83.
5	7.50	Added information about the <a href="#">Select Image Preparation Wizard payload window</a> on page 85.
5	7.50	Added <a href="#">Using the Image Preparation Wizard in Unattended Mode</a> on page 88.
5	7.20	Added <a href="#">Preparing and Capturing Thin Client OS Images</a> on page 92.
6	5.11 March 2008	In <a href="#">Prerequisites for publishing .WIM images of a Windows Vista OS or Windows Server 2008</a> on page 104, modified information about the /sources directory.
6	7.50	Updated information about spanned images in <a href="#">Prerequisites for publishing .WIM images of a Windows Vista OS or Windows Server 2008</a> on page 104
6	5.10	In <a href="#">Using the Admin Publisher</a> on page 107, added information about support for publishing .WIM files.
6	5.11 March 2008	In <a href="#">Using the Admin Publisher</a> on page 107, added a caution about the deployment method to be selected.
6	7.20 August 7, 2008	In <a href="#">Using the Admin Publisher</a> on page 107, modified step 5.
6	7.20	In <a href="#">Using the Admin Publisher</a> on page 107, modified step 8a.

<b>Chapter</b>	<b>Version</b>	<b>Changes</b>
6	7.20 August 7, 2008	In <a href="#">Using the Admin Publisher</a> on page 107, modified step 11.
6	7.50	Added topic <a href="#">Adding Drivers</a> on page 109.
7	7.20	Added a note about thin client limitations on page 114.
7	7.50	Updated table <a href="#">Expected Results on target device</a> on page 114 with encryption information.
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.
7	7.50	Removed EVNTDEST and USERTO from <a href="#">Attributes of the Behavior Class</a> on page 124.
7	7.50	In <a href="#">Table 8</a> on page 129, added information about the new partition type, Preserve.
8	7.20	Updated graphics.
9	7.50	Removed chapter OS Manager Support for HP Blades.
9	7.50	Chapter 9 is now Multicast and the OS Manager and all chapter numbers below have changed.
9	7.50	Removed information indicating that multicast does not support spanned images and that images must be a maximum of 4 GB.
9	7.50	Updated <a href="#">Minref</a> on page 149.
10	5.10	Updated prerequisites and added information about a new menu used to select the Service OS in <a href="#">Restoring Operating Systems</a> on page 176.
10	7.50	Updated first paragraph and added a note in <a href="#">Restoring Operating Systems</a> on page 176.
10	5.10	Updated the requirements for <a href="#">Using COP with OS Manager</a> on page 181.
11	7.50	Updated <a href="#">Building a Custom WinPE Service OS</a> on page 183.



<b>Chapter</b>	<b>Version</b>	<b>Changes</b>
12	5.10	Added chapter <a href="#">Building a Custom WinPE Service OS</a> on page 183.
12	7.20	<a href="#">Building a Custom WinPE Service OS</a> on page 183 no longer has separate instructions for earlier versions.
12	5.11	Modified chapter <a href="#">Building a Custom WinPE Service OS</a> on page 183 to have separate instructions for version 5.10 and 5.11.
12	5.11 March 2008	In the 5.11 section under <a href="#">Building a Custom WinPE Service OS</a> on page 183, the filename for winpe_i18n.wim was changed to winpe_cjk.wim.
12	5.11 March 2008	In the section <a href="#">Changing the Locale</a> on page 194, corrected the section in the sample default file to say [_SVC_LINUX_] from [SVC_LINUX].
12	7.50	<a href="#">Setting the System Language Parameter</a> on page 195, updated instructions to use the CSDB Editor
14	7.20	Updated <a href="#">Troubleshooting</a> on page 197.
14	5.10	Updated description of <a href="#">osclone.log</a> on page 199.
14	5.10	Added topic <a href="#">Locating the Payloads</a> on page 199.
A	7.20	Updated AppEvents table.
B	7.50	Updated introduction to <a href="#">User Messages</a> on page 215.

## Support

You can visit the HP Software support web site at:

**[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

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

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

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

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

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

To register for an HP Passport ID, go to the following URL:

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

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>17</b>
	Using this Guide with Core and Satellite Servers .....	19
	Support for SSL.....	19
	Product Architecture .....	19
	Target Devices.....	19
	Image Preparation Tools .....	19
	Image Deployment Infrastructure .....	20
	Using the HP Client Automation OS Manager .....	23
	OS Manager Components .....	23
	Product Media.....	27
	Related Documents.....	27
	Terminology .....	27
<b>2</b>	<b>System Requirements.....</b>	<b>31</b>
	Platform Support .....	32
	Server .....	32
	HP Client Automation OS Manager Server.....	32
	Target Devices .....	32
	Symantec Endpoint Protection Agent Settings for Windows XPE .....	34
	Additional configuration for XPE OS images .....	36
<b>3</b>	<b>Installing and Configuring the Server .....</b>	<b>37</b>
	IP Networking Support .....	38
	Prerequisites .....	38
	Installation Checklist.....	40
	About the OS Manager Server.....	40

Installing the OS Manager Server .....	41
Enabling Communication between the OS Manager and the Configuration Server ..	44
Enabling SSL Communication .....	44
About the Boot Server .....	45
Prerequisites.....	46
Installing the Boot Server .....	47
Configuring the Portal.....	48
Configuring the Default Behaviors Instance .....	49
About the Proxy Server .....	50
Configuring the Proxy Server.....	50
Installing the Client Automation Mini Management Server .....	51
Converting the Service OS to WinPE (optional).....	52
<b>4 Disk Encryption .....</b>	<b>53</b>
Prerequisites .....	54
Encryption Support Mode parameter (ENCMODE) .....	55
Using Microsoft's BitLocker.....	56
Reserved Space – RSVDSPACE in DRIVEMAP class .....	56
Local Service Boot and OSM client method updates .....	57
Partitioning Notes (DRIVEMAP class).....	57
<b>5 Preparing and Capturing OS Images .....</b>	<b>59</b>
Deployment Methods.....	60
Preparing and Capturing Images.....	62
Capturing pre-Windows Vista Operating Systems for Legacy Deployment .....	63
Capturing pre-Windows Vista Operating Systems for ImageX Deployment.....	64
Capturing Windows Vista Operating Systems for ImageX Deployment .....	66
Capturing Windows Server 2008 for ImageX Deployment .....	67
Capturing pre-Windows Vista Operating Systems for Windows Setup Deployment..	69
Capturing Windows Vista Operating Systems for Windows Setup Deployment .....	75
Capturing Windows Server 2008 for Windows Setup Deployment .....	76
Using Microsoft Sysprep .....	78
How Sysprep.inf files are prioritized.....	79

About the HP Client Automation OS Manager Image Preparation Wizard .....	80
Using the Image Preparation Wizard Exit Points .....	81
Preparing To Capture Remote Images .....	82
Using the HPCA OS Manager Image Preparation Wizard .....	83
Using the Image Preparation Wizard in Unattended Mode .....	88
Preparing and Capturing Thin Client OS Images .....	92
Windows XPe OS images .....	92
Windows CE OS images .....	96
Linux-based OS images .....	98
<b>6 Publishing to the HPCA CS Database .....</b>	<b>103</b>
Prerequisites for publishing .WIM images of a Windows Vista OS or Windows Server 2008 .....	104
About the .subs and .xml files .....	105
Example of Substitution .....	106
Preparing filename.xml .....	107
Using the Admin Publisher .....	107
Adding Drivers .....	109
Prerequisites .....	110
<b>7 Preparing Content .....</b>	<b>113</b>
About Discovery .....	114
About Policy .....	116
Determining Policy Assignments .....	117
Preparing Content Using the CSDB Editor .....	119
Logging On .....	122
About the OS Manager Classes .....	122
Setting Behaviors .....	123
Creating a Manufacturer or Model Instance .....	128
Assigning Operating Systems .....	128
Defining Drive Layouts .....	129
Adding Partitions .....	132
Assigning Drive Layouts .....	134
Using an Override Sysprep File .....	134

8	Implementing the OS Manager Server.....	137
	About the PXE-Based Environment.....	138
	Best Practices for PXE-Based Implementations.....	138
	Networking Boot with PXE .....	139
	About Local Service Boot .....	141
	Prerequisites.....	141
	Best Practices for Using Local Service Boot.....	142
	Booting with Local Service Boot .....	143
	Managing Your Devices.....	145
9	Multicast and the OS Manager .....	147
	Prerequisites .....	148
	Requirements .....	148
	Configuring Multicast for OS Manager.....	148
	Improving Performance and Reliability for Multicast with OS Manager .....	150
	Terminology .....	151
	About the Multicast Parameters.....	152
	How the Parameters Influence Multicast Data Transfer.....	155
	Understanding Inter-packet Delay .....	155
	About the Buffer Settings .....	156
	Handling Special Packets .....	157
	Handling the End of Image.....	158
	Auto Throttle.....	158
	Analyzing Problems.....	159
	About the Logs.....	159
	Poor Performance .....	159
	Client Time-out .....	161
	Total Image Transfer Time-out .....	161
	Network Inactivity Time-out .....	162
	Buffer Overflow .....	162
	Slow Client.....	163
	Missing Data.....	163
	Test Modules .....	165
	Using GDMCSEND.....	165
	Using GDMCRECV .....	170

Example of Using the Test Modules .....	173
Sample Test Configuration .....	174
<b>10 Advanced Features .....</b>	<b>175</b>
Restoring Operating Systems .....	176
Addressing Requirements for Capturing, Recovering, and Migrating Data .....	179
Sample Command Lines .....	180
Return Codes for HP Exit Points .....	180
Using COP with OS Manager .....	181
Requirements .....	181
Using the Proxy Server with OS Manager Server and Client Operations Profiles .....	182
<b>11 Building a Custom WinPE Service OS .....</b>	<b>183</b>
Prerequisites .....	184
Adding Drivers to the WinPE Service OS .....	186
Building a Custom WinPE Service OS and Maintaining the ISOs .....	187
Using Customized build.config Files (Advanced Option) .....	191
<b>12 Double Byte Character Support .....</b>	<b>193</b>
Supported Languages .....	194
Changing the Locale .....	194
Setting the System Language Parameter .....	195
Double-byte support for Sysprep or Unattend.txt files .....	196
<b>13 Troubleshooting .....</b>	<b>197</b>
OS Manager Server Logs .....	198
Locating the Payloads .....	199
Configuration Server and Configuration Server DB Logs .....	199
Image Preparation Wizard Log .....	199
Agent Logs and Objects .....	200
Capturing, Migrating, or Recovering Data .....	200
Basic Infrastructure Tests .....	201
Test Results .....	202

Collecting Information for Technical Support .....	202
Gathering Version Information .....	203
OS Manager Server Components .....	203
OS Manager Admin Module .....	203
NVDKIT.EXE and .TKD Files .....	204
Configuration Server and Configuration Server Database .....	204
SOS/Payload/OS Manager System Agent.....	204
OS Manager Boot Loader .....	204
Frequently Asked Questions.....	205
Using the Discover Boot Server Utility.....	208
A AppEvents .....	209
B User Messages.....	215
C Storing Multiple Logs .....	219
Index .....	221



---

# 1 Introduction

This chapter includes the following topics:

- [Using this Guide with Core and Satellite Servers](#)
- [Product Architecture](#)
- [Using the HP Client Automation OS Manager](#)
- [OS Manager Components](#)
- [Product Media](#)
- [Related Documents](#)
- [Terminology](#)

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



As of version 7.50, any time you are prompted for the OS Manager Server's IP address and port number, you must now specify the port number (by default 3469). If you do not specify the port number, the port will default to 3466, and OS Management will not work correctly.

This does not apply to Core and Satellite environments.

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



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.

## 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.



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

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



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

See [Preparing and Capturing OS Images](#) on page 59 for additional information.

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

#### **HP Client Automation Administrator Publisher**

Use the Publisher to store the image and its associated files in the Configuration Server DB. You can also use the Publisher to publish other files—such as override *Sysprep.inf* files or *unattend.txt* files—to the SYSPREP class in the Configuration Server DB. See [Preparing and Capturing OS Images](#) on page 59.

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

## Image Deployment Infrastructure

The image deployment infrastructure is comprised 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



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

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

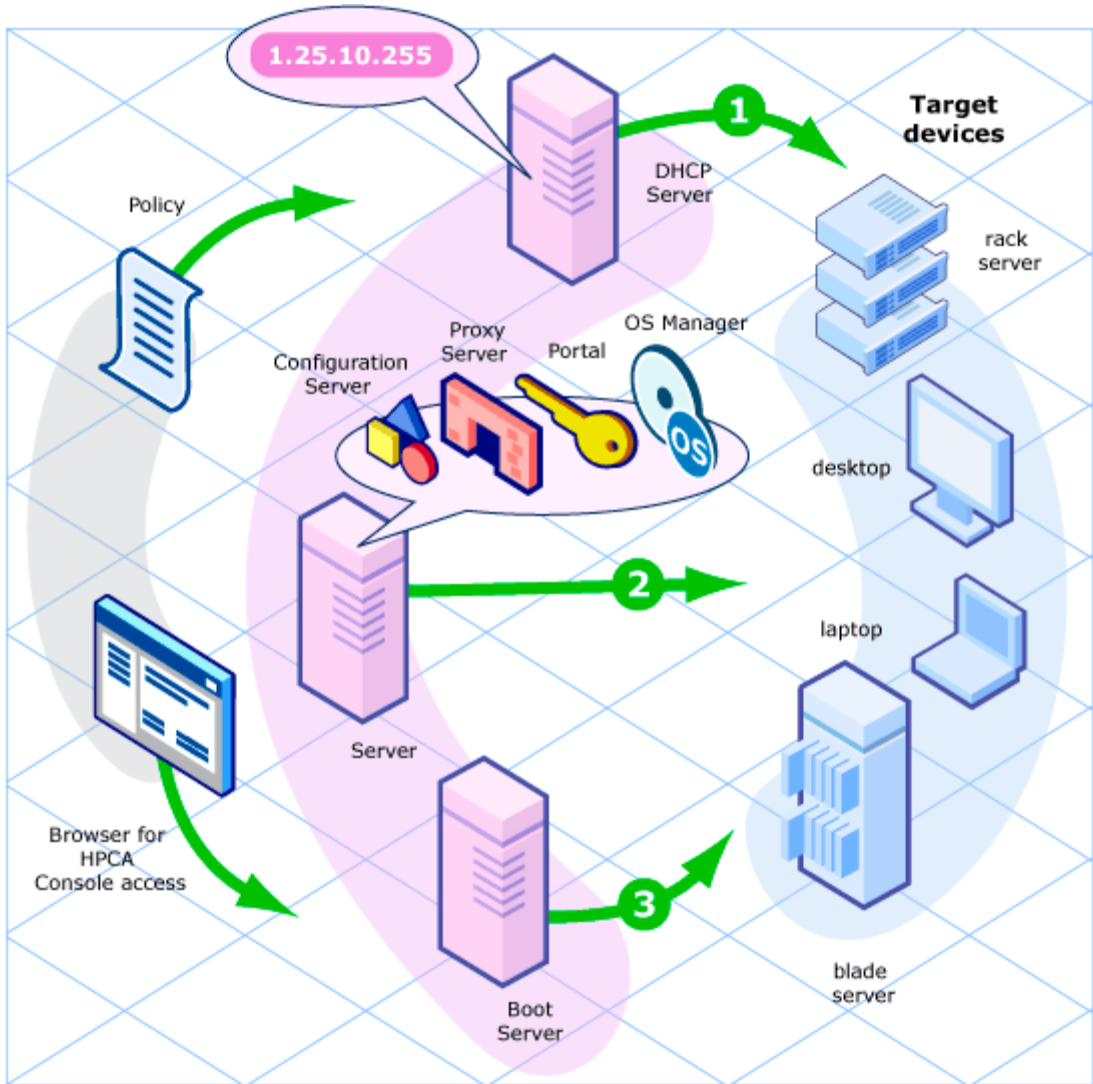


Do not install the Boot Server on the same machine as your DHCP server. See [About the Boot Server](#) on page 45.

See [Installing and Configuring the Server](#) on page 37.

Figure 1 below illustrates the deployment architecture.

**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 59. After you create the image, it is stored on the OS Manager Server.
- 3 Use the Publisher to publish the image files from the OS Manager Server to the Configuration Server DB.
- 4 (Advanced) Use the CSDB Editor to create, modify and prepare content for use in production deployments.
- 5 Use the Enterprise Manager 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.

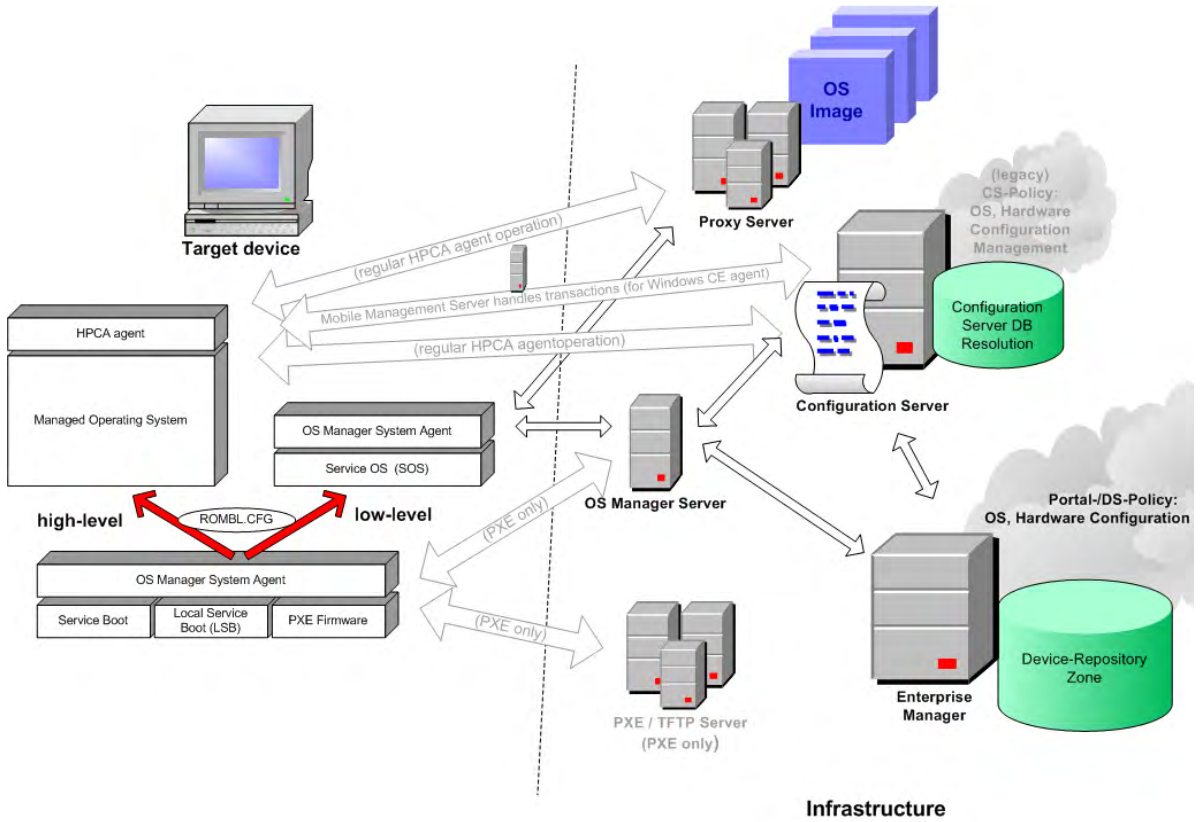
- **HP Client Automation Application Manager** is the agent that runs in the operating system of the target device and is used to manage service packs, patches, hot fixes, applications, and other content. It also works with the HP Client Automation OS Manager Boot Loader and the HP Client Automation 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.
- **HP Client Automation Enterprise Manager** is the web interface console used to manage devices, software, operating systems and patches as well as create and view reports 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, and determines which operating systems qualify for installation on the managed device.



- **HP Client Automation Mini Management Server** handles transactions between the agent and the HPCA Configuration Server when using Windows CE.
- **HP Client Automation Portal** stores information about the target devices in your environment.
- **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 allows 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**



# Product Media

In order to install the product, you must use the OS Manager 7.50 media. Before you begin, you may want to create two additional CD/DVDs:

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

## Related Documents

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

## Terminology

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

### [bare metal machine](#)

A device that does not have a local OS installed.

### [HP Client Automation agent](#)

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

### [HP Client Automation OS 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 object

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

### discovery

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

### gold image

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

### managed device

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

### native installation

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

### OS state

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

### reference machine

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

### ROM object

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

### Service Operating System (Service OS)

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

### target device

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

## unmanaged OS

An unmanaged OS can be either:

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

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



---

## 2 System Requirements

This chapter includes the following topics:

- Platform Support
- Server
- HP Client Automation OS Manager Server
- Target Devices

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](#) on page 34.
- If you are using VMware as the target device, change your target device's .vmx file to contain the following:

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

- If you want to report on, or make use of the device's make, manufacturer, and unique identifier for policy, the BIOS must support SMBIOS (for systems management) specification. If a target device lacks SMBIOS support, the only criterion available for specifying policy on that device will be the MAC address.
- An English, French, or German keyboard.
- A minimum of 128 MB of RAM.
- 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 WinPE Service OS](#) on page 186. If you are using a Linux SOS, HP will provide periodic updates of the Linux SOS.

## Symantec Endpoint Protection Agent Settings for Windows XPE

Windows XPE 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 Windows XPE as **Administrator**.
- 2 Right-click the Symantec icon in the system tray and select **Advanced Rules**.
- 3 Click **Add**.
- 4 On the General tab:
  - Add description **Allow HPCA Agent**.
  - Select Allow this traffic.
- 5 On the Applications tab, click **Browse** to add the following applications from C:\Program Files\Hewlett-Packard\CM\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:
  - Add description Allow HPCA Ports.
  - 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 XPE OS images

If you will be capturing Windows XPE operating system images, you will also need to allow access to the Image Preparation Wizard executable (`prep wiz.exe`). Note that `prep wiz.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 `prep wiz.exe`. The `prep wiz.exe` can be found in *CD Drive:\image\_preparation\_wizard\win32*.

---

# 3 Installing and Configuring the Server

This chapter includes the following topics:

- IP Networking Support
- Prerequisites
- Installation Checklist
- About the OS Manager Server
- About the Boot Server
- Configuring the Portal
- About the Proxy Server
- Installing the Client Automation Mini Management Server
- Converting the Service OS to WinPE (optional)

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

With this release, HP Client Automation adds support for **IPv6**—the latest version of the internet protocol addressing structure—to its Windows-based Core and Satellite servers. The Core and Satellite servers can now use either IP version 4 (**IPv4**) or IP version 6 (**IPv6**) for server-to-server communications. HPCA agent communications, however, are currently limited to IPv4. For details, refer to the appendix, *IPv6 Networking Support*, in the *HPCA Enterprise User Guide*.



HP Client Automation environments that use the traditional, component-based, HPCA server installations will continue to be supported on 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 7.50 or higher.



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

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

- HP Client Automation Configuration Server Database, version 7.50 or higher.



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

- HP Client Automation Administrator, version 7.50 or higher.
- HP Client Automation Proxy Server, version 7.50 or higher.
- HP Client Automation Portal, version 7.50 or higher.
- HP Enterprise Manager, version 7.50 or higher
- Microsoft Internet Explorer with the security level set no higher than medium.

# Installation Checklist

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

- 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 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 installed in `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\modules`.



To check that your license string is valid, open `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\logs\httpd-osm-port.log` and search for “License is expired”. If you find this string, you must update your license file. See [OS Manager Server Logs](#) on page 198 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 `SystemDrive:\Program Files\Hewlett-`

Packard\CM\OSManagerServer\etc\roms.cfg. If you want to change the User ID (PORTAL\_UID) and Password (PORTAL\_PASS), you must do it in roms.cfg. See [Enabling Communication between the OS Manager and the Configuration Server](#) on page 44 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.

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

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

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

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

If you are using a password to access your Configuration Server

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

```
password encrypt your password aes
```

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

The encrypted password will resemble:

```
<AES256>kITMqDenvFUdpBaYt8XBg==
```

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



The literal string `<AES256>` and the equal signs (`==`) must be included.

- 6 Restart the HPCA OS Manager service.

## Enabling SSL Communication

The OS Manager can be used as an SSL client when communicating with the Configuration Server and Portal. See the *HP Configuration Management 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 `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\etc\roms.cfg` change:  
  
`PORTAL_USE_SSL 0`  
`RCS_USE_SSL 0`  
  
to  
  
`PORTAL_USE_SSL 1`  
`RCS_USE_SSL 1`
- 7 In `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\etc\roms.cfg` change the port in the `RCS_ADDRESS` and the `RIBPORT` to match the SSL port being used.
- 8 Open `edmprof.dat` in the Configuration Server's `bin` directory 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.
- Install the Boot Server on a machine separate from your DHCP server because the PXE server and the DHCP server listen on the same DHCP port by default.
- Do not install the Boot Server on a machine that has cygwin installed because this is not supported.
- If you have more than one PXE server in your environment, each must be on a separate segment and the PXE packets should not pass between the segments. You can use the Discover Boot Server utility to determine if there are PXE servers in your environment. See [Using the Discover Boot Server Utility](#) on page 208.
- A static IP address for the Boot Server.

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

Do not use editors that automatically convert to Windows

format, such as Notepad. Use Nano or WordPad to modify the Boot Server's configuration files.

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



To enable PXE in your network environment:

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

For the Cisco switch, use the following:

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

For all other vendors, consult their documentation.

## Installing the Boot Server

### To install the Boot Server

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

The Boot Server Install window opens.

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



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

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

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

- 5 Click **Next**.
- 6 Review the installation summary and click **Install**.

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

- 7 Click **Finish**.



If you want to check that the installation was successful:

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

or

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

## Configuring the Portal

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

To update the `edmprof.dat` file

- 1 Open `edmprof.dat` in the Configuration Server's `bin` directory.
- 2 In the [MGR ROM] section
  - Set `PORTAL_HOST` to the IP address for the Portal.
  - Set `PORTAL_PORT` to the port for the Portal.
  - The `PORTAL_ZONE` setting contains the value that you specified when you installed the Configuration Server.
  - Set `DISPLAYNAME` to the same value as the `DISPLAYNAME` attribute in `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\etc\roms.cfg`.

This ensures that the display name for the device is updated when the OS Manager Server interfaces with Portal. If you chose the default during the installation, set this to **compname**.

- `PORTAL_UID` contains the ID of a Portal user who can update a device or the ROM object.
- `PORTAL_PASS` contains the password for the Portal user who can update a device or the ROM object.



```

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

```

```

[MGR_ROM]
PORTAL_HOST = 192.168.1.9
PORTAL_PORT = 3471
PORTAL_ZONE = cn=Home,cn=radia
DISPLAYNAME = compname
PORTAL_UID = {AES256}ACuqUOk5jOzI23B243dvgw==
PORTAL_PASS = {AES256}3gMlspnbrGbqVXNPDx8tWg==

```

- 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 123.

### To configure the default Behaviors instance

- 1 Log on to the CSDB Editor.  
See [Logging On](#) on page 122 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 “,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 `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc`.

- 1 Stop the HPCA Integration Server service.
- 2 Open `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\rps.cfg`.
- 3 Change the `-static-root` parameter (which is the source location) to the location of the Configuration Server DB (such as `C:/Program Files/Hewlett-Packard/CM/ConfigurationServer/DB`). Be sure to use forward slashes.
- 4 Change the `-static-type` parameter from **agent** to **server**.
- 5 Save the file.

- 6 Restart the HPCA Integration Server service.

These changes are shown in bold in the excerpt below.

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

## Installing the Client Automation Mini Management Server

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

### To install the Mini Management Server

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


The Client Automation Mini Management Server Install window opens.

- 2 Click **Next**.  
The End User License Agreement window opens.
- 3 Click **Accept**.
- 4 Click **Next** to accept the default directory.
- 5 Type the IP address or name of the Client Automation Configuration Server and click **Next**.
- 6 Type the IP address or name of the Client Automation OS Manager Server and click **Next**.
- 7 Click **Install**.

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


## Converting the Service OS to WinPE (optional)

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

 Changing the default Service OS will affect newly discovered target devices in OS Manager 7.50 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 Modify the settings for PXE by opening the Boot Server's default file (typically located in `SystemDrive:\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot\linux.cfg`), and:

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

- In the OS Manager section, change the DFTLSVOS to `_SVC_PEX86_`.
  - Save and close the file.
- 2 Modify the setting for LSB by opening the Client Automation Admin CSDB Editor and going to PRIMARY, OS, Operating Systems (ZSERVICE), Local Service Boot and in the right pane scrolling to the Service OS List (ELGBLSOS) attribute.
    - Double-click the attribute and change the setting to `_SVC_PEX86_`.
    - Save, and close the Admin CSDB Editor.
  - 3 Modify your deployment CD-ROM as instructed in [Building a Custom WinPE Service OS](#) on page 183.

---

# 4 Disk Encryption

This chapter includes the following topics:

- Prerequisites
- Encryption Support Mode parameter (ENCMODE)
- Using Microsoft's BitLocker

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.

In 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 Recovery ([PMDISRCV](#)). If you want to perform disaster recovery, you must use the OS Management Wizard with the Emergency Mode option selected in Enterprise Manager 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 2 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's BitLocker

Microsoft's BitLocker encryption technology is significantly different than other 3<sup>rd</sup> 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 RSVDSPCE 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:

- Deployment Methods
- Preparing and Capturing Images
- Using Microsoft Sysprep
- About the HP Client Automation OS Manager Image Preparation Wizard
- Preparing and Capturing Thin Client OS Images

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



As of version 7.50, any time you are prompted for the OS Manager Server's IP address and port number, you must now specify the port number (by default 3469). If you do not specify the port number, the port will default to 3466, and OS Management will not work correctly.

This does not apply to Core and Satellite environments.



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

## Deployment Methods

Table 3 on page 61 provides information about the three methods (Legacy, Microsoft ImageX, and Microsoft Windows Setup) that can be used to deploy an image.

**Table 3      Deployment methods**

<b>Method</b>	<b>Service OS Type*</b>	<b>Image format</b>	<b>Resulting Files**</b>	<b>Supported Platforms</b>
Legacy	Linux	sector-based image	ImageName.IMG ImageName.MBR ImageName.EDM ImageName.PAR <b>For WinXPe or Windows CE, the files are:</b> ImageName.IBR ImageName.EDM <b>For Linux, the files are:</b> ImageName.DD ImageName.EDM	Windows 2000 Workstation, Server, and Advanced Server x86 Windows XP x86 or AMD64/EM64 Windows 2003 Server and Advanced Server x86 or AMD64/EM64 Windows XP Embedded Windows CE Debian Linux HP Thin Connect
Microsoft ImageX	WinPE	.WIM file-based format	ImageName.WIM ImageName.EDM	Windows XP SP2 (or later) Professional x86 or AMD64/EM64T Windows Vista Enterprise, Business and Ultimate Edition x86 or AMD64/EM64T Windows Server 2008 Standard and Business edition x86 or AMD64/EM64T Windows 2003 Server SP1 and Advanced Server x86 or AMD64/EM64
Microsoft Windows Setup	WinPE	.WIM file-based format	ImageName.WIM ImageName.EDM	Windows Vista Enterprise, Business and Ultimate Edition x86 Windows Server 2008 Standard and Business edition x86

\*You must have the compatible drivers for the target device in the SOS. If you are using WinPE and the drivers are not available, see [Adding Drivers to the WinPE Service OS](#) on page 186. If you are using a Linux SOS, HP will provide periodic updates of the Linux SOS.

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

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

## Preparing and Capturing Images

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

► If you are planning to use supported [Disk Encryption](#) products the image must be captured from an *unencrypted* partition.

- [Capturing pre-Windows Vista Operating Systems for Legacy Deployment](#), on page 63
- [Capturing pre-Windows Vista Operating Systems for ImageX Deployment](#), on page 64
- [Capturing Windows Vista Operating Systems for ImageX Deployment](#), on page 66
- [Capturing Windows Server 2008 for ImageX Deployment](#), on page 66
- [Capturing pre-Windows Vista Operating Systems for Windows Setup Deployment](#), on page 69
- [Capturing Windows Vista Operating Systems for Windows Setup Deployment](#), on page 75
- [Capturing Windows Server 2008 for Windows Setup Deployment](#), on page 76
- [Preparing and Capturing Thin Client OS Images](#) on page 92

# Capturing pre-Windows Vista Operating Systems for Legacy Deployment

## Task 1 Prepare the Reference Machine

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



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

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

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

- 3 Install the HP Client Automation Application Manager 7.50 for Windows with the OS Manager feature from the HPCA agent media. The Application Manager is required so that when the OS image is deployed, the device can connect to the OS Manager Server. If you need to update the Application Manager, you must use agent self-maintenance.
- 4 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.
- 5 Keep the image file size as small as possible. The ideal configuration is a partition just large enough to fit the operating system, plus additional space for the HPCA agent.



HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see [Adding Partitions](#) on page 132.

The following helps minimize the size of the image file.

- a Create free space.  
HP recommends that after you have created the smallest partition with the least amount of free disk space as possible, set the `ExtendOemPartition = 1` in the [Unattended] section of `Sysprep.inf`, to allow for the small image to be installed on a target device with a much larger drive. When the `ExtendOemPartition` is set to true, the

Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The Application Manager can then use the free space on the volume for application installations.

- b Disable hibernation if you are using a laptop.
- c If necessary, remove the recovery partition.
- d Disable the paging file. The page file will be enabled automatically when mini-setup is run after the deployment.
- e Turn off System Restore.
- f Turn off Indexing Service and Disk Compression.
- g Turn off On Resume Password Protect.

### **Task 2** Pre-requisites

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



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

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

See [Using Microsoft Sysprep](#) on page 45 for details.

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

See [About the HP Client Automation OS Manager Image Preparation Wizard](#) on page 80.

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

### **Task 2** Copy utilities to the HPCA OS Manager Server

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



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

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

## Task 2 Prepare the Reference Machine

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



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

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

- 2 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.
- 3 Keep the file system as small as possible which will minimize the size of the .WIM file.



HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see [Adding Partitions](#) on page 132.

- a Delete unnecessary files and directories from the files system.
- b Turn off System Restore.

## Task 3 Pre-requisites

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



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

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

See [Using Microsoft Sysprep](#) on page 45 for details.

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

See [About the HP Client Automation OS Manager Image Preparation Wizard](#) on page 80.

## Capturing Windows Vista Operating Systems for ImageX Deployment

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

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

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

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

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

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



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

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

- 2 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.
- 3 Turn off User Access Control.
- 4 Keep the file system as small as possible which will minimize the size of the .WIM file.



HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see [Adding Partitions](#) on page 132.

- a Delete unnecessary files and directories from the files system.
- b Turn off System Restore.

### **Task 3** Prepare unattend.xml

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

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

See [About the HP Client Automation OS Manager Image Preparation Wizard](#) on page 80.

## Capturing Windows Server 2008 for ImageX Deployment

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

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

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

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

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

## Task 2 Prepare the Reference Machine

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



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

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

- 2 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.
- 3 Turn off User Access Control.
- 4 Keep the file system as small as possible which will minimize the size of the `.WIM` file.



HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see [Adding Partitions](#) on page 132.

- a Delete unnecessary files and directories from the files system.
- b Turn off System Restore.

## Task 3 Prepare `unattend.xml`

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

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

See [About the HP Client Automation OS Manager Image Preparation Wizard](#) on page 80.


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

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

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

#### **Task 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 OS Manager media and that the reference machine meets the following requirements:

- 1 Connectivity to a OS Manager Server.
  - 2 A target drive, recommended being on an extended partition, that:
    - Will be used as if the target drive is currently formatted and empty (has no data). If the target drive is not formatted or it is formatted and contains data, the user will be prompted to format the drive.
    - A user can pre-format the drive with FAT32 if they format the drive and ensure that there is no data on the drive.
-  Note that FAT32 cannot be expanded after deployed. NTFS can be expanded and is the default.
- Is at least 1.5 GB. If the target drive is larger, it will take more processing time when the drive is imaged or the image may be larger than necessary depending on how the “Optimize Compression of Unused Disk Space” check box is set in the HPCA OS Manager Image Preparation Wizard.



All data on the target drive will be lost.

- 3 A separate drive (to increase speed), such as the `C:` drive, with the HPCA Windows Native Install Packager software already installed. See [Install the HPCA Windows Native Install Packager](#) on page 71.
- 4 You must also have access to the following items; specify their location when using the HPCA Windows Native Install Packager:
  - The setup files for the Application Manager.
  - The `i386` directory from your operating system media. You can slipstream any necessary service packs into this directory. See the `readme.txt` file associated with each service pack for more information about how to do this.



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

- If your device is running Windows XP, you cannot use the `i386` directory for Windows 2000.
  - If your device is running Windows 2003, you cannot use the `i386` directory for Windows 2000 or Windows XP.
- `Unattend.txt`  
You can create the file manually or use Windows Setup Manager on your Windows media. Sample files are available on the Image Capture media in `\samples`.

## Task 5 Create `Unattend.txt`

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



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

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

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

You must use the [GuiUnattended] section, rather than `$OEM$\cmdlines.txt`, because the Application Manager setup uses Windows installer to install the Application Manager on the target device and `$OEM$\cmdlines.txt` cannot run the Windows Installer. The `AutoLogon` and `AutoLogonCount` statements ensure that the Application Manager is installed during the first user logon after the operating system is installed.

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

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

- You can also create separate `unattend.txt` files for any necessary customizations. You can use the Admin Publisher to publish these files to the SYSPREP class in the Configuration Server DB and then you can connect them to the appropriate OS image. See [Using an Override Sysprep File](#) on page 134. When the image is deployed, the customized `unattend.txt` will be merged with the original file.



See [Using the Admin Publisher](#) on page 107 for information about the Admin Publisher. When publishing `Unattend.txt` files, follow the instructions as if you were publishing a `Sysprep.inf` file.

## Task 6 Install the HPCA Windows Native Install Packager

- 1 On the Image Capture media, go to `\windows_native_install` and double-click **setup.exe**.
- 2 Click **Next**.  
The End User License Agreement window opens.
- 3 Review the terms and click **Accept**.
- 4 Select the directory to install the product in and then click **Next**.  
The Summary window opens.
- 5 Click **Install**.

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

## Task 7 Run the HPCA Windows Native Install Packager

To run the HPCA Windows Native Install Packager

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

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

- a The Client Automation area contains options used to set up options related to Client Automation products.
- b The Windows Setup area gathers information needed to perform the OS installation.
- c The Package area gathers information needed by HPCA about the package that you are creating.



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

- 2 In the Client Automation Client Source Directory field, enter the path for the Application Manager.
- 3 Select the check boxes for the Client Automation products that you want installed.
- 4 Select the Run first connect after install check box to perform an HPCA OS connect after the OS is installed. If this is not selected, the HPCA OS connect will not occur automatically after the OS is installed.
- 5 In the Optional Packager Command Line Arguments box, type parameters used by the WNI application. The options can be placed all on one line or on several lines. Specify the options in the keyword-value format, such as

```
-trace_level 9
```

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





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

There are many parameters that can be used to create logs. The following example describes how to create a file called

```
C:\temp\nvdwni.log.
```

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

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

- `-trace_file filename.log`

6 Click **Next**.

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

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



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

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



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

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



All existing data found on this drive will be lost.

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

- 11 Click **Next**.
- 12 In the Image Name text box, type the name of the package that will be stored in the `\upload` directory on the OS Manager Server. This name has a maximum length of eight characters and should be composed of alphanumeric characters only.
- 13 In the Image Description text box, type a description of the image (up to 255 characters).
- 14 In the Client Automation OS Manager Server text box, specify the IP address or host name for the OS Manager Server where the image should be uploaded.
- 15 In the Client Automation OS Manager Port text box, specify the port for the OS Manager Server.
- 16 Select the Optimize Compression of Unused Disk Space check box to null all unused disk space on the target drive before imaging it. This reduces the size of the image but causes the HPCA OS Manager Image Preparation Wizard to run longer.
- 17 Click **Next**.
- 18 Review the Summary and then click **Create**.



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

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

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



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

- 20 Insert the Image Capture media, and then click **OK**.
- 21 Click **Finish**.
- 22 Reboot the device and the image is uploaded to your OS Manager Server's `\upload` directory.

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

## Capturing Windows Vista Operating Systems for Windows Setup Deployment

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

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

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

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

### Task 2 Prepare the Reference Machine

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



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

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

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

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



HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see [Adding Partitions](#) on page 132.

- a Delete unnecessary files and directories from the files system.
  - b Turn off System Restore.
- 5 If you are going to run the HPCA OS Manager Image Preparation Wizard from the Image Capture media, set the boot order to CD-ROM first. If you are going to run the HPCA Image Preparation Wizard from another location, set the boot order to network first.

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

See [About the HP Client Automation OS Manager Image Preparation Wizard](#) on page 80.

## Capturing Windows Server 2008 for Windows Setup Deployment

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

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

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

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

## Task 2 Prepare the Reference Machine

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



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

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

- 2 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the OS Manager Server is finished.
- 3 Turn off User Access Control.
- 4 Keep the file system as small as possible which will minimize the size of the .WIM file.



HP supports deploying the image to the primary boot partition of the primary boot drive. If you want to add additional partitions to the primary boot drive, see [Adding Partitions](#) on page 132.

- a Delete unnecessary files and directories from the files system.
  - b Turn off System Restore.
- 5 If you are going to run the HPCA OS Manager Image Preparation Wizard from the Image Capture media, set the boot order to CD-ROM first. If you are going to run the HPCA OS Manager Image Preparation Wizard from another location, set the boot order to network first.

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

See [About the HP Client Automation OS Manager Image Preparation Wizard](#) on page 80.

# Using Microsoft Sysprep

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

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

## To set up Sysprep

- 1 Go to `DEPLOY.CAB` in the `SUPPORT\TOOLS` folder of the Microsoft operating system installation media. See Microsoft's documentation for details.
- 2 Extract the Microsoft Sysprep files from the `Deploy.cab` file using the appropriate operating system media. Copy these files to `C:\SysPrep` on the reference machine and make sure the directory and files are not set to read-only.



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

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

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

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

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

- 3 Be sure that the reference machine is part of a `WORKGROUP` and not a domain in order to use the Microsoft Sysprep.
- 4 Create a `Sysprep.inf` and save it to `C:\Sysprep`.

## To create Sysprep.inf

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



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

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



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

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

- Adjust the `TimeZone` value for your enterprise.
- Set up the `AdminPassword`.
- Make sure to include a product key so that the user will not need to enter this at the target device.
- In order to have an unattended installation, you must include `UnattendMode = FullUnattended` in the `[Unattended]` section.
- Set `ExtendOemPartition` to 1, so that Microsoft Sysprep will extend the OS partition into any available non-partitioned space that physically follows on the disk.
- If `JoinDomain` is present in `Sysprep.inf`, then `Sysprep.inf` has to have the Admin User ID and Password of an account in the domain that has the rights to join the computer to the domain. Note that `JoinDomain` is case sensitive.

## How Sysprep.inf files are prioritized

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

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

- 1 Sysprep embedded in the image (lowest priority). If there is no separately published `Sysprep.inf` (override Sysprep), just the `Sysprep.inf` in the image will be used.
- 2 Override Sysprep (a Sysprep file that is separate from the gold image. See [Using an Override Sysprep File on page 134](#) for details).
  - ▶ Only one override `Sysprep.inf` will be resolved.
- 3 Sysprep attached to policy criteria (highest priority).
  - ▶
    - To attach a Sysprep file to policy, you must publish the Sysprep file to the Configuration Server DB and then use the Admin CSDB Editor to manually connect the Sysprep instance to the appropriate Policy instance.
    - Even if you override the `Sysprep.inf`, the `ComputerName` (COMPNAME) and `JoinDomain` (COMPDOMN) are still updated by the OS Manager based on the Computer Name and Domain stored in the ROM object in the Portal.

## About the HP Client Automation OS Manager Image Preparation Wizard

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

- 1 Creates an object that contains information (including hardware and OS information capabilities) about the reference machine.
- 2 (Optional Exit Points, not available for Legacy images) Executes the exit points that are available for your use as needed. `PRE.COMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.COMD` is executed after Sysprep has sealed the image. See [Using the Image Preparation Wizard Exit Points on page 81](#) for details.
- 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.
- 5 Creates and copies files to `SystemDrive:\Program Files\SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload` on the OS Manager Server.

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

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

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

- `ImageName.WIM`  
This file contains a set of files and file system information from the reference machine.
- `ImageName.EDM`  
This file contains the object containing inventory information.

## Using the 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.



This is not supported for Legacy images.

To use the exit points:

- 1 Create the files `PRE.COMD` and `POST.COMD`.

- 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%\prep wiz\pre` and `%temp%\prep wiz\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.

## Preparing To Capture Remote Images

The following section explains how to prepare images on remote machines.



Currently supported for Microsoft Image X only.

### To capture remote images

- 1 Connect to the remote machine to be captured.
- 2 Copy `\image_preparation_wizard` from the ImageCapture media to a network share. See [Product Media](#) on page 27 if you need more information about where to get this media.
- 3 Map a drive from the remote machine to be imaged to the network share that has `\image_preparation_wizard`.
- 4 Prepare the remote machine as necessary. See the following for information on how to prepare the machine.
  - [Capturing pre-Windows Vista Operating Systems for ImageX Deployment](#), on page 64
  - [Capturing Windows Vista Operating Systems for ImageX Deployment](#), on page 66
  - [Capturing Windows Server 2008 for ImageX Deployment](#), on page 66

# Using the HPCA OS Manager Image Preparation Wizard

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 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.

When capturing a remote image, the CD-ROM is not required. See [Preparing To Capture Remote Images](#) on page 82

- 1 Insert the ImageCapture media into the reference machine. See [Product Media](#) on page 27 if you need more information about where to get this media.
- 2 Go to `\image_preparation_wizard` and double-click `prep wiz.exe`.

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

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

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

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



Note that when you plan to deploy using Windows XP Service Pack 2, Windows Vista or Windows 2008 using ImageX or Windows Setup, the 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`. See *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` before using the Admin Publisher to publish the image to the Database.



When using the Admin Publisher, you will be given an option to select where to publish the agent from. This is advantageous because you can package the agent independently and can update the agent as needed by publishing a new version to the Configuration Server DB. After you do this, all new .WIM deployments will automatically use the latest agent.

3 Click **Next**.

The End User License Agreement window opens.

4 Click **Accept**.

5 The deployment methods that may appear are:

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

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

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

7 Click **Next**.

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

9 Click **Next**.

The Span Disk Image window opens.

- 10 Type the amount of the total uncompressed disk space (in MB) to use for each image file. Type 0 (zero) if you do not want to create a spanned image.

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

- 11 Click **Next**.

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

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



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

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. However, please remember that it is important to have this agent installed if you are using the Legacy method to capture an image.

## 16 Select the appropriate options.



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

- **Build Mass Storage Section in Sysprep.inf.**

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



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



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

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

- **Optimize compression of unused disk space**

Select this check box to optimize compression of unused disk space. This adds zeroes up to the end of the system drive partition. Note that this may take some time depending on the size of the hard drive.

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

- **Resize partition before OS upload**

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

- **Perform client connect after OS install**

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

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

17 Click **Next**.

The Summary window opens.

18 Click **Start**.

19 Click **Finish**.

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

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



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

21 Click **Next**.

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

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

23 Click **Finish** to run Sysprep.

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



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

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

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



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

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



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

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

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

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

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

Next, you will want to publish your image to the Configuration Server DB. See [Publishing to the HPCA CS Database](#).

## 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 27 if you need more information about where to get this media.
- 2 Go to `\samples\prep wiz_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. Below are the values that you may need to change.

**Table 4 Variables in the configuration file to be modified**

Variable Name	Description	Sample Value
RISHOSTPORT	The OS Manager Server's IP address	<code>xxx.xxx.x.x:port</code>
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"
PREPWIZPAYLOAD (for future releases)	Payload that the administrator wants to use. The payload contains Local Service Boot (LSB)	Use the default value <code>"/OSM/PREP WIZ/payload/default/"</code>

<b>Variable Name</b>	<b>Description</b>	<b>Sample Value</b>
	data to be delivered to target devices	
OSEDITION (Required for Vista)	Specifies the edition of Vista used.	"Enterprise"

Variable Name	Description	Sample Value
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:

```
prep wiz -mode silent -cfg <fully qualified path>\<config_file>
```

Where <config\_file> is the operating system-specific configuration file.

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.

# Preparing and Capturing Thin Client OS Images

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

- [Windows XPe OS images](#) on page 92
- [Windows CE OS images](#) on page 96
- [Linux-based OS images](#) on page 98

## Windows XPe OS images



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

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

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

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

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

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

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

- 5 When prompted for the IP address and Port number, type the IP address and port number for your HPCA Configuration Server.

The Application Manager is installed.

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

The Image Preparation Wizard performs the following tasks:

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

— *ImageName.IBR*

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

— *ImageName.EDM*

This file contains the object containing inventory information.



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

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

#### To use the Image Preparation Wizard

- 1 Insert the ImageCapture media into the reference machine. Thin client devices require a USB CD-ROM drive. See [Product Media](#) on page 27 if you need more information about where to get this media.
- 2 Click **Browse** to open the *\image\_preparation\_wizard\win32\* directory.

- 3 Double-click **prepwiz.exe**. The Image Preparation Wizard verifies that `etprep.exe` and `fbreseal.exe` are available before continuing.  
The Welcome window opens.
- 4 Click **Next**.  
The End User Licensing Agreement window opens.
- 5 Click **Accept**.
- 6 Type the IP address or host name and port for the OS Manager server. This must be specified in the following format: `xxx.xxx.xxx.xxx:port`. The OS Manager server port reserved for OS imaging is 3469.  
If the Image Preparation Wizard cannot connect to the OS Manager server, a message opens and you must:
  - Click **Yes** to continue anyway.
  - Click **No** to modify the host name or IP address.
  - Click **Cancel** to exit the Image Preparation Wizard.
- 7 Click **Next**.  
The Image Name window opens.
- 8 Type a name for the image file. This is the image name that will be stored in the `/upload` directory on the OS Manager server.
- 9 Click **Next**.  
A window opens so you can enter a description for the image.
- 10 Type a description for the image file.
- 11 Click **Next**.  
The Options window opens.
- 12 Select the appropriate options.  
**Perform client connect after OS install.**  
Select this check box to connect to the OS Manager server after the OS is installed to verify the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.
- 13 Accept the defaults and click **Next**.  
The Summary window opens.
- 14 Click **Start**.

Click **Finish**.

The wizard prepares the image.

15 Click **OK**.

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



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



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



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

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

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

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

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

Next, you will want to publish your image to the Configuration Server DB. See [Publishing to the HPCA CS Database](#).

## Windows CE OS images

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

- Product media
- Image Preparation CD-ROM

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

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

The Application Manager is installed.

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

The Image Preparation Wizard performs the following tasks:

- 1 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
- 2 Restarts the reference machine into the service operating system (booted from the ImageCapture media). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.
- 3 Creates and copies the following files to *SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload* on the OS Manager Server.
  - *ImageName.IBR*  
This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Windows CE images can be deployed to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.
  - *ImageName.EDM*  
This file contains the object containing inventory information.





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

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

### To use the Image Preparation Wizard

- 1 Insert the ImageCapture media into the reference machine. Thin client devices require a USB CD-ROM drive. See [Product Media](#) on page 27 if you need more information about where to get this media.
- 2 Click **Browse** to open the `\image_preparation_wizard\WinCE\` directory.
- 3 Double-click **prep wiz.exe**.
- 4 Type the IP address or host name and port for the OS Manager server. This must be specified in the following format: `xxx.xxx.xxx.xxx:port`.

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

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

- 5 Click **OK**.

The wizard prepares the image.

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



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

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

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

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

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

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

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

Next, you will want to publish your image to the Configuration Server DB. See [Publishing to the HPCA CS Database](#).

## Linux-based OS images

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

- Product media
- Image Preparation CD-ROM

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

► For additional thin client device information see the readme file included with `ThinClient.tar`.

- 1 Login to the target thin client device.
- 2 Create a new directory called `/mnt/opt/HPCA`.

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

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

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

```
./install -E -i HPCA_Configuration_Server
```


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

The Application Manager is installed.

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

The Image Preparation Wizard performs the following tasks:

- 1 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
- 2 Restarts the reference machine into the service operating system (booted from the Image Prep CD you created). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.
- 3 Creates and copies the following files to `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload` on the OS Manager Server.
  - `ImageName.DD`  
This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Linux-based images can be deployed only to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.
  - `ImageName.EDM`  
This file contains the object containing inventory information.

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

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

### To use the Image Preparation Wizard

- 1 Insert the ImageCapture media into the reference machine. Thin client devices require a USB CD-ROM drive. See [Product Media](#) on page 27 if you need more information about where to get this media.



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

- 2 On the Image Preparation CD, go to `/image_preparation_wizard/linux` and run `./prep wiz`.

The Welcome window opens.

- 3 Click **Next**.

The End User Licensing Agreement window opens.

- 4 Click **Accept**.

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

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

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

- 6 Click **Next**.

The Image Name window opens.

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

8 Click **Next**.

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

9 Type a description for the image file.

10 Click **Next**.

The Options window opens.

11 Select the appropriate options.

**Perform client connect after OS install.**

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

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

The Summary window opens.

13 Click **Start**.

14 Click **Finish**.

The wizard prepares the image.

15 Click **OK**.

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



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



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



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

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

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

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

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

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

Next, you will want to publish your image to the Configuration Server DB. See [Publishing to the HPCA CS Database](#).

---

# 6 Publishing to the HPCA CS Database

This chapter includes the following topics:

- Prerequisites for publishing .WIM images of a Windows Vista OS or Windows Server 2008
- Using the Admin Publisher
- Adding Drivers

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



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

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

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

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

- Copy the `\agent` folder from the agent media to the device where you are publishing the image. (If this folder can be referenced during the promote, via a DVD or network drive, it does not need to be copied locally).

This folder is only required the first time you publish a .WIM file or if you want to publish an updated agent package. The agent will be published as a separate package which ensures that all future deployments of your .WIM files will automatically receive the latest agent available.


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



Server's `\upload` directory to the device where you are publishing the image. 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.

- Copy `substitutes` and `unattend.xml` to the same directory as `filename.wim`. Samples of these files are available on the Image Capture media in `\samples`. If you choose to use the samples, modify information as needed such as the setting the time zone and entering the product key. See the instructions below for more information.


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

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

## About the `.subs` and `.xml` files

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

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

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

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

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

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

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

## Example of Substitution

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

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

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

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
        <component name="Microsoft-Windows-UnattendedJoin"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMICConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <Identification>
                <JoinDomain>anything</JoinDomain>
            </Identification>
        </component>
    </settings>
    <cpu:offlineImage
        cpu:source="wim://hpfcovcm/c$/vista_inst/vista.wim#W
        indows Vista ULTIMATE" xmlns:cpu="urn:schemas-
        microsoft-com:cpu"/>
</unattend>
```

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

```
//un:settings[@pass='specialize']//un:component[@name=Microsoft-Windows-UnattendedJoin']  
[@processorArchitecture='x86']/un:Identification/un:JoinDomain  
,VistaTeam
```

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


## Preparing filename.xml


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

# Using the Admin Publisher

To use the Admin Publisher

- 1 Go to **Start→All Programs→HP Client Automation Administrator→Publisher→Client Automation Admin Publisher**.  
The Logon screen opens.
- 2 In the User ID text box, type your HPCA Administrator user ID (by default **rad\_mast**).
- 3 In the Publishing Options windows select **OS Image** from the drop-down list.
- 4 Click **OK**.
- 5 Use the Select window to find and select the file you want to publish (typically stored in the `\upload` directory on the OS Manager Server). Only supported file types appear in the window.


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


 If you are publishing the agent to be used with a `.WIM` file, you must have 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. Then, be sure to select the appropriate `.msi` file.

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

If you chose to publish a `.WIM` file, the WIM Deployment Configuration window opens.

- a From the Deployment method drop-down list box, select the appropriate method, Microsoft ImageX or Windows Setup.

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

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

- b If you chose Microsoft Setup, from the Sources directory text box, browse to the sources directory from the Windows Vista installation media.
- c In the Client media location, browse to the correct path for the agent media. It may take a few moments for the path to appear.

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

- 8 Click **Next**.
- 9 Use the Package Information section to enter the package information. Note that the Limit package to systems with section is not available when publishing OS images.
- 10 Click **Next**.
- 11 On the Configure window, select **Create new**.



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

- 12 Enter the appropriate information in the rest of the fields.
- 13 In the Assignment type group box, select whether the service is mandatory or optional. By default, Mandatory is selected, which will distribute this service to all available subscribers.

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

- 14 Click **Next**.
- 15 Review the Summary section to verify the package and service information you provided during the previous steps. When you are satisfied, click **Publish**.
- 16 Click **Finish** to exit the Admin Publisher.

The service is now ready for distribution to your enterprise.



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

## Adding Drivers

You can add drivers to previously prepared images by creating delta packages that are deployed after the image is laid down on a new local

partition. This is limited to the Microsoft Windows Setup deployment method based on Microsoft's documentation. Additional options may exist but would require further scripting.

## Prerequisites

- Publish your OS Service. The Publisher automatically creates a connection, `OS.ADDON.ServiceName_*`, under this service.
- If you are creating an OS Driver file:
  - Create a directory, such as `C:\MyDrivers`. Below that, create a directory called `\osmgr.hlp` with a subfolder called `drivers`.
  - Store individual drivers in `...\drivers` or create additional subdirectories under `...\drivers`.
- If you are creating a Service OS Driver file:
  - Create a directory, such as `C:\MyServiceDrivers`. Below that, create a directory called `\work`.
  - Store individual drivers in `...\work` or create additional subdirectories under `...\work`.

### To publish delta packages

- 1 Go to **Start→All Programs→HP Client Automation Administrator→Publisher→Client Automation Admin Publisher**.  
The Logon screen opens.
- 2 In the User ID text box, type your HPCA Administrator user ID (by default `rad_mast`).
- 3 In the Publishing Options windows select **OS Add-ons/extra POS drivers** from the drop-down list.
- 4 Click **OK**.
- 5 Use the Select Drivers window to select the root directory you want to publish from. Everything below this root directory will be recursively scanned, included and published.
- 6 From the Add-on Type drop down list, select **OS Driver** file or **Service OS Driver**.
- 7 From the Select Target Service drop down list, select the OS service to which you want to add these drivers.

- 8 In the optional Suffix text box, you can type a number that can be used to track packages. For example, if the 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.
- 9 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. If you modify this name, there will be no connection between the OS service and the ADDON instance unless you create the connection yourself.
- 10 Click **Next**.
- 11 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.






---

# 7 Preparing Content

This chapter includes the following topics:


- [About Discovery](#)
- [About Policy](#)
- [Preparing Content Using the CSDB Editor](#)

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 not been disabled. If you use these features, they will simply be ignored on a thin client device.

## About Discovery

When a target device boots, it communicates with the OS Manager Server to determine whether a ROM object exists. This process is called **discovery**. If a ROM object does not exist, one will be created the first time the target device communicates with the OS Manager Server. After a ROM object is established in the Portal, the OS Manager Server and the target device can communicate. Use the 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**

<b>If the target device...</b>	<b>then...</b>
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 not prompt the user for workstation or server. If no policy is assigned, no OS can be installed. The user will be informed of this and instructed to press <b>Enter</b> . The device shuts down.

<b>If the target device...</b>	<b>then...</b>
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 <i>unmanaged</i> 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 (e.g., whether the resolved OS is installed or not, whether a user is prompted or not).
has no recognizable partitioning and the Encryption Support Mode parameter <code>ENCMODE</code> is set to its default value of <code>AUTO</code> 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 <code>ENCMODE</code> is set to <code>NONE</code> .	If the disaster recovery behavior setting <code>PMDISRCV=_CONFIRM_</code> then the target device shuts down so the administrator can recover data from the target device. If the disaster recovery behavior setting <code>PMDISRCV=_AUTO_</code> then the appropriate OS is reinstalled.
Has no recognizable partitioning and the Encryption Support Mode parameter <code>ENCMODE</code> is set to <code>ENC</code> .	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 [Determining Policy Assignments](#) on page 117 for important information about implementing policy,

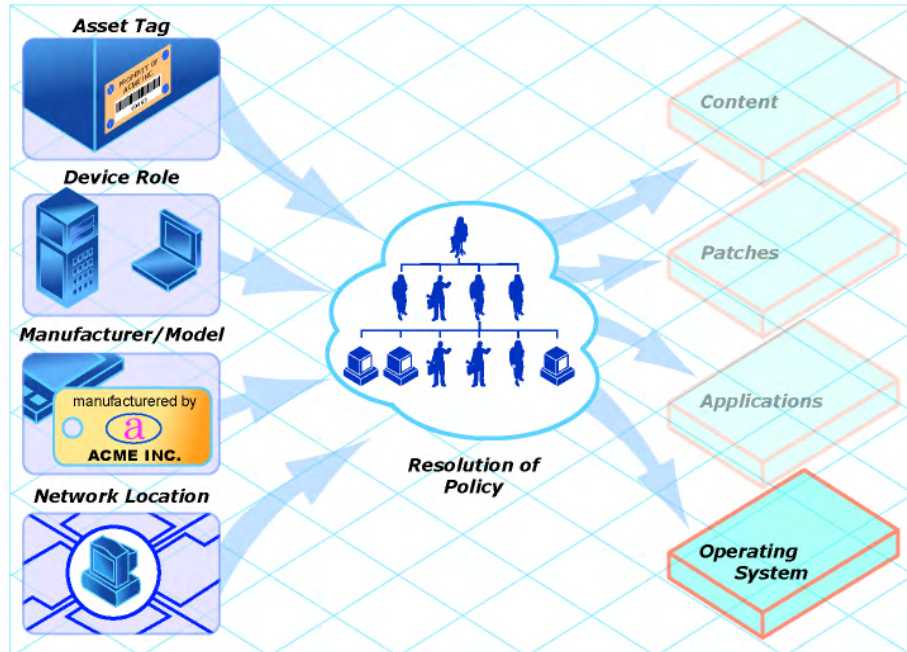
Manufacturer, model, and subnet are based on attributes related to a device. Role is *not* based on a device's attributes. It is simply a grouping of devices, similar to how you might assign policy based on departments. You can set policy based on a device's assigned role—such as server or workstation.

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

## Determining Policy Assignments

We recommend that you select a single criterion for policy.

**Figure 3 Resolution of Policy**



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

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



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

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

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.

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

**Figure 4 Class relationships**



## Preparing Content Using the CSDB Editor

Typically, you will use the Enterprise Manager to simply assign an operating system to a set of target devices and initiate the deployment. However, in some cases 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 scenarios below, you must be logged into the CSDB Editor as an administrator.

**Table 6 Administrative Procedures**

<b>If you want to...</b>	<b>Then...</b>
<p>Install an OS on a bare metal machine</p> <p>Note: This does not apply to Local Service Boot implementations.</p>	<ol style="list-style-type: none"> <li>1 Create any necessary policy instances, such as subnet or role. If you are creating a manufacturer or model policy instance, see <a href="#">Creating a Manufacturer or Model Instance</a> on page 128.</li> <li>2 Connect the OS service to the policy instances. See <a href="#">Assigning Operating Systems</a> on page 128.</li> <li>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 <a href="#">Setting Behaviors</a> on page 123.</li> <li>4 Boot the target device. When the device boots up, the appropriate OS (according to policy) is installed and a ROM object is created.</li> </ol>
<p>Bring an unmanaged machine with an installed OS under Client Automation management and install the appropriate OS as per policy.</p> <p>Reminder: The target device must have the Application Manager with the HPCA OS Manager feature installed.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>2 Use the OS Management Wizard in the Enterprise Manager.</li> </ol>
<p>Force a re-installation of the current OS without retaining any existing data.</p>	<ol style="list-style-type: none"> <li>1 Use the OS Management Wizard in the Enterprise Manager.</li> </ol>



<b>If you want to...</b>	<b>Then...</b>
Force the installation of a valid OS that you choose without retaining any existing data.	<ol style="list-style-type: none"> <li>1 Assign policy so that the new OS that you want to install is the <i>only</i> OS connected to policy.</li> <li>2 OS Management Wizard in the Enterprise Manager.</li> </ol>
Initiate the installation of a different OS.	<ol style="list-style-type: none"> <li>1 Set the Select OS (PMACKOVW) behavior to <code>_NEVER_</code> to give the administrator control over policy. See <a href="#">Setting Behaviors</a> on page 123.</li> <li>2 Assign policy so that the new OS that you want to install is the <i>only</i> OS connected to policy.</li> <li>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.</li> </ol> <p>Note that if you do not set the Behavior to <code>NEVER</code> the user will be prompted to confirm whether they want to reinstall the OS.</p>
Allow the user to decide which OS to install.	<ol style="list-style-type: none"> <li>1 Verify that your policy will result in more than one OS available for the target devices.</li> <li>2 Set the PMSLCTOS behavior to <code>_LOCAL_</code>. See <a href="#">Setting Behaviors</a> on page 123.</li> <li>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.</li> </ol>
The following are additional options that can be used in many scenarios	
Use an override Sysprep file.	<ul style="list-style-type: none"> <li>• Connect a Sysprep instance to the operating system instance. See <a href="#">Using an Override Sysprep File</a> on page 134. 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.</li> </ul>
Add partitions.	<ol style="list-style-type: none"> <li>1 Use the Drive Layouts Class to specify the type of partition. See <a href="#">Defining Drive Layouts</a> on page 129.</li> <li>2 Add a partition. See <a href="#">Adding Partitions</a> on page 132. <i>All existing data will be lost.</i></li> <li>3 Assign the appropriate drive layouts to your target devices. See <a href="#">Assigning Drive Layouts</a> on page 132.</li> </ol>

If you want to...	Then...
Create a replace, cache, or merge type partition.	<ol style="list-style-type: none"> <li>1 Use the Drive Layouts class to specify the type of partition. See <a href="#">Defining Drive Layouts</a> on page 129.</li> <li>2 Assign the appropriate drive layouts to your target devices. See <a href="#">Assigning Drive Layouts</a> on page 134.</li> </ol>

## Logging On

To log on to the Client Automation Administrator CSDB Editor

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



Take care when modifying these classes as 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.

To access 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](#) below.
- 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 129.
- 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*.
- Operating Systems (ZSERVICE)  
Stores the OS services to be deployed to your target devices.
- Partition Table Spec (PARTTION)  
Lists the specifications for the partitions that you may add in addition to the OS boot partition. See [Adding Partitions](#) on page 132.
- Sysprep Files (SYSPREP)  
Lists the Sysprep files and unattend.txt files stored in your database. See [Using an Override Sysprep File](#) on page 134.

## 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	Indicate whether the user is allowed to select a machine role. <ul style="list-style-type: none"><li>• <b>_LOCAL_</b> 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.</li><li>• <b>_CENTRAL_</b> disables the ability to select roles. A role selection remains in effect until you (the administrator) void or</li></ul>

	<p>override the selection.</p> <p>Default: <code>_CENTRAL_</code> (applies to Core and Satellite environments only)</p>
PMACKOVW	<p>Specifies whether to prompt the user before overwriting or modifying the OS.</p> <ul style="list-style-type: none"> <li>• <code>_ALWAYS_</code> (Default) Prompts the user before a reinstallation.</li> <li>• <code>_NEVER_</code> Does not prompt the user, but installs the OS. <ul style="list-style-type: none"> <li>— Caution: <code>NEVER</code> is designed for use with unattended devices. Use this option with caution, as the user will not be prompted before the OS is overwritten.</li> </ul> </li> <li>• <code>_VALID_</code> This option has been deprecated.</li> </ul>
PMINITL	<p>Specifies whether an OS should be installed over an existing file system on a recently discovered, but unmanaged device.</p> <p>The <code>PMINITL</code> attribute is referenced only if there is no <code>rombl.cfg</code> on the device. If there is a <code>rombl.cfg</code>, this indicates that the device is already under management and <code>PMINITL</code> will not be referenced at all.</p> <ul style="list-style-type: none"> <li>• <code>_LOCAL_</code> (default) Prompts the user.</li> <li>• <code>_KEEP_</code> Does not prompt the user and keeps the current OS.</li> <li>• <code>_REINSTALL_</code> Does not prompt the user and reinstalls the operating system, regardless of what exists.</li> </ul>
PMDISRCV	Specifies the action to be taken when there

	<p>is no valid bootable partition.</p> <ul style="list-style-type: none"> <li>• If <code>PMDISRCV = _CONFIRM_</code>, the target device shuts down so that the administrator can recover data from the target device.</li> <li>• If <code>PMDISRCV = _AUTO_</code>, the appropriate OS is reinstalled.</li> </ul>
<p>RUNPARAM</p>	<p>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 <i>HP Client Automation Enterprise Application Manager and Application Self-service Manager Installation and Configuration Guide</i> and the HP support web site.</p> <p>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.</p> <p>Do not remove the <code>cop=y</code> parameter; it is necessary because COP must be enabled to use the OS Manager.</p> <p>In the RUNPARAM (RunOnce Parameter String) change <code>IP=RCSSERVER</code></p> <p>to reference the appropriate Configuration Server for your environment. If your Configuration Server is running on a non-default port, also add <code>“,port=&lt;Configuration Server port number&gt;”</code>. The default port for Configuration Server is 3464.</p>
<p>ROMAPARAM</p>	<p>Typically, use this only if instructed by Technical Support.</p> <p>Also used in conjunction with the <code>TESTMODE</code> flag.</p>

BANDWIDTH	<p>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).</p> <p>The default definition is in bytes/sec.</p> <p>The default value is blank (no bandwidth limitation) which means that the download process will run at the maximum speed of the network interface.</p>
KBDMAP	<p>Sets the keyboard mappings:</p> <ul style="list-style-type: none"> <li>• <b>en</b> (default) loads English keyboard mappings</li> <li>• <b>fr</b> loads French keyboard mappings</li> <li>• <b>de</b> loads German keyboard mappings</li> </ul>
LANG	<p>Specifies the language to be supported.</p> <ul style="list-style-type: none"> <li>• en_US = English</li> <li>• zh_CN = Simplified Chinese</li> <li>• ja_JP = Japanese</li> <li>• ko_KR = Korean</li> </ul>
ACKTMOUT	<p>Specifies how long ACKTMOUT waits before assigning the default AUTOROLE.</p> <ul style="list-style-type: none"> <li>• Set ACKTMOUT = 0 to disable the timeout.</li> <li>• Set ACKTMOUT = <i>number of seconds</i> to wait the specified length of time before continuing.</li> </ul>
AUTOROLE	<p>The ROLE that is assigned if a timeout occurs.</p>

- 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_nvdmmodel`.

For example, if you have an HP Compaq dc7700 Small Form Factor machine, manufacturer (`nvdmanufact`) will be displayed as HEWLETT\_PA and the model (`nvdmmodel`) 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.

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



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

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

To specify a drive layout

- 1 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 you want to create.

**Table 8**      **Types of Partitions**

Type	Description
Add	Creates one or more extended partitions at the end of the hard disk. See <a href="#">Adding Partitions</a> on page 132 for more information.

Type	Description
Replace (default)	<p>Replaces the current mappings on the target device with the partition that is defined with the OS image being installed. If there are no DRIVEMAP instances connected to the OS being installed, this is the default method.</p> <p>Important: If you use Replace, <i>all existing data will be lost.</i></p>
Cache	<p>Creates a hidden back-up partition at the end of the target drive. The size of the partition will be dynamically determined by the size of the OS installation image. All files necessary to reinstall the OS will be saved (in compressed form) in this partition. Note that during the reinstallation, the name and size of the image are confirmed.</p> <p>Important: If you use the Cache type, <i>all existing data will be lost.</i></p> <p>See <a href="#">Restoring Operating Systems</a> on page 176 for information about restoring this image.</p>
Merge (default in Core and Satellite environments)	<p>Use for migration purposes. Replaces or updates an OS on a machine where existing data needs to be preserved. Merge will overlay only the existing boot partition and will not touch data on any other partitions.</p> <ul style="list-style-type: none"> <li>• If the boot partition to be installed is larger than the space already defined for the partition, the installation will fail. The starting point of the existing partition will be used and the boot partition will be placed at the beginning of the drive segment defined in the partition.</li> <li>• If the target drive does not contain existing partitions, the boot partition definition will be used to partition the target drive.</li> </ul>

Type	Description
Pres	<p>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.</p> <p><b>Note:</b> This requires the ImageX method of OS deployment. An attempt to use any other deployment method will result in an error.</p> <p>To do this:</p> <ul style="list-style-type: none"> <li>• 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/folders being placed in the named folder is acceptable.</li> <li>• During the resolution/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 <i>except</i> for the contents of C:\OSMGR.PRESERVE are removed.</li> <li>• The new OS image is deployed to the (preserved) file system.</li> <li>• 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/folders being restored properly is acceptable. Note that all data in C:\OSMGR.PRESERVE remains until explicitly removed by the (user-defined) restore process.</li> </ul> <p><b>NOTE:</b> You cannot use this Partition Type if your target device has been BitLocker prepared. If you try to do so, you will receive an error.</p>

- 4 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

and then add a second hard drive, the drive letter mappings are reassigned so that the primary partitions are in alphabetical sequence. See the example below.

### Drive 1

PARTITION	LOGICAL DRIVE
Primary	C
Extended	E
	F
	G

## Drive 2

Primary	D
Extended	H
	I
	J



The partition will be added after the boot partition. Make sure you allow enough space for the OS. Note that if the total requested space would exceed the capacity of the drive where the OS is being installed, the installation will fail.

### To add partitions

- 1 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 9 PARTITION Class Attributes**

Attribute in the Database	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\_DRVIEMAP from the ROLE base instance. Only one connection is allowed.



Remember that you can add partitions *or* merge, replace, or cache partitions. You cannot do both.

## 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`.

Below 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 10 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	[Unattended] OemSkipEula = Yes ExtendOemPartition = 1	[Unattended] oemskippeula=Yes extendoempartition=1
[Identification] JoinWorkgroup = "WORKGROUP"	[Identification] JoinWorkgroup = JoinDomain = "TESTDOM1"	[Identification] joindomain="TESTDOM1"
[guirunonce] C:\TEMP\KEEPRUNNINGTHIS.CMD C:\TEMP\RUNADIFFERENTONE.CMD C:\TEMP\STOPRUNNINGTHIS.CMD	[guirunonce] + C:\TEMP\RUNTHISONEINSTEAD.CMD - C:\TEMP\ANDRUNTHISONE.CMD	[guirunonce] C:\TEMP\KEEPRUNNINGTHIS.CMD C:\TEMP\RUNTHISONEINSTEAD.CMD C:\TEMP\ANDRUNTHISONE.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 [Using the Admin Publisher](#) on page 107.

- 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:

- About the PXE-Based Environment
- About Local Service Boot
- Managing Your Devices

After you have successfully installed your OS Manager infrastructure, consider how you want to implement the OS Manager in your environment. We recommend that you work with Professional Services to determine what is best for your unique situation. This chapter is intended to help you understand your options. They are:

- Installations initiated by the network  
This refers to the PXE-based environment. The OS Manager can assume management of the operating system on target devices that are booted from the network.
- Installations initiated locally  
This refers to the Local Service Boot (LSB). The OS Manager can assume management of the OS on target devices that are not booted from the network.



We strongly recommend that you choose one method for a particular target device. If you have a bare metal machine or a machine that needs disaster recovery, you *must* use PXE.

## About the PXE-Based Environment

The PXE-based environment allows the OS Manager to assume management of the OS on target devices that are booted from the network. Typically, we recommend that you use the PXE-based environment because it provides a fully automated solution for all scenarios.

### Best Practices for PXE-Based Implementations

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

- 1 Install the OS Manager Server infrastructure before making any changes to your target devices. See Chapter , [Installing and Configuring the Server](#).
- 2 Agents that exist on your target devices will continue running any previously scheduled agent connects. The OS Manager will not make any changes to the device until you assign policy.

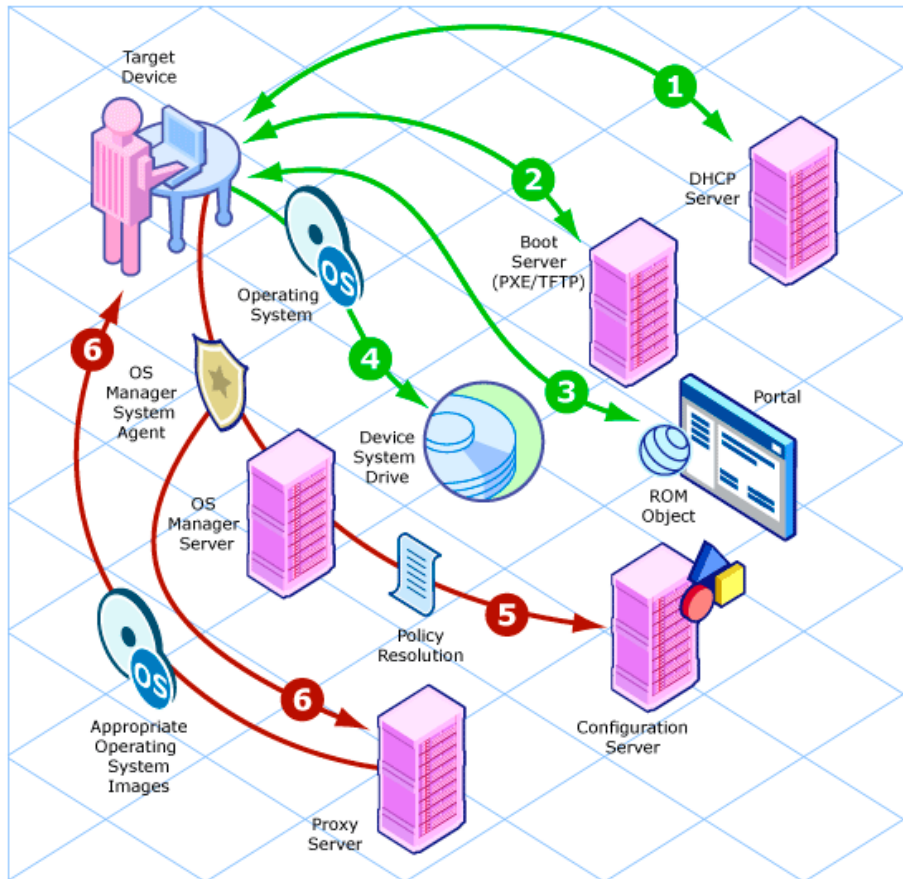
- 3 After your infrastructure is installed and stable, set the network boot as the primary boot device on your target devices.
- 4 The next time the device boots, a ROM object will be created in the Portal. The OS Manager Server and the target device use the ROM object to communicate.

At this point, the OS Manager has discovered the target device, but its OS is likely considered unmanaged unless you assigned policy prior to booting the target device. The target device will continue to boot into its existing OS until you assign policy and perform an agent connect.

## Networking Boot with PXE

[Figure 5](#) on page 140 and the text following it give an overview of the boot process.

**Figure 5 Networking boot with PXE process flow**



- 1 The target device obtains an IP address from a DHCP server.
- 2 The (managed) target device boots from the network (via the PXE server), and the TFTP server delivers the OS Manager Boot Loader to the target device.
- 3 The OS Manager Boot Loader looks at the Portal to see if a ROM object exists.
  - If there is no ROM object, an object is created in the Portal.
  - If there is a ROM object, it must be decided whether there is a valid OS or not.

- 4 If there is a valid OS on the machine, it boots to the existing OS located on the device's system drive.

or

If there is not a valid OS on the device, the boot process continues by loading the OS Manager System Agent from the TFTP server to the target device.

- 5 The OS Manager System Agent and the Configuration Server communicate through the OS Manager Server to handle policy resolution of the correct OSs for the target device.
- 6 The OS Manager System Agent downloads the appropriate images from the Proxy Server and installs them on the target device.



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

## About Local Service Boot

The Local Service Boot allows the OS Manager to assume management of existing OSs on devices that are not booted from the network.

The advantages of Local Service Boot are that existing machines do not need to be PXE-enabled and the boot order does not need to be configured locally in the BIOS for each target device. This option is also less network-intensive because the OS Manager System Agent is only downloaded when the LSB service is downloaded to the target device. Since this intermediate OS is local, it does not need to be downloaded again unless there is an update. In a PXE environment, the OS Manager System Agent is downloaded every time it is needed.



If you have a bare metal machine or a machine that needs disaster recovery, you *must* use PXE.

## Prerequisites

- You must have an operating system and the Application Manager installed on the target device so that you can deploy the LSB service.

- You must be using HPCA Client Operations Profiles as configured for the OS Manager Server and it must be enabled. See [Using COP with OS Manager](#) on page 181.



The Image Preparation Wizard sets up Client Operations Profiles, and when the image is deployed, Client Operations Profiles is enabled. However, if you want to use the Local Service Boot on a machine where the OS has not been deployed by the OS Manager Server, you must enable Client Operations Profiles. To do this, use COP=Y on the radskman command line. Refer to *Configuring Client Operations Profiles* in the *HP Client Automation Enterprise Application Self-service Manager Installation and Configuration Guide*.

## Best Practices for Using Local Service Boot

If you already have HP Client Automation implemented in your environment and want to use the Local Service Boot for the OS Manager, we recommend that you:

- 1 Install the OS Manager Server infrastructure. See Chapter , [Installing and Configuring the Server](#).
- 2 Use Client Operations Profiles to specify the IP address and port of the OS Manager Server in the form of a Service Access Profile (SAP) instance.

When you set up the SAP, be sure to:

- Set TYPE to ROM to identify this SAP as an OS Manager Server server.
- Set ROLE to Z.
- Set URI to specify the fully qualified IP address (or hostname) and port of the OS Manager Server that serves the agents on the subnet. For example:

<http://OSManagerServer.domain.com:3469>.



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

You must create a LOCATION instance using the subnet with underscores as the name (10\_10\_10\_0) and connect it to the SAP instance.

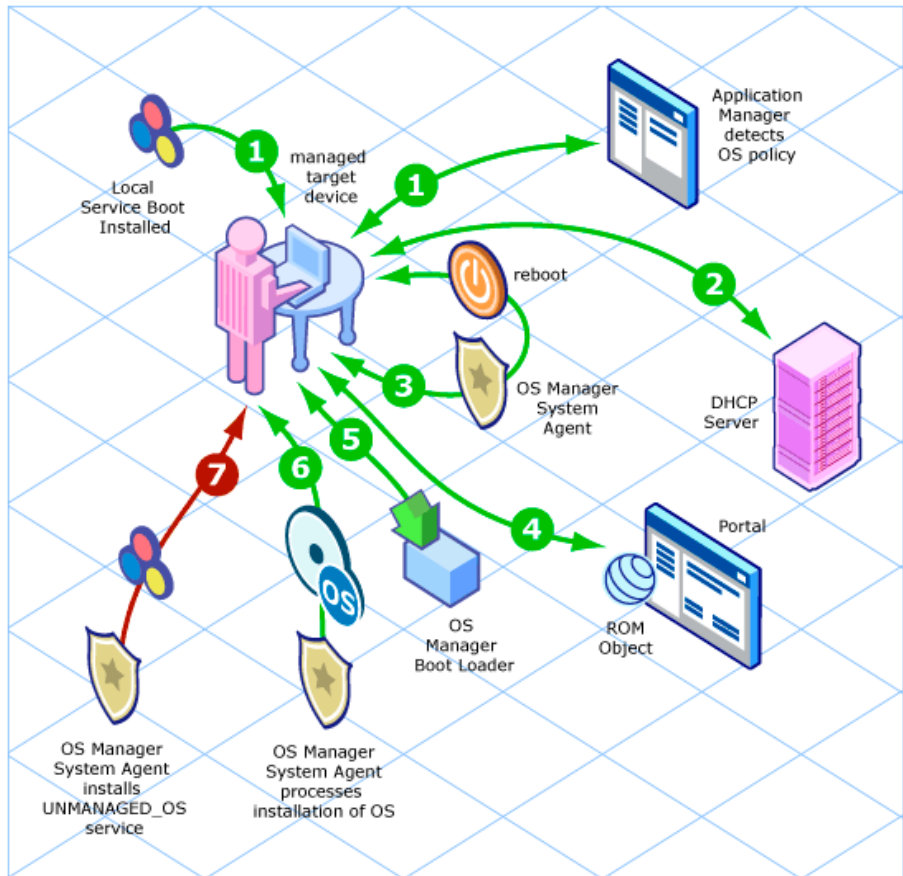
- 3 Set up policy to use the Application Manager to install the Local Service Boot service (LSB) on your target devices. Local Service Boot (LSB) must be distributed based on subnet, model or manufacturer.

After the LSB service is installed on the target devices (which creates the `Romb1.cfg` file on the root of the drive), they will reboot and be discovered. At this point, the OS Manager has discovered the target device, but its OS is still unmanaged. The target device will continue to boot into its existing OS until you assign policy and bring the machine under management.

## Booting with Local Service Boot

[Figure 6](#) on page 144, and the text following it give an overview of the boot process.

**Figure 6 Booting with Local Service Boot**



- 1 After the Local Service Boot service is installed on a target device, the Application Manager is responsible for detecting OS policy changes on the managed target device.
- 2 The target device obtains an IP address from a DHCP server.
- 3 When the device restarts, the device boots into the intermediate 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 support web site for product updates and release notes.

## Managing Your Devices

Whether your devices are in a PXE-based environment or Local Service boot environment, after your existing devices are discovered and set to be unmanaged, nothing will happen until you take action.

If you want to change the OS, you must:

- 1 Specify policy.
- 2 Select the appropriate devices and 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 Professional Services to determine what is best for your environment.



---

# 9 Multicast and the OS Manager

This chapter includes the following topics:

- Prerequisites
- Requirements
- Configuring Multicast for OS Manager
- Improving Performance and Reliability for Multicast with OS Manager
- Analyzing Problems
- Test Modules

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.

## 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 11 Description of ROMA Parameters**

Parameter	Description
multicastIPAddress	This parameter specifies the Multicast Server host. You can also use the host name. 3463 is the default Multicast Server port.
mcastretrycount	This parameter specifies the number of times that the client will retry multicast if there is a failure. The default value is 1.
mcastretrywait	This parameter specifies how long to wait before the client will start the retry. The default value is 240 seconds.

- 5 **Modify** `SystemDrive:\Program Files\Hewlett-Packard\CM\MulticastServer\etc\mcast.cfg` as needed.
  - `root`  
Specifies the root directory from which the Multicast Server will retrieve resources.
  - `address`  
Specifies a range of multicast IP addresses available for use with dynamic windows. Refer to the *HP Client Automation Multicast Server Installation and Configuration Guide* for more information about dynamic windows.
  - `Minref`  
Specifies the minimum number of clients that are required to contact the multicast server to start a multicast session. By default, `minref=2`. You may want to change this to take advantage of multicast's functionality. 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

`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 12 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



<b>Parameter</b>	<b>Used by</b>	<b>Definition</b>	<b>Default Value</b>
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 <code>numpktblks</code> parameter described below.	4098
nacdelay	Receiver	The delay, in milliseconds, between resends of a specific NACK.	0.5
nacresend	Receiver	The number of times to resend each NACK.	2
netinact0	Receiver	Network inactivity time-out. The number of minutes of network inactivity allowed between received packets before the receiver fails.	5
numpktblks	Sender or Receiver	Defines the size of the pool from which resend requests are fulfilled.	64

Parameter	Used by	Definition	Default Value
pktsperblk	Sender or Receiver	<p>Specifies the number of packets within a resend block.</p> <p>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.</p> <p>This value must be a multiple of 32. If you do not follow this requirement, your value will be adjusted and noted in the <code>gdmcsend.log</code> and the OS Manager System Agent logs.</p>	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	<p>Throttle frequency.</p> <p>Specifies how often to check to see if the inter-packet delay should be adjusted.</p>	8
throthighth	Sender	<p>Throttle high threshold.</p> <p>The number of average resends per block that will trigger an increment of the inter-packet delay.</p>	-1 (disabled) Note: To enable this, set it to a positive integer.
throtincr	Sender	<p>Throttle increment.</p> <p>The value, in milliseconds, that is automatically added to (or subtracted from) the current inter-packet delay each time the throttle is adjusted.</p> <p>See <a href="#">Auto Throttle</a> on page 158 for more information.</p>	0.01
throtlowth	Sender	<p>Throttle low threshold.</p> <p>The number of average resends per block that will trigger a decrement of the inter-packet delay.</p>	-1 (disabled) Note: To enable this, set it to a positive integer.

Parameter	Used by	Definition	Default Value
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 retransmitted.
- `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 how to identify, analyze and resolve multicast data transfer problems.

### About the Logs

The sender's log — `gdmcsend.log` — is typically stored in `SystemDrive:\Program Files\Hewlett-Packard\CM\MulticastServer\logs`.

The receiver log is typically appended to the end of the OS Manager System Agent log for the device.

### Poor Performance

As mentioned before, poor multicast transfer performance is usually due to poor network and/or agent conditions. Such conditions result in the generation of an excessive number of resend requests (NACKs) from one or more of the clients, slowing down the entire transfer.

Before you can resolve the performance issue, you must first determine the root cause of the problem. To do so, examine the contents of the multicast sender's log file, `gdmcsend.log`. Review the following steps to guide you in determining the cause of the problem.

- 1 Determine the average number of resends per block for the transfer in question. Look for the line in the log file in the form:

Avg resends per block = 0.00283688

Averages less than one are very good. This indicates that most of the packet blocks were sent only one time, with relatively few resends. Large values may indicate a problem. What to consider large depends on the value of the inter-packet delay, `gddelaybp`. Remember, there is a trade-off between raw data transfer rates and packet loss, so you can expect more NACKs when the inter-packet delay is small.

- 2 If the average resends per block indicates that there is a problem, examine the per-client statistics for the transfer. In the same log file, look for lines in the form:

```
Client stats:
Client: 16.119.237.171 (0xabed7710) NACKs = 19714
Client: 16.119.237.207 (0xabed7710) NACKs = 102
Client: 16.119.237.122 (0xabed7710) NACKs = 17
Client: 16.119.237.217 (0xabed7710) NACKs = 8
```

Each client is identified by its IP address. The client that has been issued the most resend requests (NACKs) appears at the top of the list.

If there are one or more agents that top the list whose NACK count far exceed those of the other agents, it is a strong indication that the problem is specific to the agents in question. After the problematic agents have been identified, you can try to determine what sets them apart from the others. Some considerations:

- a Are the problematic clients on a different subnet than the others? If so, the problem may be specific to that subnet. Check the routers in the path from the server to the clients to see if any have seen a large number of errors on any of their ports. If so, it can be a router, port, or cabling problem.
- b Are the agents in question slower than the others? Slow clients may be unable to keep up with high raw data transfer rates, causing them to miss more packets and in turn, NACK more often. If this is the case, you have a few options:
  - Increase the inter-packet delay (`gddelaybp`) in order to lower the raw data transfer rate, so the slower agents will be better able to keep up. Even with the lower transfer rate, if the number of NACKs from these agents is significantly reduced, the actual throughput may increase.
  - Whenever possible, do not include these clients in multicast sessions with faster agents. Put them in their own multicast session, or use unicast to deploy images to them.



- c If the clients are of comparable speed, the local network connections or cabling may be at fault. Check the cables and connections closest to the agents to see if they are causing the problem.
- 3 If all of the clients show a large number of NACKs, the problem is probably more systemic.
    - a The network may have been especially congested during the time of the transfer. Performing the transfer when the network is less busy may yield better results.
    - d Check the relevant network routers, connections and cabling as described above. This time, make sure to check the cables and connections from the server to the network.
    - e It could be that all of the machines are just too slow to keep up with the current raw data transfer rate. Increase the inter-packet delay to see if fixes the problem.

In some cases, enabling the auto-throttle feature is a better alternative than manually increasing the inter-packet delay. After the proper threshold values are set, the auto-throttle will adjust the inter-packet delay as needed.

## Client Time-out

Agents can time out for one of two reasons:

- 1 **Total image transfer time-out** occurs when the total time it takes to transfer the image exceeds the value of the `recvtimeout` parameter.
- 2 **Network inactivity time-out** occurs when the time between received packets exceeds the value of the `netinactio` 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 159, can be used to identify and resolve the problem.

## Network Inactivity Time-out

A log file message in the form:

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

is indicative of a network inactivity time-out.

This type of failure can be caused by almost anything that disrupts the flow of data from the server to the client. Premature termination of the multicast sender and various network problems can occasionally be at fault.

In some cases, it can result from the loss of one or more strategic packets. For example, the client in question may not have seen the last packet of the image. If this is the case, it will not know it needs to NACK the missing data. Having sent the last block and not seeing any NACKs, the server will not send more data. Expecting more data, the client will wait for the next packet until `netinact0` has been exceeded.

We can determine if the client missed the last packet of the image by examining the log files. In the sender's log file, `gdmcsend.log`, look for two lines in the form:

```
Last block: 3524
Packets in last block: 54
```

If they exist, then you know the sender sent the last packet.

Now, in the client's log file, look for a line like:

```
Last buffer size = nnn
```

If this line is not there, then you know the client did not see the last packet.

To remedy this problem, increase the value of the `lprcount` parameter. This will cause the last packet of the image to be retransmitted more times, increasing the probability that the client will see at least one of the redundant packets.

## Buffer Overflow

The primary causes of buffer overflow are slow clients and missing data.

## Slow Client

If the client is too slow, it may not be able to write out data fast enough, causing its buffer capacity to be exceeded. To determine if this is the case, look to the client's log file.

First, look for a line in the form:

```
Current block: 3289, High block: 3353
```

In this example, the value of the `numpktblks` parameter is 64. The fact that the difference between the current block (3289) and the high block (3353) is 64 indicates that all the buffers are in use.

Following this line are entries for every block that is not full. If there are no such entries or just a few near the high block range, it shows that most of the buffers are full, but the agent has not had the chance to write them out yet. For example, if the following line is:

```
Block: 3353, 32 packets of 256
```

It shows that all but the high block are full. This indicates that the agent may be too slow for the current raw data transfer rate. Here, you may want to consider increasing the inter-packet delay to see if the agent can better keep up with the lower raw data transfer rate.

## Missing Data

On the client, if a block is missing data, it cannot be written out. After that block becomes current, writing will stop and will not resume until the missing data is filled in. In the meantime, the remaining buffers are used to hold the incoming data. If the missing data is not filled in soon enough, the buffers may overflow. Normally, the client will NACK the missing data and the holes will be filled in long before this happens.

In the client's log file, the indicators of this condition are similar to those of the slow client case. The line:

```
Current block: 3289, High block: 3353
```

should look essentially the same, showing all of the buffers in use.

In this case however, the following line will show that the current buffer is not full:

```
Block: 3289, 32 packets of 256
```

Now the question becomes, why is this data missing? The agent should have sent a NACK requesting that this block be resent and the data should have been resent by the server.

There are two possibilities: the NACK was never sent or the server never received it.

First, let us see if the block was indeed NACK'ed. In the client's log file, look for the statistics associated with the block in question:

```
Block: 3289, 32 packets of 256  
Resends requested: 1
```

Here you see one NACK was sent for the block.

Now, see if all of the NACKs the client sent got through to the server. In the client log file, there should be a line in the form:

```
Total resend requests = 8
```

Here, you see that the agent sent eight NACKs to the server. In the server log file, look at the per-agent data. After the line:

```
Client stats:
```

is a list of agents and the number of NACKs the server has received from each. Using the agent's IP address, find the line associated with the client in question. It should look something like this:

```
Client: 16.119.237.171 (0xabed7710) NACKs = 8
```

Here you can see that the server did receive all the NACKs the client sent. If these numbers were not the same, it would indicate that one or more NACKs had been lost. In that case, you should increase the value of the `nackresend` parameter. This will cause each NACK packet to be retransmitted more times, increasing the probability that the client will see at least one of the redundant packets.

For the case where the server has seen all the NACKs sent from the client, it probably indicates that the client did not issue a NACK when it needed to.

In the agent log file, look for the following line:

```
Max resend hits = n
```

Here, `n` is the number of times the client did not issue a NACK because the value of the `maxresendreq` parameter had been exceeded. If you cannot remedy the cause of the excessive number of NACKs, you may want to increase the value of `maxresendreq`, thus enabling the client to NACK a given block more times.

# Test Modules

The following commands are provided as test tools that you can use to manually test different combinations of parameters, rather than running tests in the full OS Manager environment.

## Using GDMCSEND



The `gdmcsend` command can be run from a Windows environment only.

`gdmcsend` is the server side multicast send command.

On the 5.00 media in `Infrastructure\extended_infrastructure\multicast_server\multicast_test_modules\` there is a script called `gdmsend.cmd` that can be used for testing.

### To start the multicast test sender module

- 1 Copy the multicast test send modules (`gdmcsend.exe`, `gdmcsend.cmd`, and `TESTDATA0004`) from the `extended_infrastructure\multicast_server\multicast_test_modules` directory on the infrastructure CD to a temporary directory.
- 2 Rename `TESTDATA0004` to `GDMCTESTDATA`.
- 3 Edit `gdmsend.cmd` and change `DP` on line 19 from `0.0` to `0.5`.
- 4 Edit `gdmsend.cmd` and change `OFFSET` on line 49 from `60` to `0`.
- 5 Run `gdmsend`.

If you want to modify the script, use a text editor to open the file and modify the parameters. Then, you can run this file to test the changes you made. See [Example of Using the Test Modules](#) on page 173.



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

Below are two forms of the command and the valid options for each. Explanations of the parameters follow.

Use this command if you are using reliable delivery resend mode.

```
gdmcsend -rm D|B -ma multicast_address -mp multicast_port -np
nac_port -f file_name -npb nblocks -ppb npackets[-dpl 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 13 gdmcsend command options**

Option	Corresponding parameter in mcast.cfg	Description	Default
<b>-dl</b> <i>linger_delay</i>	lingerdelay	The delay, in milliseconds, between checking for resend requests after the last packet has been sent.	64.0
<b>-dp</b> <i>delay</i>	gdelaybp	Delay, in milliseconds, after sending each packet.	0.0625
<b>-dp1</b> <i>delay</i>	N/A	Delay, in milliseconds, after sending the first packet.	5
<b>-f</b> <i>filename</i>	N/A	Name of the file containing the data to be sent.	N/A
<b>-lc</b> <i>n</i>	lingercount	Linger count. The number of times to check for resend requests (NACKs), after the last packet has been sent.	256

<b>Option</b>	<b>Corresponding parameter in mcast.cfg</b>	<b>Description</b>	<b>Default</b>
<b>-lf</b> <i>log_file</i>	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
<b>-lpr</b> <i>n</i>	lprcount	Last packet resend. The number of times to resend the last packet.	4
<b>-lprd</b> <i>delay</i>	lprdelay	Last packet resend delay. The delay, in milliseconds, between last packet resends.	0.25
<b>-ma</b> <i>multicast_address</i>	N/A	Multicast address. The address to which the data is sent.	N/A
<b>-mp</b> <i>multicast_port</i>	N/A	Multicast port. The port to which the data is sent.	N/A
<b>-ni</b> <i>ip_address</i>	N/A	Network interface. The IP address identifies the specific local network interface to use when sending data.	selected automatically
<b>-np</b> <i>nac_port</i>	N/A	NACK port. The port from which resend requests are read.	9514

Option	Corresponding parameter in <code>mcast.cfg</code>	Description	Default
<code>-npb nblocks</code>	N/A	Number of packet blocks. The number of packet blocks available to be resent.	N/A
<code>-nr n</code>		The number of times to resend each packet. This option only applies when resend mode ( <code>-rm</code> ) is set to <b>F</b> .	0
<code>-offset n_bytes</code>	N/A	Skip the first <i>n_bytes</i> bytes of the file.	0
<code>-ppb npackets</code>	N/A	Packets per block. The number of packets in each packet block (must be a multiple of 32).	N/A
<code>-rm F B D</code>	N/A	Resend mode. <b>F = fixed</b> Each packet block is resent a fixed number of times (as specified by the <code>-nr</code> option). <b>B = backup</b> Resend all blocks from the lowest number requested to the current block (last block sent by the sender). <b>D = discrete</b> Resend only requested blocks.	B



<b>Option</b>	<b>Corresponding parameter in mcast.cfg</b>	<b>Description</b>	<b>Default</b>
<b>-tf</b> <i>throttle_frequency</i>	throtfreq	The minimum number of packet blocks between throttle adjustments.	8
<b>-ti</b> <i>throttle_increment</i>	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
<b>-tmax</b> <i>throttle_maximum</i>	throtmax	The maximum value of the inter-packet delay before throttling will stop.	0.5
<b>-tmin</b> <i>throttle_minimum</i>	throtmin	The minimum value of the inter-packet delay before throttling will stop.	0.0
<b>-tthigh</b> <i>high_throttle_threshold</i>	throthighth	The average number of resends per block that will trigger an increment of the inter-packet delay.	-1 (throttling disabled)
<b>-ttlow</b> <i>low_throttle_threshold</i>	throtlowth	The average number of resends per block that will trigger a decrement of the inter-packet delay.	-1 (throttling disabled)
<b>-ttl n</b>	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, `gdmcrecv.sh`. For an example of how this may be used, see [Example of Using the Test Modules](#) on page 173.



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

Below are two sample commands and explanations of the parameters follow.

Use this command if you are using reliable delivery resend mode.

```
gdmcrecv -rm D|B -ma multicast_address -mp multicast_port -np
nac_port-na nac_address -npb nblocks -ppb npackets[-t
timeout_minutes] [-nit timeout_minutes][-mr max_resend_req] [-
nd nac_delay] [-nr nac_resends][-lf log_file] [-bt
block_threshold] [-ni ip_address][-pmf freq] [-stderr]
```

Use this command if you are using the fixed resend mode which resends each packet block a fixed number of times.

```
gdmcrecv -rm F -ma multicast_address -mp multicast_port -ppb
npackets[-t timeout_minutes] [-nit timeout_minutes][-lf
log_file] [-ni ip_address]
```

**Table 14 gdmcrecv command options**

Option	Corresponding parameter in mcast.cfg	Description	Default
<code>-bt</code> <i>block_threshold</i>	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

<b>Option</b>	<b>Corresponding parameter in mcast.cfg</b>	<b>Description</b>	<b>Default</b>
<b>-lf</b> <i>log_file</i>	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
<b>-ma</b> <i>multicast_address</i>	N/A	Multicast address. The address from which data is read.	N/A
<b>-mp</b> <i>multicast_port</i>	N/A	Multicast port. The port from which data is read.	N/A
<b>-mr</b> <i>max_resend_req</i>	maxrsndreq	The maximum number of times a resend can be requested for each block.	128
<b>-na</b> <i>nac_address</i>	N/A	NACK address. The address to which resend requests are sent.	N/A
<b>-nd</b> <i>nac_delay</i>	nacdelay	The delay, in milliseconds, between sending resend requests.	0.5
<b>-ni</b> <i>ip_address</i>	N/A	Network interface. The IP address that identifies the specific local network interface to use to receive data.	selected automatically

<b>Option</b>	<b>Corresponding parameter in mcast.cfg</b>	<b>Description</b>	<b>Default</b>
<b>-nit</b> <i>timeout_minutes</i>	netinacto	The time to wait, in minutes, between received packets before failing.	5
<b>-np</b> <i>nac_port</i>	N/A	NACK port. The port to which resend requests are sent.	9514
<b>-npb</b> <i>nblocks</i>	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
<b>-nr</b> <i>nac_resend</i>	nacresend	The number of times each NACK should be resent.	4
<b>-pmf</b> <i>freq</i>	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
<b>-ppb</b> <i>npackets</i>	pktsperblk	Packets per block. The number of packets in each packet block (must be a multiple of 32 and match the value used by the sender).	N/A

Option	Corresponding parameter in <code>mcast.cfg</code>	Description	Default
<code>-rm F B D</code>	N/A	Resend mode. <b>F = fixed</b> Each packet block is resent a fixed number of times (as specified by the <code>-nr</code> option). <b>B = backup</b> Resend all blocks from the lowest requested to the current. The receiver will only send resend requests (NACKs) for the lowest block needed. <b>D = discrete</b> Resend only requested blocks. The receiver will send resend requests (NACKs) for every block needed.	B
<code>-stderr</code>	N/A	Write log messages to <code>stderr</code> (standard error), as well as the log file.	FALSE
<code>-t</code> <code>timeout_minutes</code>	<code>recvtimeout</code>	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 `gdmrecv`, 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:

- Restoring Operating Systems
- Addressing Requirements for Capturing, Recovering, and Migrating Data
- Using COP with OS Manager

This chapter discusses advanced features that are available with the OS Manager. These features are for use by those who are extremely comfortable with HP Client Automation.

## Restoring Operating Systems

The OS Manager allows you to restore your operating system in last resort situations. Restoring the operating system provides you with a working operating system however *you will lose all data* and you may need to perform some customizations such as changing the computer name or installing the agent.



The ROM object will not be updated and therefore may not reflect the device's actual state.

### Pre-requisite

- The ImageDeploy media. See [Product Media](#) on page 27 if you need more information about how to create this media.
- A working operating system stored on the network, to a cached location or on a CD/DVD.

### To recover your operating system

- 1 Insert the CD-ROM that you created from the `ImageDeploy.iso` in the `\service_cd` folder on the product CD-ROM.
- 2 Boot the target device.
- 3 When asked which Service OS to use, select `_SVC_LINUX_` or `SVC_PEX86_`.
- 4 You will see several messages and then a menu opens with the following choices:
  - 1. Service OS networking (default selection if no option is chosen)
  - 2. Install OS from cache partition
  - 3. Install OS from CD or DVD
- 5 Type the number corresponding to the action you want. If you select:
  - 1. Service OS Networking you must be connected to a network.



If you chose to use the Linux Service OS, and DHCP is found, you will be prompted for the OS Manager Server's IP address and then the appropriate OS image will be installed to your device.

or

If DHCP is not found, you will be prompted for network information such as the following before the appropriate OS image can be installed to your machine:

- IP address for the target device
- Default gateway
- Subnet
- Subnet mask
- DNS address
- OS Manager Server IP address

You may choose to store the network information on a USB drive or floppy disk. To do this, prepare the following .ini files:

- romsinfo.ini

This includes information about the OS Manager Server. It should be ordered from the top down with the most-specific information to the least-specific information. When a match to the OS Manager Server s found on the left, the information on the right will be used.

In the sample romsinfo.ini file below:

```
[ROMSInfo]
192.128.1.99=192.168.123.*, 192.168.124.*,
192.128.125.*
osm.usa.hp.com=192.168.*
osm.hp.com=*
```

The first line looks at the machine to see if it falls within one of the subnets listed (192.168.123.\*, 192.168.124.\*, 192.128.125.\*). The asterisk is used as a wildcard. If there is a match, then the machine will use the OS Manager Server with the IP address specified on the left (e.g., 192.128.1.99).

If no match is found, then the second line of the file is used. This one looks at the machine to see if it falls within a subnet that begins with 192.168.\*. If so, the machine will use osm.usa.hp.com to find the OS Manager Server.

If no match is found again, the third line of the file is used. This one indicates that `osm.hp.com` should be used to find the OS Manager to be used by the machine, no matter what subnet it is part of.

```
[ServiceCD]
source=net
netif=eth0
```

The first line defines where to get the image. Valid values are `net`, `cd`, or `cache`. Use this if you want to prevent the user from being prompted for this information.

The second line defines which NIC to use. If there are multiple NIC cards and you do not specify this parameter, then the first NIC card that is discovered will be used. Valid values are `eth0` – `eth3`.

– `netinfo.ini`

This includes the networking information. If there is more than one section (such as a `[SubnetDisplayName2]`), you will be prompted about which information to use.

▶ You can use `addr` to specify a range of IP addresses. This allows you to store the information on one USB drive or floppy disk that will be useful for multiple machines.

```
[SubnetDisplayname1]
addr=192.168.123.50-192.168.123.69
gateway=192.168.123.254
subnet=192.168.1.0
netmask=255.255.255.0
dns=192.168.123.1
```

▶ If you do not know the DNS, leave the keyword `dns=` in the `.ini` file.

Insert your recovery CD-ROM and then insert the USB drive or floppy disk shortly after the device begins to boot. When configuration is complete, you will see the message “Network configuration successful.”

- 2. Install OS from cache partition.

If you have a target device that is managed by the OS Manager and you created a cache type partition as described in [Table 8](#) on page 129, 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 Core 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 (such as personality information), HP provides the ROM Client method (`romclimth.tkd`), which has two exit points. This method is stored in `SystemDrive:\Program Files\Hewlett-Packard\CM\Agent`.

The exit points call two optional scripts—`Novapdc.cmd` (data capture) and `Novapdr.cmd` (data restore)—that must be also stored in `SystemDrive:\Program Files\Hewlett-Packard\CM\Agent`. You can use these scripts to customize data capture, recovery, and restoration for any product that you would like to use.

Capturing, recovering and migrating data relies on the OS Manager User Agent because data can be captured only when the OS is running. The Application Manager senses the change to a device's desired state and triggers the data capture if `Novapdc.cmd` is available in `SystemDrive:\Program Files\Hewlett-Packard\CM\Agent`. Then, the target device reboots and the new operating system is installed. If `Novapdr.cmd` is available, the ROM Client method begins the restore process after the OS has been installed on the target device.

## Sample Command Lines

The following is a sample of a command line used to capture data using HP Client Automation Settings Migration Manager.

```
Path\SE.exe /autoextract /http IntegrationServer:Port  
UniqueName overwrite:yes /allusers
```

The following is a sample of a command line used to restore data using HP Settings Migration Manager.

```
Path\SE.exe" /autoinject /http IntegrationServer:Port  
UniqueName /allusers
```

See *HP Settings Migration Manager's* documentation for more details.

## Return Codes for HP Exit Points

The following return codes are returned from the HP exit points `Novapdc.cmd` and `Novapdr.cmd`. The values may vary depending on the software that you are using with these exit points. If the return value of the method is not equivalent to the following, use the standard batch error level conditional processing and the exit command to make them correspond to the following:

**Table 15 HP Exit Point Return Codes**

Code	Description
0	Successful.
1	An error occurred and will be logged, but processing will continue. The log is located in <code>SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log</code> .
2	<b>For <code>Novapdc.cmd</code> (capture):</b> <ul style="list-style-type: none"><li>A fatal error has occurred and will be logged. The log is located in <code>SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Logs\romclimth.log</code>. Processing of the service has ended.</li></ul> <b>For <code>Novapdr.cmd</code> (restore):</b> <ul style="list-style-type: none"><li>An error has occurred and will be logged. The log is located in <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.</li></ul>

## 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 141 for more information.
- Name instances in `PRIMARY.CLIENT.LOCATION` only by subnet.
  - If you are using Client Operations Profiles, failover for the location of data is supported in the following scenarios:
    - If the first SAP is a CD but there are no valid resources on the current CD or there is no CD.
    - If there is more than one SAP for a Proxy Server, the OS Manager will failover from one SAP to another, respecting the connection order in the `LOCATION` instance. Client Operations Profiles can only be used to redirect the Application Manager and/or OS Manager Server to an alternate data source.

- If you want to deploy an image using a CD resource, set `TYPE` to `DATA` and `ROLE` to `Z`. Then, specify the URI as `cdr://` to indicate that you want to use the agent's local CD/DVD drive. The first CD/DVD drive detected is used.

## Using the Proxy Server with OS Manager Server and Client Operations Profiles

If you have a Proxy Server that contains OS images and applications, you would set up your SAP instances as follows:

- For the Proxy Server that contains OS images, create an SAP instance with the following settings:
  - `TYPE=DATA`
  - `ROLE=Z`
- If there is a Proxy Server that contains the all other data (such as applications), create the SAP instance with the following settings:
  - `ROLE=D`
- If there is a Proxy Server that contains all data, create SAP instances with the following settings:
  - `ROLE=DZ`

---

# 11 Building a Custom WinPE Service OS

This chapter includes the following topics:

- Prerequisites
- Adding Drivers to the WinPE Service OS
- Building a Custom WinPE Service OS and Maintaining the ISOs
- Using Customized build.config Files (Advanced Option)

HP provides a script that allows you to:

- For OS Manager versions 5.1x and later, update the WinPE Service OS when a new `winpe.wim` is made available through an updated WAIK. The `winpe.wim` from the WAIK is used as the basis for building the customized WinPE SOS.
- For OS Manager versions 5.1x and later, add extra drivers or packages that do not exist in the WinPE SOS provided. Follow the instructions below in conjunction with your knowledge of Microsoft's Windows Automated Installation Kit to rebuild the WinPE Service OS with the drivers and packages necessary for your environment.
- Add support for Chinese, Japanese and Korean languages.
- For OS Manager versions 5.1x and later, 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.
- For OS Manager versions 5.1x and later, 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.
- For OS Manager versions 5.0 and before, create a new `Media.iso` if you have updates that need to be applied such as fixes from HP.
- For OS Manager versions 5.0 and before, create a new `Service.iso` if you have updates that need to be applied such as fixes from HP.

## Prerequisites

- For OS Manager versions 5.1x and later, a machine with Windows Automated Installation Kit (WAIK) installed.



Do not use the machine where your Boot Server is installed.

- A good understanding of Microsoft's process to add drivers and other information to the WinPE SOS.
- Go to `\custom_build` on the product media and copy `build_scripts.zip` to the machine.
- For OS Manager versions 5.1x and later, Image Capture and Image Deploy CDs.
- For OS Manager versions 5.0 and before, the product media CD and the Service CD for the appropriate version.



- Do not run this script on a machine that has cygwin installed as this is not supported.
- For OS Manager versions 5.1x and later, if you are generating a new `ImageCapture.iso` or `ImageDeploy.iso`, you must do the following to include the updated files necessary for your ISO.
  - a Create a build items directory on the machine such as `c:\build_items`.
  - b Copy the updated files that you received from CPE to the build items directory. Create subdirectories as needed, based on the structure on the Image Capture or Image Deploy media. If any required files are not in this directory, you will be prompted to insert the previous Image Capture or Image Deploy media so the files can be copied.
  - c (Optional) You can include `romsinfo.ini` (on page 177) or `netinfo.ini` (on page 178) in the build items directory for use on the ImageDeploy CD.
  - d (Optional) You can include `rombl_capture.cfg` and `rombl_deploy.cfg` in the build items directory for use on the appropriate iso. To create these files, copy `rombl.cfg` from the previous `ImageCapture.ISO` or `ImageDeploy.ISO`, modify and rename them as necessary. The files contain information such as the menu timeout settings, and the default Service OS.
 

If you do not include these files in the directory, the script prompts you for the previous CD-ROM and retrieves the files from the media. If you choose not to insert a CD-ROM then a standard `rombl.cfg` file will be created automatically.
- If you want to add support for Chinese, Japanese and Korean (CJK) without making additional changes to the iso:
  - Remove any existing `winpe.wim` files from the `build_items` directory.
  - Copy `winpe_cjk.wim` from the `\custom_build\lang_support` directory on the product CD-ROM to the `build_items` directory.
  - Rename `winpe_cjk.wim` to `winpe.wim`.
  - See [Building a Custom WinPE Service OS and Maintaining the ISOs](#) on page 187 to run the script.



If you want to use the CJK-enabled `winpe.wim` file without rebuilding the `winpe.wim` file, be sure to type `N` when prompted to recreate the `winpe.wim`.

- If you are using the ImageDeploy CD to install from CD or are installing from a cache and want messages to appear in your local language, copy the `\custom_build\lang_support\i18n` directory from the product CD-ROM to the `build_items` directory. You may remove the `.msg` files that are not needed for your local language.
- (Advanced option) If you are using a pre-existing `winpe.wim` file:
  - It is strongly recommended that the pre-existing `winpe.wim` was built using the same version of WAIK that is installed on the computer where you are executing the build scripts.
  - The file must have the following packages installed:
    - WinPE-HTA-Package
    - WinPE-Scripting-Package
    - WinPE-XML-Package
    - WinPE-WMI Package
  - If your `winpe.wim` file has been prepared using the `peimg /prep` command see Microsoft WAIK, `peimg`, and ImageX documentation for restrictions.


## Adding Drivers to the WinPE Service OS

For OS Manager versions 5.1x and later, if you would like to add drivers to the WinPE Service OS, you can do this when running the build scripts. For example, if you have a driver that needs a reboot, you must do it in “offline” mode, which means that the `build_script` will pause and you can make any necessary changes at that time. This is described in detail in the steps below.




Additionally, you can add drivers to WinPE while it is running (“online”). The drivers must be fully contained without need for a reboot and the device must have connectivity to the OS Manager Server. During the startup of the WinPE SOS, any drivers that exist in `CSystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\SOS\WinPE\drivers` will be downloaded and installed using `drvload.exe`.

## Building a Custom WinPE Service OS and Maintaining the ISOs


 Be sure to review [Prerequisites](#) on page 184 before using the script.

To use HP's script to build a custom WinPE Service OS and Maintain the Image Capture/Deploy ISOs

- 1 Copy `Build_scripts.zip` to a location on the machine with WAIK installed.
- 2 Unzip `Build_scripts.zip` to a directory such as `C:\Build_scripts`.
- 3 Go to a Windows command prompt and change to the new directory. In this example, the directory would be `C:\Build_scripts`.
- 4 Type `run`.
- 5 When asked whether you want to create a new WIM file, type **Y** or **N**.


 If you are using `winpe_cjk.wim` and do not want to rebuild the `winpe.wim` file, be sure to type **N** when prompted to recreate the `winpe.wim`

- 6 If you type **Y**, you will be prompted to type the path to your Windows AIK tools directory, type the directory such as `C:\Program Files\Windows AIK\Tools`.
- 7 When asked whether you want to use the `winpe.WIM` file from the Microsoft Windows AIK, type **Y** or **N**.

 It is strongly recommended that you use the `winpe.WIM` file from the Microsoft Windows AIK.

If you type **N**, you will be reminded to ensure that your pre-existing `winpe.wim` file is built according to specifications. Then, you will be prompted to specify the fully qualified path of the pre-existing `winpe.WIM` file.

- 8 When asked whether you want to include the local font support packages (Chinese, Japanese and Korean), type **Y** or **N**.
- 9 When asked whether you want to pause the WIM creation process to add extra drivers or packages, type **Y** or **N**.

- 10 When asked whether you want to provide a path to a directory for additional drivers to be added during the WIM creation process, type **Y** or **N**.
- 11 If you typed **Y** to the previous question, you will be asked to enter the fully qualified path to the directory with the drivers.
- 12 When asked whether you want to create a new Image Capture ISO, type **Y** or **N**.
- 13 When asked whether you want to create a new Image Deploy ISO, type **Y** or **N**.
- 14 When asked which Service OSs to include on the ISOs, type the appropriate selection. Then, press **Enter**.
- 15 When asked if you want to create a new `rombl.cfg` or use a pre-existing `rombl.cfg` type the appropriate number. If you choose to use a pre-existing `rombl.cfg`, skip to step 17.
- 16 When asked which Service OS you want to boot by default, type the appropriate selection. Then, press **Enter**.
- 17 When asked to configure the boot menu for the Image Capture CD/DVD, type the appropriate value for your environment based on the on-screen description.
- 18 When asked to configure the boot menu for the Image Deploy CD/DVD, type the appropriate value for your environment based on the on-screen description.
- 19 When prompted to type the fully qualified path to the build items, type the directory such as `C:\build_items` and press **Enter**.
- 20 When prompted to type the fully qualified path for the temporary work directory, type a directory such as `C:\build_work`. This directory will be referred to as the `<work-dir>` in later steps.
  -  If the directory already exists and has information in it, you will be asked whether you want to delete the information or not. If you choose no, you will be asked to type a directory again. If you prefer to exit, press **Ctrl + C** to exit the process. If you choose yes, the information will be overwritten.
- 21 When prompted to type the fully qualified path for the output directory, type a directory such as `C:\build_output`.

► If you are prompted to create ISOs for CAS, type **n**.

- 22 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.
- 23 The information you entered will be saved and the WinPE directory creation begins.
- 24 If you indicated that you wanted to pause the WIM creation process to add extra drivers or packages, the process will pause after the WinPE directory is created and the contents of `winpe.wim` are extracted into the WIM directory, e.g., `C:\build_work\WIM`. There are two ways to do this:

- a Use the `peimg` command to make your modifications. This uses `PEimg.exe` which is included in the WAIK in `C:\Program Files\Windows AIK\Tools\PETools\PEimg.exe`. See the WAIK documentation for information about how to use this command or type `peimg /help`.

This method is useful for testing the additional drivers and packages you are including. After you have successfully added the drivers and packages, you may want to use the next method so that you do not have to repeat this step manually each time you build a new `winpe.wim`.

- b Add drivers to a driver list. After you see a message indicating that all required information is gathered, `build.config` will be created in `C:\Build_scripts` to store this information that is needed to build the `winpe.wim` and ISOs. Use a text editor to open this file and add the appropriate drivers below the empty DRIVERS list. For example:

```
declare DRIVERS = " \  
    cdrom.inf \  
    e:\tmp\work\WIM\windows\inf\adp94xx.inf \  
    e:\tmp\work\WIM\windows\inf\3com*.inf \  
"
```

If you do not specify a directory, the script will search for the driver in the `<work-dir>\WIM\Windows\inf`. If you prefer, provide a fully qualified path that specifies the location and driver, such as `c:\anydirectory\mydrivers.inf`. The last option is to provide a path with a filename containing a wild card, such as

`c:\anydirectory\md*.inf` which will install all `md*.inf` files found in `c:\anydirectory`.

After you are done, type **run** to continue and the drivers will be added to `winpe.wim`.

If you run the script again in the future, you will be prompted about whether you want to keep the `build.config` file or replace it with a new one. Also, the script will pause automatically. If you do not have additional packages or drivers to add, simply type **run** to continue.

25 This process takes some time as you will see from the messaging on screen. When done, you will see a message indicating that the SOS creation process completed successfully and be returned to a command prompt.

26 Go to the directory where the `WinPE.wim` was built, such as `C:\WinPE_output` and

- For PXE, copy `winpe.wim` to `SystemDrive:\Program Files\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot`.
- For LSB, use the CSDB Editor to replace the `winpe.wim` in the LSB package.
- For the CD, you must create a new ISO using the `winpe` scripts.

If you chose to create a `ImageCapture.iso` or `ImageDeploy.iso`, it will be stored in this directory as well.

#### To use HP's script to Maintain the Media/Service OS ISOs

- 1 Copy `Build_scripts.zip` to a location on the machine.
- 2 Unzip `Build_scripts.zip` to a directory such as `C:\Build_scripts`.
- 3 Go to a Windows command prompt and change to the new directory. In this example, the directory would be `C:\Build_scripts`.
- 4 Type **run**. If you have run this script before, the version previously selected appears in blue text.
- 5 From the version list, select the version to be used.
- 6 When asked whether you want to create a new Media ISO, type **Y** or **N**.
- 7 When asked whether you want to create a new Service ISO, type **Y** or **N**.
- 8 When prompted to type the fully qualified path to the build items, type the directory such as `C:\build_items` and press Enter.

- 9 When prompted to type the fully qualified path for the temporary work directory, type a directory such as `C:\build_work`. This directory will be referred to as the `<work-dir>` in later steps.



If the directory already exists and has information in it, you will be asked whether you want to delete the information or not. If you choose no, you will be asked to type a directory again. If you prefer to exit, press **Ctrl + C** to exit the process. If you choose yes, the information will be overwritten.

- 10 When prompted to type the fully qualified path for the output directory, type a directory such as `C:\build_output`.
- 11 When prompted as to whether the Media CD is loaded, type **Y** or **N**.

The information you entered will be saved and the ISO creation begins. This process takes some time as you will see from the messaging on screen. When done, you will see a message indicating that the ISO creation process completed successfully and be returned to a command prompt.

- 12 When prompted as to whether the Service CD is loaded, type **Y** or **N**.
- 13 Go to the directory, such as `C:\build_output`, to access your new `Media.ISO` and `Service.ISO`.

## Using Customized `build.config` Files (Advanced Option)

If you choose, you can take an existing `build.config` file and save it with another name. You may want to do this if you need to maintain varying sets of configurations or if you are testing based on an existing configuration. You can add drivers to the file as specified above.

Place the file in the directory where you unzipped the `build_scripts.zip` file, such as `C:\build_scripts`.

When you run the script, instead of typing `run` use the following command:

```
run.cmd -f mybuild.cfg
```

If you do not include the `-f` parameter, the default `build.config` will be created and used.





---

# 12 Double Byte Character Support

This chapter includes the following topics:

- Supported Languages
- Changing the Locale

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 creating an image (with the HPCA OS Manager Image Preparation Wizard or the HPCA Windows Native Install Packager) the locale for your reference and target devices must match. For example, if you want to create a Simplified Chinese OS image, you must run the Image Preparation Wizard or the Windows Native Install Packager on a Simplified Chinese reference machine.



If there are no double-byte requirements, do not make any of the following changes.

## Supported Languages

- Simplified Chinese
- Japanese
- Korean

## Changing the Locale

To add support for Simplified Chinese, Japanese, or Korean in a PXE environment

- 1 Use a UNIX based text editor to open `C:\Hewlett-Packard\CM\BootServer\X86PC\UNDI\boot\linux.cfg\default`.

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

The file looks similar to the following:

```
[OS Manager]
DFLTSVOS=_SVC_LINUX_
ISVR=10.10.10.1:3469

[_SVC_LINUX_]
KERNEL=bzImage
APPEND initrd=rootfs.gz root=/dev/ram0 rw quiet pci=nommconf
[SVC_PEX86]
PEBCD=rombl.bcd
PEAPPEND=initrd=winpe.wim
```

Add the **LANG** parameter to the end of the **APPEND** line and set it to **LANG=CJK**. As a result, the line will look similar to the following:

```
APPEND initrd=rootfs.gz root=/dev/ram0 rw LANG=CJK
```

- 2 Save and close the default file.

To add support for Simplified Chinese, Japanese, or Korean when restoring from the Service CD-ROM

- Specify **LANG=CJK** in the **ServiceCD** section of the `romsinfo.ini` file.

## Setting the System Language Parameter

In this section, you will set the System Language parameter in the Behavior instance. Doing so sets the locale for the service operating system and OS Manager System Agent messaging. This affects PXE environments, LSB environments and restoring operating systems from a CD-ROM or DVD.

To set policy to enable support for other languages

- 1 Log in to the CSDB Editor.
- 2 Go to the appropriate PRIMARY.OS.BEHAVIOR instance.
- 3 Double-click the LANG attribute
- 4 Select the appropriate language.
  - en\_US = English
  - zh\_CN = Simplified Chinese
  - ja\_JP = Japanese

— ko\_KR = Korean

- 5 Drag and drop the BEHAVIOR instance to the appropriate POLICY instance.

## Double-byte support for Sysprep or Unattend.txt files

If using double byte characters unattend.txt the file must be encoded in UTF-8 coding.

For Sysprep files, follow double-byte character rules as stated by Microsoft.

---

# 13 Troubleshooting

This chapter includes the following topics:

- OS Manager Server Logs
- Locating the Payloads
- Configuration Server and Configuration Server DB Logs
- Image Preparation Wizard Log
- Agent Logs and Objects
- Capturing, Migrating, or Recovering Data
- Basic Infrastructure Tests
- Collecting Information for Technical Support
- Gathering Version Information
- Frequently Asked Questions
- Using the Discover Boot Server Utility



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

## OS Manager Server Logs

The OS Manager Server writes several logs, which can be used to track progress and diagnose problems. The log files for the OS Manager Server are:

- `httpd-port.log`

This is the main log, stored by default in `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\logs`. It contains information about the actions that you perform, as well as version and build numbers.

Replace *port* with your port number, for example, `httpd-3469.log`.

Each time you start the web server a new log is written. The old log is saved as `httpd-port.nn.log`.

- `httpd-port.YY.MM.DD.log`

This log, stored by default in `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\logs`, contains the web server activity for each day. If the log is empty, it means that there was no activity that day.

- `httpd-port.error.txt`

This log, stored by default in `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\logs`, contains messages written to any logs that contain the prefix **ERROR**. This allows you to view all errors in a single location.

- `machineID-all.log`

This log, stored by default in `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload`, is a comprehensive log that is written after the OS Manager System Agent is executed. You will find one log for each device managed by the OS Manager. Open this log with WordPad, rather than Notepad.



This log may be named `macAddress-all.log` if the machine instance has not been created.

The following example from this log shows that the Configuration Server and Proxy Server address are in use, which confirms a successful image deployment.

```
20030703 10:10:01 Info: ::HOSTINFO(RCSHOST)
:10.10.10.2:3464

20030703 10:10:01 Info: ::HOSTINFO(RPSHOST)
:10.10.10.2:3466
```

## Locating the Payloads

Payloads are the files that contain the modules that run under the Service OS. These files are provided by HP and can be found:

- in `\OSManagerServer\OSM\SOS\linux\payload` for Linux
- in `\OSManagerServer\OSM\SOS\winpe\payload` for WinPE

The payload file for Linux is named `LNX-version_00000.tgz` and the payload file for WinPE is named `WPE-version_00000.tgz`. The second three digits are the version number and the last five digits are the build number

## Configuration Server and Configuration Server DB Logs

Refer to the *HP Client Automation Enterprise Configuration Server User Guide*.

## Image Preparation Wizard Log

- `setup.log`  
This log is created while the Image Preparation Wizard is running in Windows. It is located in the `\setup` directory of the TEMP environment variable. It may be in a location similar to `c:\winnt\temp\setup.log`.
- `osclone.log`  
This log is created while `osclone` is running and is found in the local directory from which `osclone` is run (the Service OSs `\work` directory). When `osclone` is complete, the `osclone.log` is uploaded to the OS Manager's `\upload` directory as `imagename.log`.

## Agent Logs and Objects

Use the agent logs (*SystemDrive:/Program Files/Hewlett-Packard/CM/Agent/Logs*) and agent object information (*SystemDrive:/Program Files/Hewlett-Packard/CM/Agent/LIB*) on the managed device to confirm that the following OS Manager Server services have installed successfully during the first agent connect:

- Operating System Service
- OS Manager Server agent files

If policy dictates that the Local Service Boot service is installed, you can also confirm that the LSB service has been installed.

You may want to review the following agent logs located in *SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\Logs*:

- *Connect.log*
- *Romclimth.log*  
This log stores information about operating system (OS) service resolution.
- *LSB.log*  
This log contains information about LSB installation.

You may want to review the following agent object information (located in *SystemDrive:\Program Files\Hewlett-Packard\CM\Agent\LIB*):

- *OS/ZSERVICE/MASTER.edm*  
Review the ZMASTER object for the OS Service.

## Capturing, Migrating, or Recovering Data

If you use this capability, logs will be available in *C:\Program Files\Hewlett-Packard\CM\Agent* on the managed device.



# Basic Infrastructure Tests

After you have installed your OS Manager Server infrastructure, the following tests may help you to determine whether your environment is properly configured.

## Test 1: For use in an environment without bare metal machines

If you can answer yes to all of the following questions:

- Are you able to boot (via PXE) to a device that has not been discovered by OS Manager Server and does not have an OS that is managed by OS Manager Server?
- Does a device object get created in the Portal when a device is discovered?
- When a device is discovered, is a log uploaded to the OS Manager's `\upload` directory?

Then the following are working correctly:

- DHCP, PXE/TFTP Server, Configuration Server, Portal, and OS Manager Server are working correctly.
- The Configuration Server has the files needed to handle OS Manager Server objects.
- Service OS (Linux and/or WinPE) is able to handle the target device.

## Test 2: For use in an environment with bare metal machines

If you can answer yes to all of the following questions:

- Are you able to boot a bare metal machine via PXE?
- Does a device object get created in the Portal when a device is discovered?
- When a device is discovered, is a log uploaded to the OS Manager Server's `\upload` directory?
- Is an OS installed on the machine?

Then:

- DHCP, PXE/TFTP Server, Configuration Server, Portal, and OS Manager Server are working correctly.
- The Configuration Server has the necessary files to handle OS Manager Server (COP) objects.

- Service OS (Linux and/or WinPE) is able to handle the target device.
- OS Policy correctly chose one OS.
- The OS State for the MACHINE instance is set to DESIRED.

## Test Results

If any of the tests failed, you may have some problems with your infrastructure. Be sure to collect the following information:

- How are you trying to set up the infrastructure?
- In what order did you install the components?
- Gather the necessary logs related to your problem.

## Collecting Information for Technical Support

If you need to contact Technical Support for assistance, be sure to review the latest release notes and confirm that you have installed any fixes. If you still need assistance, then collect the following information:

- Hardware information (including manufacturer, model, BIOS/firmware version for the NIC card, hard drive controller card, and hard drive).
- Gather the following files or folders:
  - *SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID-all.log*
  - *SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID\_rnl.log*
  - *SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\logs* **directory**

**or**

  - *SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\RomVer.log*
  - *SystemDrive:\Program Files\Hewlett-Packard\CM\ConfigurationServer\log\nvdmr001.log*. **The 001 represents the ID used during the installation of the Configuration Server.**

- If specifically requested, gather the `.MBR` and `.PAR` files from `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\UPLOAD` on the OS Manager Server.
- What results you were expecting, what actually happened, and any other related details.
- Whether the problem can be reproduced. If so, specify the exact steps (providing detailed information) to reproduce the issue.
- Specify whether the issue occurs on more than one device.
- Indicate whether the image was ever successfully deployed. If so, what has changed since the successful deployment?
- If deployment of an image stops and goes to a bash prompt, be sure to collect the `OSSELECT.log` file. Use the following command to copy the `OSSELECT.log` to the Integration Server `\upload` folder:
 

```
curl -T osselect.log
http://$ISVR:$ISVRPORT/upload/osselect.log
```

## Gathering Version Information

### OS Manager Server Components

To determine the versions of the OS Manager components, go to `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer` and run `Romver.cmd`. The log is created in the same directory.

### OS Manager Admin Module

To determine the versions of the OS Manager Admin Module components, go to `SystemDrive:\Program Files\Hewlett-Packard\CM\ManagementPortal` and run `Romadver.cmd`. The log is created in the same directory.

To determine the versions of the Configuration Server, go to `SystemDrive:\Program Files\Hewlett-Packard\CM\ConfigurationServer` and run `Rcsver.cmd`. The log is created in the same directory.

## NVDKIT.EXE and .TKD Files

- The module and version information for the following items can be found by running the `Romver.cmd` mentioned above.
  - `nvdkit.exe`
  - `expandsmbios.tkd`
  - `roms.tkd`
  - `roms_udp.tkd`
- See the `httpd-port.log` for version and build information.

## Configuration Server and Configuration Server Database

*HP Client Automation Enterprise Configuration Server User Guide*

## SOS/Payload/OS Manager System Agent

To determine the version of the SOS and payload that you were running, you can use a text editor to open `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID_rn1.log`. Look for **Extracting payload file and check LNX-version for the Linux SOS and WPE-version for the WinPE SOS**. If you find `OSD-50` this indicates you are using a 5.0 payload. Next look for `SOSVERSION=` to determine the version of the SOS.

To determine the version of the OS Management System Agent that you are running, you can use a text editor to open `SystemDrive:\Program Files\Hewlett-Packard\CM\OSManagerServer\upload\machineID-all.log`. The line will read similar to the following:

```
TKD Version: 7.20 Build ROMA Repository Revision:  
$Revision: 1.106 $ running
```

## OS Manager Boot Loader

The version of OS Manager Boot Loader is displayed during the boot sequence. To find out the version number, you should do a PXE boot and one of the first lines will contain the version number. The version can also be found in `ROMBL_REV=` in the `machineID-all.log`.

## Frequently Asked Questions

- Can I upgrade from my previous version?  
See the *HP Client Automation Enterprise OS Manager Migration Guide*.
- Can I use the Linux SOS for Hardware Configuration Elements if I'm deploying Windows Vista and WinPE?  
Yes. In the Hardware Configuration Element class use the variable `Service OS Needed to Run Method (ELGBLSOS)` and in the Operating System class, use the variable `Service OS List (ELGBLSOS)` to define the Service OS. If the Service OS (SOS) for the Hardware Configuration Element and the Operating System do not match, the target device will reboot into the appropriate SOS as needed. The same applies if you are deploying a sequence of Hardware Configuration Elements, some of which need to use the Linux SOS and some of which need to use the WinPE SOS.
- Can you use varying versions of the OS Manager Server modules?  
Mixing and matching OS Manager Server modules is not supported unless you are directed by HP's Technical Support team to do so.
- Will my data partitions be captured with the system partition during the Image Preparation process?  
Multiple partitions on the source image will cause image deployment failures. Remove all partitions on the source other than the one that you want to capture. It is recommended that the partition contain only 100 MB of free space.
- What should I do if my image was not captured properly?  
Ensure that you prepared your reference machine correctly. See [Preparing and Capturing OS Images](#) on page 59 for details.
- Are dynamic disks supported with OS Manager Server?  
Not yet.
- What if I want to kick off a batch file to execute a backup program before sending a new image to a machine?  
Use the exit point (`Novapdc.cmd`). Rename your batch file (which contains the backup program) to `Novapdc.cmd` and store it on the target device in `SystemDrive:\Program Files\Hewlett-Packard\CM\Agent`. This will run before the new OS is deployed.  
  
Use `novapdr.cmd` to restore your data. For more information see [Addressing Requirements for Capturing, Recovering, and Migrating Data](#) on page 179.

- 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 /a`. If you find `boot.ps` and `tftp`, the installation was successful.

- How do I know if the appropriate port is listening?  
From the command prompt `netstat -a`, you will receive a list of the ports and an indication of whether they are listening.
- What do I do if I receive a message that says “Checking Machine Status Times Out” or “Cannot find ROMS infrastructure?”  
You may receive this message if you are blocking ports or using a

firewall. Be aware that you must be using both UDP and TCP. Verify that your ports are open, in particular ports 3469, 3471 and 2074. Go to the .cfg for each HPCA IS product that you are running and find the value for the port. After you know which port is not working, you can check your firewall to make sure it is not blocking the specified port.

- What do I do if I receive a message similar to the following during image deployment:

```
20061127 13:37:18 Info: *** Installing Standard Image
20061127 13:37:18 Error: InstallNvdm: An error occurred
retrieving Current Partition information, err:

sfdisk: ERROR: sector 0 does not have an msdos signature
20061127 13:37:18 Info: Partitioning Hard Disk 20061127
13:37:18 Info: rpsadr: CASSEVER:3467
20061127 13:37:18 Info: rpshost: CASSEVER
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://CASSEVER: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 administrator.
20061127 13:37:18 Info: *** Start of Update Machine
=====*** Start of Update Machine
=====
```

Check the configuration of your DNS server. Depending on the configuration, you may experience difficulties working with the short name and may need to use the IP address or fully qualified name.

## Using the Discover Boot Server Utility

Use the following command to send out a DHCP discover request in order to identify the PXE servers that are in the environment. This is an essential command when trying to determine if a machine is able to access the PXE server.

```
./discoverbootserver.sh
```

Note that the results may be complicated to read. Contact Technical Support for more information.



# A AppEvents

The following AppEvents are stored in the Events section in the ROM object.

**Table 16 AppEvents**

<b>Message</b>	<b>Description</b>
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 <code>unattend.txt</code> file could not be retrieved from the server.
Sysprep.inf error	The <code>sysprep.inf</code> file could not be retrieved from the server.
OS install Successful	OS was successfully installed.
NOOP install Successful	No OS install was required. Hardware Configuration Elements may have been processed and the OS Manager may have been updated to indicate that the machine is in desired state with respect to the OS currently installed OS.

<b>Message</b>	<b>Description</b>
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 ( <code>_INCONSISTENT_OS</code> ). The device is unusable and the OS Manager does not know how to proceed. Therefore, the device has been turned off until the administrator changes policy and sends a WOL to the machine.
Admin activity required - Multiple OSs resolved and central control	Multiple OSs were resolved for this device and administrative action is required because the user was not given the option to select the OS.
Admin activity required - Multiple OSs resolved and central control	During policy resolution, several eligible OSs were found for the device. However, the behavior setting does not allow for user selection of the OS. Therefore, the administrator must intervene and determine what OS should be installed on the device. Until then, the device is usable as long as the OSSTATE is not set to INVALID.

<b>Message</b>	<b>Description</b>
Admin activity required - No OS has been selected	<p>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 (<code>_INCONSISTENT_OS</code>).</p> <p>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.</p>
Admin activity required - OSSTATE set to <code>_INCONSISTENT_</code>	<p>On a managed device that was in its desired state, <code>Rombl.cfg</code> was lost. This may indicate serious corruption and therefore, the OS Manager changed the value of OS State to <code>_INCONSISTENT_</code> and will allow the device to be used "as is".</p> <p>If possible, during the next HPCA OS Connect, <code>Rombl.cfg</code> will be recreated. If this does not happen, the administrator should force a reinstall of the OS.</p>
Admin activity required - <code>_UNMANAGED_OS_</code> is resolved through general policy criteria	An <code>_UNMANAGED_OS_</code> 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.
<code>%1\$s %2\$s</code> has been selected	<p><code>%1</code> = "OS" or "Hardware Configuration"</p> <p><code>%2</code> = The name of the OS or LDS</p> <p>Indicates what has been selected based on policy.</p>
<code>%1\$s %2\$s</code> already installed	<p><code>%1</code> = "OS"</p> <p><code>%2</code> = "OS name"</p> <p>The OS referenced has previously been installed.</p>

<b>Message</b>	<b>Description</b>
%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.
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.

<b>Message</b>	<b>Description</b>
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.
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 17 Messages for Timeouts**

Messages	User Action
This machine is installed with a factory pre-imaged OS that is managed by the Client Automation OS Manager. The Client Automation OS Manager System Agent is unable to connect to the Client Automation OS Manager infrastructure to configure this machine. The machine cannot be used. The system will retry later.	N/A
The local machine does not contain a usable OS. Networking problems prevented the Client Automation OS Manager System Agent from connecting to the Client Automation OS Manager infrastructure to install this machine. The machine cannot be used. The system will retry later.	N/A
The local machine contains a usable OS. Networking problems prevented the Client Automation OS Manager System Agent from connecting to the Client Automation OS Manager infrastructure to determine policy for this machine. The machine will be booted to the local Operating System.	N/A
This machine has an OS installed but is not currently managed by the OS Manager. It contains a local partition but no management marker and no machine object. Select <b>install</b> to install an operating system according to policy or <b>use</b> to keep the existing operating system for now. Please select <b>install</b> or <b>use</b> .	Select <b>install</b> to install the resolved OS, or select <b>use</b> to continue to use the existing OS.

<b>Messages</b>	<b>User Action</b>
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.
<p>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:</p> <p>ACPI:                               \$::acpi  APIC:                                 \$::apic  Minimum CPU speed:               \$::cpuspeed  Minimum RAM size:                 \$::mem  Boot Hard Drive Type:             \$::boottype  Minimum Hard Drive Size:         \$::hdsiz</p> <p>The machine cannot be used and will shut down until an administrator specifies policy and performs a Wake On LAN.</p>	N/A
The current state of this machine is unusable. Policy returned multiple OSs for this machine. The machine will shut down until an administrator selects an eligible OS and performs a Wake On LAN.	N/A
The current state of this machine is unusable. Policy returned multiple Hardware Configurations for this machine. The machine will shut down until an administrator selects an eligible Hardware Configuration and performs a Wake On LAN.	N/A
Policy requires that the OS must be reinstalled on this machine. Select an OS from the following list:	Select an OS.
Policy requires that the Hardware Configuration must be reinstalled on this machine. Select a Hardware Configuration from the following list:	Select a Hardware Configuration.



<b>Messages</b>	<b>User Action</b>
<p>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.</p>	<p>N/A</p>
<p>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.</p>	<p>N/A</p>
<p>Policy requires that the OS for this machine must be reinstalled. Is it ok to install the new OS now?</p>	<p>Indicate whether it is okay to continue the installation.</p>
<p>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?</p>	<p>Specify whether to use the existing installation or to refresh the current OS.</p>
<p>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.</p>	<p>N/A</p>
<p>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.</p>	<p>N/A</p>
<p>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.</p>	<p>N/A</p>



## C Storing Multiple Logs

Typically, after an OS is installed, the logs stored on the OS Manager Server are rewritten each time. Now, you have the option to store multiple logs per machine on the OS Manager Server.

To store multiple logs on the OS Manager Server

- 1 Use a text editor to open `SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\etc\put.cfg`.

```
# -----  
# - RIS Put Server - for file uploads  
#  
# Put::cfg array is used by the PutEnter proc to allow a user-specified  
# number of previous files with the identical name to be saved.  
# -ROLLOVER is the max number of files to keep, each file has the  
# same root name with the suffix of .1, .2, etc.  
# -TYPELIST may include any number file extensions: e.g., ".log .txt .edm"  
# The default of -ROLLOVER is 0 (zero) and only the current version is stored.  
# -----  
  
file mkdir [set dir $Config(ROOT)/upload]  
  
Put_AddRoot /upload $dir  
  
namespace eval Put {  
    array set cfg [list \  
        -ROLLOVER 0 \  
        -TYPELIST ".log"  
    ]  
}
```

- 2 Set `-ROLLOVER` to the number of logs that you want to be able to store. For example, if you set `-ROLLOVER` to 3, you will be able to store and review the previous three actions performed on the target device.



# Index

## A

ACKTMOUT, 127

actual throughput, definition, 151

Add partition, 129

adding a partition, 133

address parameter, 149

Admin Publisher, using, 107

Advanced Programmable Interrupt Controller, 34

agent receiver, definition, 151

agent, definition, 151

APIC. See Advanced Programmable Interrupt Controller

APIC device, 87

assigning

- drive layouts, 134
- operating systems, 128
- policy, 117

Assignment type group box, 109

AutoLogon, 71

AutoLogonCount, 71

AUTOROLE, 127

## B

bandwidth throttle, 127

BANDWIDTH, 127

bare metal machine, 138

- definition, 27

behaviors

- setting, 123

Behaviors, 123

BIOS power management, 63, 65, 67, 68, 75, 77

BitLocker, 56

boot menu

- change configuration, 184
- configure, 188

Boot Server, 21

- installing, 45, 47
- ISVR, 46
- system requirements, 46

-bt option, 170

Build Mass Storage Section in Sysprep.inf check box, 86

build.config file, 190

- customizing, 191

build\_scripts.zip, 184

building a custom WinPE Service OS, 183

## C

Cache partition, 130

CD/DVD boot, 55

Check Point PointSec Full Disk Encryption, 54

Client Automation Configuration Server Database

- version requirement, 39

Client Automation Proxy Server, 25

Configuration Server, 40, 204

- bin directory, 38
- version information, 38
- version requirement, 38

Configuration Server Database, 204

Configuration Server DB, 23

configuring Proxy Server, 50

Connect.log, 200

Core, 19

Core, 38

- Core, 41
- Core, 45
- Core, 198
- Core servers, 38
- creating a manufacturer or model instance, 128
- CSDB Editor
  - logging on, 122
- customer support, 10
- CWINDOW parameter, 150
- cygwin, 46, 185
- D**
- damaged
  - master boot record, 125
- DBVER attribute, 39
- default Service OS
  - change, 184
- device object
  - definition, 28
- DHCP broadcast, 46
- DHCP Server, 21
- disaster recovery, 54, 138
- Discover Boot Server utility, 46, 208
- discovery, definition, 28, 114
- Disk Encryption, 53
- DISPLAYNAME, 48
- dl option, 166
- document changes, 4
- dp option, 166
- dp1 option, 166
- drive layouts
  - assigning, 134
  - defining, 129
  - specifying, 129
- Drive Layouts, 123
  - Class, 121

- DRIVEMAP, 123
- driver list, 189

## E

- edmprof file, 42
  - excerpt, 48
  - OS Manager settings, 48
  - updating, 48
- ENCMODE, 53, 55
- Encryption, 53
- Encryption Support Mode parameter, 53, 55
- exit points, 80, 81, 180, 205
  - for Image Preparation Wizard, 80, 81
- expandsmbios.tkd, 204
- ExtendOemPartition parameter, 63, 71, 79
- Extra Command Line Parameters text box, 73

## F

- f option, 166
- Force OS Install task, 120
- FORMAT attribute, 133

## G

- gddelaybp parameter, 152, 158, 160, 166
- gdmcrecv command, 170
  - options, 170
- gdmcsend command, 165, 170
  - options, 166
- gdmcsend.log, 159
- gdmrecv command, 165
- gdmrecv.sh, 170, 173
- gdmsend.cmd, 173
- gold image
  - definition, 28
- GuiUnattended, 70

## H

- HAL, 34, See Hardware Abstraction Layer
- Hardware Abstraction Layer, 34
- hibernation, 64
- HP Client Automation Administrator
  - version requirement, 39
- HP Client Automation Administrator Publisher, 20
- HP Client Automation agent
  - definition, 27
- HP Client Automation Application Manager, 24
- HP Client Automation Configuration Server, 21, 24
- HP Client Automation Configuration Server Database, 24
- HP Client Automation Enterprise Manager
  - version requirement, 39
- HP Client Automation Integration Server, 41
- HP Client Automation Mini Management Server, 25
- HP Client Automation OS connect
  - definition, 27
- HP Client Automation OS Manager Boot Loader, 24
- HP Client Automation OS Manager Image Preparation Wizard, 20
- HP Client Automation OS Manager Server, 24
- HP Client Automation OS Manager Server Requirements, 32
- HP Client Automation OS Manager System Agent, 24
- HP Client Automation Portal
  - version requirement, 39
- HP Client Automation Proxy Server
  - version requirement, 39
- HP Client Automation Windows Native Install Packager
  - creating images, 20
- HP CSDB Editor, 25
- HPCA Client Operations Profiles, 142
- HPCA Core, 19, 38, 41, 45, 198
- HPCA OS Manager Image Preparation Wizard, 80, 83
  - using, 83
- HPCA Satellite, 19, 38, 41, 45, 198
- HPCA Windows Native Install Packager
  - Extra Command Line Parameters, 73
  - Image Description text box, 74
  - Image Name text box, 74
  - installing, 71
  - Optimize Compression check box, 74
  - OS Manager Port text box, 74
  - ROM Server text box, 74
  - Target drive drop-down list, 73
  - using, 72
  - Windows Setup window, 73
- httpd-3469.error.txt, 198
- httpd-port.log, 41, 198, 204
- httpd-port.YY.MM.DD.log, 198
- HW Config, 123
- HW Config Element, 123

## I

- i386 Directory text box, 73
- Image Description text box, 74
- Image Name text box, 74
- Image Preparation Architecture, 19
- Image Preparation Wizard, 93, 97, 100
  - exit points, 80, 81
  - logs, 199
  - unattended, 7, 88
  - using, 93, 97, 100
- image, definition, 151
- ImageDeploy.ISO, 25
- IMAGEDESC, 89
- IMAGENAME, 89
- ImageName.EDM, 81, 93, 96, 99
- ImageName.IMG, 81
- ImageName.MBR, 81
- ImageName.PAR, 81

- images
  - deploying, 20
- ImageX, 43, 64, 66, 67
- infrastructure test, 201
- installing
  - Boot Server, 47
  - HPCA Windows Native Install Packager, 71
- Integration Server, 21
- internet protocol addressing structure \, 38
- inter-packet delay, 158, 160
- IP Networking Support, 38
- IP version 4, 38
- IP version 6, 38
- IPv4, 38
- IPv6, 38

## J

- JoinDomain parameter, 79

## K

- KBDMAP, 127
- keyboard mappings, 127

## L

- LANG, 127
- last packet resend, 167
- last packet resend delay, 167
- lc option, 166
- LDS, 123
- lf option, 167, 171
- license file, 41
  - checking validity, 41
  - location, 41
- Limit package to systems with section, 109
- lingercount parameter, 152, 158, 166
- lingerdelay parameter, 152, 158, 166
- Linux Service OS. *See* Service OS

- LME, 123
- Local Service Boot, 25
  - alternative to PXE, 141
  - best practices, 142
  - prerequisites, 141
- log\_file, 170
- logging on to CSDB Editor, 122
- logs
  - Connect.log, 200
  - httpd-3469.error.txt, 198
  - httpd-port.log, 198, 204
  - httpd-port.YY.MM.DD.log, 198
  - LSB.log, 200
  - machineID-all.log, 198
  - osclone.log, 199
  - OSSELECT.log, 203
  - romclimth.log, 180
  - Romclimth.log, 200
  - setup.log, 199
- lpr option, 167
- lprcount parameter, 153, 157, 162, 167
- lprd option, 167
- lprdelay parameter, 153, 157, 167
- LSB, 25
- LSB, 143
- LSB.log, 200

## M

- ma option, 167, 171
- machineID-all.log, 198
- managed device
  - definition, 28
- MANUFACT Class, 116
- manufacturer or model instance, creating, 128
- Mass Storage Drivers, 86
  - list, 86
- maxresendreq parameter, 164
- maxrsndreq parameter, 153, 171



- McAfee Safeboot, 54
- mcast.cfg file, 149, 166, 170
  - address parameter, 149
  - CWINDOW parameter, 150
  - Minref parameter, 149
  - root parameter, 149
- mcastretrycount parameter, 149, 158
- mcastretrywait parameter, 149
- menu
  - operating systems, 118
- Merge partition, 130
- messages, timeout, 215
- Microsoft Sysprep, 64, 65
- Minref parameter, 149
- MODEL Class, 116
- mp option, 167, 171
- mr option, 171
- multicast, 148
  - configuring, 149
  - parameters, 152
  - receive command, 170
  - send command, 165
- Multicast Server, 148
- multicast transfer, definition, 151
- multicast.rc file, 150
- multicastIPAddress parameter, 149
- multiple logs, 219

## N

- na option, 171
- nac\_port option, 167
- nacdelay parameter, 153, 171
- NACK. See negative acknowledgement
- NACK port, 167
- nackdelay parameter, 157
- nackresend parameter, 157, 164
- nacresend parameter, 153, 172
- nano editor, 170
- native installation, definition, 28
- nd option, 171
- negative acknowledgment, definition, 152
- netinact parameter, 153, 161, 172
- netinfo.ini, 178, 185
- network boot, 55
- networking boot, 139
- ni option, 167, 171
- NIC card
  - PXE-compliant, 47
- nit option, 172
- Novapdc.cmd, 179, 205
- Novapdr.cmd, 179
- np option, 172
- npb option, 168, 172
- nr option, 168, 172
- NULL instance, 123
- numpktblks parameter, 153, 156, 158, 163, 172
- nvdkit.exe, 204
  - version information, 204

## O

- offset option, 168
- operating system menu, 118
- operating systems
  - assigning, 128
  - assigning, 128
- Operating Systems, 123
- Optimize compression of unused disk space check box, 74, 86
- Optional Packager Command Line Arguments, 72
- OS Domain
  - Behavior Class, 123
  - Drive Layouts Class, 123
  - HW Config Class, 123
  - HW Config Element Class, 123

- Operating Systems Class, 123
- Partition Table Spec Class, 123
- Sysprep Files Class, 123
- OS Manager
  - Boot Loader, 40
    - version information, 204
  - IP address, 46
  - port, 46
  - Port text box, 74
  - System Agent, 40
  - version information, 203
- OS Manager Admin Module
  - version information, 203
- OS Manager classes, accessing, 122
- OS Manager Server, 21
  - logs, 198
  - text box, 74

- OS state
  - definition, 28

osclone.log, 199

OSEDITION, 90

- OSM System Agent
  - logs, 204

OSSELECT.log, 203

Override Sysprep File, 134

## P

Package Information section, 109

packet blocks, 158

packet loss, definition, 151

packet resend, 167

packet, definition, 151

packets per block, 168

PARINFO attribute, 133

PARTITION Class, 133

Partition Table Spec, 123

- partitions
  - adding, 133

- extending, 64

PARTTION, 123

PARTYPE attribute, 133

Payload, 204

peimg command, 189

Perform client connect after OS install check box, 86, 94, 101

performance, definition, 151

PGP Whole Disk Encryption, 54

PIC. *See* Programmable Interrupt Controller

pktsperblk, 172

pktsperblk parameter, 154, 156

Platform Support, 32

PMACKOVW, 125

PMDISRCV, 125

PMDISRCV attribute, 115

-pmf option, 172

PMINITL, 125

PMROLE, 124

PMSLCTOS attribute, 121

policy assignments, 117

POLICY Domain

- MANUFACT Class, 116

- MODEL Class, 116

- ROLE Class, 116

- SUBNET Class, 116

Portal

- Zone name restrictions, 42

PORTAL\_HOST, 48

PORTAL\_PASS, 48

PORTAL\_PORT, 48

PORTAL\_UID, 48

PORTAL\_ZONE, 48

-ppb option, 172

-ppb option, 168

pre-execution environment. *See* PXE

- prepwiz.exe, 83, 94, 97
- prepwiz\_unattend, 89
- PREPWIZPAYLOAD, 89
- Product Architecture, 19
- Programmable Interrupt Controller, 34
- Proxy Server, 41, 50
  - co-locating, 50
  - configuring, 50
- Publisher, 23
- put.cfg, 219
- PXE, 25, 139
  - boot, 47
  - Client, 46
  - packets, 46
  - server, 46
- PXE boot, 33, 55
- PXE environment
  - best practices, 138
- PXE/TFTP servers, 21, 23
- PXE-compliant NIC card, 47

## R

- radskman command line, 126
- raw data transfer rate, definition, 151
- receiver, definition, 151
- recvtimeout parameter, 154, 161, 173
- reference machine
  - definition, 28
  - preparing, 69
- reliability, definition, 152
- remote images, 82
  - capture, 82
- Replace partition, 130
- resend block, definition, 152
- resend mode, 168
- resend request, definition, 152
- resend requests, 158

- Resize partition before OS upload check box, 86
- RISHOSTPORT, 89
- rm option, 173
- rm option, 168
- ROLE Class, 116
- roles
  - selecting, 124
- ROLLOVER parameter, 219
- ROM object, 43, 114, 144
  - definition, 28
- ROMA Parameters field, 149
- ROMAPARAM, 126
- ROMBL.CFG, 25
- rombl\_capture.cfg, 185
- rombl\_deploy.cfg, 185
- romclimth.log, 180
- Romclimth.log, 200
- romclimth.tkd, 179
- roms.tkd, 204
- roms\_udp.tkd, 204
- romsinfo.ini, 177
- root parameter, 149
- rps.cfg, 50
- RunOnce parameter string, 49
- RUNPARAM, 126

## S

- Satellite, 19, 38, 41, 45, 198
- Satellite servers, 38
- Select window, 107
- selecting roles, 124
- sender, definition, 152
- server requirements, 32
- Server Requirements, 32
- server, definition, 152

- Service Multicast Eligible option, 148
- Service Operating System, 24
- Service Operating System (Service OS)
  - definition, 28
- Service OS, 25, 52
  - default, 188
- setting behaviors, 123
- setting policy, 117
- setup.cfg, 89
- setup.log, 199
- Setupmgr.exe, 79
- SIM. *See* System Image Manager
- SIZE attribute, 133
- SMBIOS, 43
- SOS, 25, 204, *See* Service Operating System
- SSL, 5, 6, 19, 44
- static-root parameter, 50
- static-type parameter, 50
- stderr option, 173
- SUBNET Class, 116
- support, 10
- supported language, 127
- Symantec Endpoint Protection Agent, 34
- SYSPREP, 123
- SYSPREP Class, 71, 109
- Sysprep File
  - Override, 134
- Sysprep Files, 123
- Sysprep.inf file
  - creating, 79
  - prioritizing, 80
- SysprepMassStorage section, 86
- system behavior changes
  - using disk encryption support, 54
- System Image Manager, 23

- system requirements
  - Boot Server, 46
  - target devices, 32
- System Requirements, 31

## T

- t option, 173
- target device
  - definition, 28
  - properties, 114
  - requirements, 32
  - using VMware, 33
- Target Device Requirements, 32
- Target Devices, 19
- Target drive drop-down list, 73
- technical support, 10
  - collecting information, 202
- TESTMODE flag, 126
- tf option, 169
- TFTP. *See* Trivial File Transfer Protocol
- TFTP server, 141
- thin client
  - target device requirements, 33
- Thin client
  - prepare and capture images, 92
- throtfreq parameter, 154, 159, 169
- throthighth parameter, 154, 158, 169
- throtincr parameter, 154, 159, 169
- throtlowth parameter, 154, 158, 169
- throtmax parameter, 155, 159, 169
- throtmin parameter, 155, 159, 169
- throttle threshold, 158
- ti option, 169
- timeout messages, 215
- TimeZone parameter, 79
- tmax option, 169
- tmin option, 169

Trivial File Transfer Protocol, 45

Trusted sites, 43

-tthigh option, 169

-ttl option, 169

ttl parameter, 155, 169

-ttlow option, 169

Type of Data to Publish drop-down list, 135

## U

UDP protocols, 46

unattend.txt file

- description, 70

- recommended size, 70

- text box, 73

unattended mode

- Image Preparation Wizard, 7, 88

UnattendMode parameter, 79

unicast, 160

UNITS attribute, 133

unmanaged OS

- definition, 29

UNMANAGED\_OS service, 145

user messages, 215

user prompt

- for overwriting or modifying OS, 125

using Microsoft Sysprep, 78

## V

version and build, 198

version.nvd, 38

## W

WIM file, 23

Windows Automated Installation Kit (WAIK), 184

WinMagic SecureDoc, 54

WinPE Service OS

- add drivers or packages, 184

- update, 184

winpe.wim

- using a pre-existing file, 186, 187

## Z

ZSERVICE, 123

