

# HP Client Automation Starter and Standard

for the Windows® operating system

Software Version: 7.20

---

## Administrator Guide

Manufacturing Part Number: None

Document Release Date: April 2009

Software Release Date: July 2008



## Legal Notices

### Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

### Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### Copyright Notices

© Copyright 2006-2009 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

### 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.

### Acknowledgements

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.

The table below lists new features added for this release.

**Table 1 New features added for HP Client Automation 7.20**

Chapter	Version	Changes
All	7.20	Client Configuration Manager (CCM) was rebranded to HP Client Automation Starter and Standard (HPCAS). <ul style="list-style-type: none"><li>• CCM Basic is now HP Client Automation Starter.</li><li>• CCM Premium is now HP Client Automation Standard</li></ul>
2	7.20	Page 34, <a href="#">VMware Requirements</a> : Added requirements for installing HPCAS in a VMware environment.
4	7.20	Page 64, <a href="#">Device Details</a> : Properties tab now contains an Advanced Properties section.
4	7.20	Page 64, <a href="#">Device Details</a> : Last logged on user was added to Device Details window.

4	7.20	Page 85, <a href="#">Software Details</a> : Properties tab. New Pre-Uninstall Command Line text box added.
4	7.20	Page 74, <a href="#">Group Details</a> : Properties tab now displays criteria used to create dynamic reporting groups.
4	7.20	Page 56, <a href="#">Device Management</a> : Remote Control interface updated. This no longer uses a wizard, but now opens directly in the remote interface.
4	7.20 April 2009	Page 116, <a href="#">Job Status</a> : Added Hibernation information.
5	7.20	Page 129, <a href="#">Inventory Management Reports</a> : Included information for creating S.M.A.R.T alert reports.
5	7.20	Page 129, <a href="#">Inventory Management Reports</a> : New Blade server reports are now included.
6	7.20	Page 145, <a href="#">Synchronizing Infrastructure Servers</a> : Added information for new synchronize feature which allows the synchronization of the service cache on selected Infrastructure Servers with the HPCAS Server.
6	7.20	Page 149, <a href="#">Locations</a> : Infrastructure Locations added. These are used to assign Infrastructure Servers to specific subnets.
6	7.20	Page 157, <a href="#">Configuring S.M.A.R.T</a> : S.M.A.R.T. monitoring and reporting configuration added.
7	7.20	Page 167, <a href="#">Wizards</a> : Unnecessary steps were removed from most wizards.
7	7.20	Page 174, <a href="#">Group Creation Wizard</a> : Group creation wizards were modified to allow for a Display Name and Description to be added.
7	7.20	Page 169, <a href="#">Agent Deployment Wizard</a> : The Agent Deployment wizard now includes a Silent Mode option.
11	7.20	Updated list of supported applications.



## 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 a support contract.

To find more information about access levels, go to:

**[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:

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

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>20</b>
	Audience .....	20
	Summary .....	20
	Overview .....	22
	HP Client Automation Starter Features .....	23
	HP Client Automation Standard Features .....	24
	The HPCAS Console .....	25
	Management Agent .....	27
	HP Client Automation Administrator Publisher .....	28
	The Image Preparation Wizard .....	28
	The Settings Migration Manager .....	29
	Getting Help .....	29
<b>2</b>	<b>Installing HPCAS .....</b>	<b>31</b>
	System Requirements .....	31
	Platform Support .....	31
	Web Browsers .....	31
	Server .....	31
	Database .....	32
	Target Devices .....	32
	Firewall Settings .....	32
	Target Devices .....	32
	HPCAS Server .....	33
	SQL Server .....	33
	Infrastructure Servers .....	33
	Sygate Firewall Settings .....	34
	VMware Requirements .....	34
	Installing HPCAS .....	35
	Manually Installing the Management Agent .....	41
	Installing the Management Agent on Thin Clients .....	41



Linux-based Thin Clients.....	41
Windows XPe .....	43
Windows CE.....	44
Removing HPCAS.....	44
Configuring PXE for OS Deployment.....	44
<b>3 Getting Started.....</b>	<b>47</b>
Logging In .....	47
Quick Start Tasks.....	47
<b>4 Management .....</b>	<b>55</b>
Device Management .....	56
General .....	56
Devices .....	57
Importing Devices.....	59
Deploying the Management Agent from the Devices Tab .....	60
Removing the Management Agent .....	60
Discovering Software/Hardware Inventory .....	61
Discovering Patch Compliance .....	61
Discovering Application Usage .....	61
Remote Control .....	62
Power Management.....	63
Removing Devices .....	63
Device Details .....	64
Current Jobs .....	65
Past Jobs .....	66
Group Management.....	67
General .....	67
Group Types .....	68
Groups.....	68
Creating a Group .....	70
Deploying the Management Agent to a Group .....	71
Removing the Management Agent from a Group.....	71
Discovering Software/Hardware Inventory for a Group .....	72
Discovering Patch Compliance a Group.....	72
Discovering Application Usage Data a Group .....	73
Power Management.....	73
Removing Groups .....	73

Group Details .....	74
Group Details Window Tasks .....	76
Adding and Removing Devices from Static Groups.....	77
Adding and Removing Software Entitlement from Groups.....	77
Deploying, Removing, and Synchronizing Software from Groups .....	78
Adding and Removing Patch Entitlement from Groups .....	78
Deploying Patches to Groups.....	79
Current Jobs .....	79
Past Jobs.....	80
Software Management .....	81
General .....	81
Software .....	82
Deploying Software.....	83
Adding Group Entitlement .....	84
Importing a Service .....	84
Exporting a Service .....	85
Removing Software from HPCAS.....	85
Software Details .....	85
Current Jobs .....	89
Past Jobs.....	89
Patch Management.....	91
General .....	93
Patches.....	94
Deploying Patches .....	94
Adding Group Entitlement .....	95
Importing a Service .....	95
Exporting a Service .....	96
Patch Details.....	96
Current Jobs .....	99
Past Jobs.....	99
OS Management .....	101
General .....	101
Operating Systems.....	102
Deploying Operating Systems .....	103
Deploying an OS Image using Local Service Boot (LSB).....	107
Deploying an OS Image using PXE.....	108
Deploying an OS Image using the Service CD .....	109
Adding Group Entitlement .....	110
Importing a Service .....	110
Exporting a Service .....	111

Removing Operating Systems from the Library.....	111
OS Details .....	111
Current Jobs .....	113
Past Jobs.....	114
Job Management.....	115
General .....	115
Current Jobs .....	115
Job Controls .....	115
Job Status.....	116
Job Details.....	118
Past Jobs .....	119
<b>5 Reporting .....</b>	<b>121</b>
Search Options.....	122
Display Options .....	122
Search Criteria.....	123
Report Windows.....	123
Using Search Options to Select Filters .....	124
The Directory/Group Filters Area .....	124
The Data Filters Area .....	125
Using Display Options to Select Reporting Views .....	127
Reporting View Types .....	128
Inventory Management Reports.....	129
Patch Management Reports.....	130
Usage Manager Reports.....	130
Viewing HP Hardware Reports.....	131
About Reporting Windows .....	132
Using the Windows Action Bar .....	133
Applying Filters from Report Data.....	135
Creating Dynamic Reporting Groups .....	136
<b>6 Configuration.....</b>	<b>137</b>
Support.....	137
Downloading Log Files.....	138

Updating Licensing Information.....	139
Console Access .....	139
Creating additional console users .....	140
Removing console users .....	140
Viewing and Modifying Console User Details.....	141
Changing the Console Password .....	141
Infrastructure Management .....	142
Servers .....	142
Managing Infrastructure Servers.....	143
Deploying the Infrastructure Service.....	144
Synchronizing Infrastructure Servers .....	145
Server Details Window.....	147
Locations.....	149
Location Details .....	151
Patch Management – Configuration.....	151
Configuring Patch Acquisition Schedule .....	152
Configuring Patch Acquisition Settings .....	153
OS Management .....	155
Hardware Management .....	156
Configuring CMI .....	156
Configuring S.M.A.R.T. ....	157
Configuring TPM.....	158
Reporting.....	159
Database .....	160
Usage Settings.....	160
Usage Collection.....	161
Configuring Usage Collection Filters .....	163
Defining Usage Criteria .....	164
Maintenance .....	166

## 7 Wizards..... 167

Import Device Wizard.....	168
Agent Deployment Wizard .....	169
Agent Removal Wizard.....	170
Software/Hardware Inventory Wizard.....	171

Patch Compliance Discovery Wizard.....	171
Application Usage Collection Wizard.....	172
Power Management Wizard.....	173
Group Creation Wizard .....	174
Software Deployment Wizard .....	177
Service Import Wizard .....	178
Service Export Wizard.....	178
Software Synchronization Wizard .....	179
Patch Deployment Wizard .....	180
Service Entitlement Wizard.....	181
Software Removal Wizard.....	182
User Creation Wizard.....	182
OS Deployment Wizard .....	183
Usage Collection Filter Creation Wizard .....	185
Infrastructure Deployment Wizard.....	185
Infrastructure Removal Wizard.....	186
Infrastructure Location Creation Wizard .....	186

## 8 Preparing and Capturing OS Images ..... 189

Windows OS Images.....	189
Task 1 - Prepare the Reference Machine.....	189
Task 2 - Create Answer Files .....	192
Prepare unattend.xml (for Windows Vista deployments).....	192
Create Sysprep.inf (for non-Vista OSs only).....	192
Task 3 - Run the Image Preparation Wizard .....	194
Thin Client OS Images .....	199
Windows XPe OS images.....	199
Task 1 – Prepare the XPe Reference Machine.....	199
Task 2 – Run the Image Preparation Wizard.....	200
Windows CE OS images .....	203
Task 1 – Prepare the CE Reference Machine .....	203
Task 2 – Run the Image Preparation Wizard.....	203
Embedded Linux OS images .....	206

Task 1 – Prepare the Embedded Linux Reference Machine.....	206
Task 2 – Run the Image Preparation Wizard.....	207
Publishing and Deploying OS images .....	210

## 9 Using the Publisher ..... 213

Publishing Software .....	214
Publishing Windows Installer Files.....	214
Publishing Using Component Select.....	216
Publishing Operating System Images.....	218
Prerequisites for publishing .WIM images of a Vista OS.....	219
About the .subs and .xml files.....	219
Example of Substitution.....	220
Preparing filename.xml.....	222
Publishing OS Images.....	222
Publishing HP Softpaqs .....	223
Publishing BIOS Settings .....	225
Creating a BIOS Settings File .....	227
Viewing Published Services .....	228
HP Client Automation Administrator Agent Explorer .....	229

## 10 Using the Application Self-service Manager ..... 231

Accessing the Application Self-service Manager .....	231
Application Self-service Manager Overview .....	232
Global Toolbar .....	233
The Menu Bar.....	233
Catalog List .....	234
Service List .....	234
Using the Application Self-service Manager User Interface .....	235
Installing Software.....	236
Refreshing the Catalog .....	236
Viewing Information .....	236
Removing Software .....	237
Viewing History.....	238
Adjusting Bandwidth.....	238

Viewing Status .....	239
Customizing the User Interface.....	240
General Options .....	240
Service List Options.....	242
Connection Options.....	244
HPCA System Tray Icon .....	246
HPCA Status window .....	246

## 11 Settings Migration ..... 249

Supported Applications and Settings.....	250
Microsoft Office Supported Applications .....	250
Other Supported Applications.....	250
Windows Options .....	251
Control Panel (Settings) .....	251
Microsoft Office Support Notes .....	252
Microsoft Office.....	252
Microsoft Access.....	254
Microsoft Excel.....	255
Microsoft FrontPage .....	256
Microsoft Groove.....	256
Microsoft InfoPath.....	257
Office Assistant Settings.....	257
Office Shortcut Bar.....	257
Microsoft OneNote.....	257
Microsoft Outlook .....	258
Microsoft PowerPoint .....	259
Microsoft Project.....	260
Microsoft Publisher .....	261
Microsoft Word.....	262
Other Supported Application and Operating System Notes .....	263
Adobe Acrobat.....	263
CuteFTP Pro .....	264
FileZilla .....	264
AOL Instant Messenger .....	264
MSN Messenger.....	265
Yahoo Messenger.....	265
Lotus Notes .....	265
Microsoft Internet Explorer .....	266
Microsoft NetMeeting.....	266

Microsoft Outlook Express .....	267
Mozilla Firefox .....	267
Norton AntiVirus Corporate Edition .....	267
Visio .....	268
WinZip .....	268
WS_FTP Pro .....	269
Data Transport .....	269
Windows Options .....	269
Desktop Shortcuts .....	270
Dial-Up Networking .....	270
Folder Options .....	270
Local Printer Logging .....	270
Mapped Network Drives .....	270
Network and Shared Printer Connections .....	271
Taskbar and Quick Launch Bar .....	271
User Documents and Media Files .....	271
My Documents .....	271
My Music .....	271
My Pictures .....	271
My Videos .....	271
Windows Address Book .....	272
Control Panel .....	272
Accessibility Options .....	272
Display .....	272
Internet Options .....	272
Keyboard .....	272
Mouse Settings .....	273
Power Management .....	273
Regional Settings .....	273
Sounds .....	273
Time Zones .....	273
Creating the Configuration Template .....	273
Using the Settings Migration Utility .....	275
Backing Up Settings .....	275
Stored Settings and Files .....	277
Restoring Settings .....	277
Migrating Settings during OS Deployment .....	279
File Rules .....	279
Accessing File Rules .....	280
File Rules Dialog Box .....	281



12FAQs .....	285
How do I access the HPCAS console? .....	286
How do I determine what version I am using? .....	286
How do I change my console password? .....	286
How do I begin to manage a device in my environment? .....	287
How do I schedule inventory collection? .....	287
How do I view inventory information for managed devices? .....	288
How do I automate patch acquisition? .....	288
How do I configure the patch compliance discovery schedule? .....	289
How do I deploy software to all of my managed devices? .....	289
How do I acquire a particular Microsoft patch? .....	290
How do I update my license key? .....	290
How do I create a group of devices to target for an OS Service Pack? .....	290
How do I deploy software to a single device? .....	291
How do I install the Management Agent without using the console? .....	291
How do I publish a Windows Installer package? .....	292
How do I publish setup.exe? .....	292
How do I know that all my devices received the software? .....	292
How do I make software available for a user to install? .....	293
How do I generate a device compliance report? .....	293
How do I capture an OS image? .....	293
How do I add additional drivers to an OS image? .....	294
How do I publish an OS image? .....	294
How do I deploy an OS image? .....	294
How do I start collecting usage data? .....	295
How do I contact support? .....	295
13Troubleshooting .....	297
Log Files .....	297

Agent Deployment Issues.....	298
OS Deployment Issues.....	299
Application Self-service Manager Issues .....	300
Power Management Issues .....	300
Patch Management Issues .....	301
<b>A About Double-Byte Character Support .....</b>	<b>303</b>
Supported languages .....	303
Changing the locale .....	303
Double-byte support for Sysprep files.....	304
<b>Index .....</b>	<b>305</b>



# 1 Introduction

HP Client Automation Starter and Standard (HPCAS) is a PC software configuration management solution that provides software and HP hardware management features, including OS image deployment, patch management, remote control, HP hardware driver and BIOS updates, software distribution and usage metering all from an integrated web-based console.

This guide introduces HPCAS, shows you how to setup and install the product components, and provides detailed information and instructions for using the HPCAS console, Publisher, Application Self-service Manager and the Image Preparation Wizard.

See [Overview](#) on page 22 for an overview of HPCAS features and components.

## Audience

This guide is intended for administrators who will be installing, configuring, and using HP Client Automation Starter and Standard.

## Summary

### [Chapter 1, Introduction](#)

This chapter contains an overview of HPCAS and its available features and components.

### [Chapter 2, Installing](#)

This chapter provides detailed steps for installing and configuring HPCAS and its components.

### [Chapter 3, Getting Started](#)

This chapter provides quick start instructions for HPCAS, including where to start, what to do first, and how to begin using the HPCAS console.

## Chapter 4, Management

This chapter provides a closer look at the Management tab and each of its functions.

## Chapter 5, Reporting

This chapter contains instructions for how to use the Reporting tab to create and view reports.

## Chapter 6, Configuration

This chapter contains information about your HPCAS installation, and configuration options for the HPCAS console and components.

## Chapter 7, Wizards

This chapter includes step by step instructions for each of the HPCAS wizards.

## Chapter 8, Preparing and Capturing OS Images

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

## Chapter 9, Using the Publisher

This chapter includes instructions for using the HPCAS Publisher.

## Chapter 10, Using the Application Self-service Manager

This chapter contains instructions for how to use the Application Self-service Manager (installed with the Management Agent).

## Chapter 11, Settings Migration

This chapter contains information for the backup and restoration of user settings using Settings Migration Manager and the Settings Migration Utility.

## Chapter 12, FAQs

This chapter includes frequently asked questions regarding common management tasks available when using HPCAS and its components.

## [Chapter 13, Troubleshooting](#)

This chapter includes information and steps to resolve common issues encountered while using HPCAS.

## [Appendix A, About Double-Byte Character Support](#)

This appendix includes information about double-byte character support.

# Overview

HP Client Automation is available in the following product levels:

- Starter
- Standard
- Enterprise

Information for using Starter and Standard is included in this guide. For information on HP Client Automation Enterprise, refer to the HP Software Support web site.

The following sections detail what features are available with each of the Starter and Standard licenses:

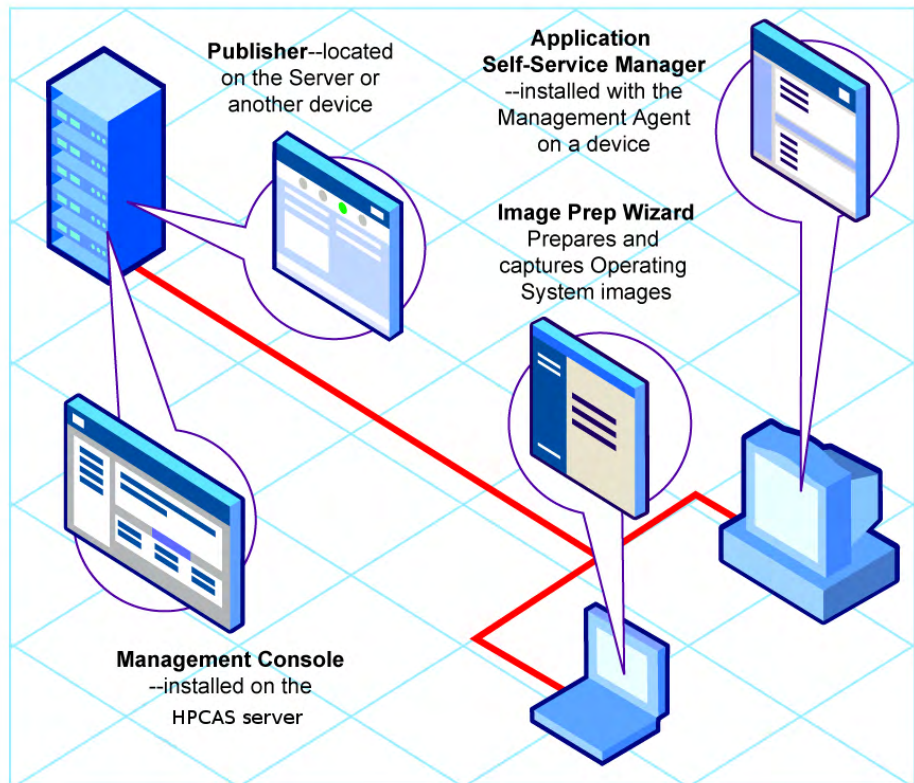
- [HP Client Automation Starter Features](#) on page 23
- [HP Client Automation Standard Features](#) on page 24

The following sections contain summary information about each HPCAS component:

- [The HPCAS Console](#) on page 25
- [Management Agent](#) on page 27
- [HP Client Automation Administrator Publisher](#) on page 28
- [The Image Preparation Wizard](#) on page 28
- [The Settings Migration Manager](#) on page 29

The following figure illustrates a sample environment with HPCAS components installed.

**Figure 1     Sample HPCAS Environment**



## HP Client Automation Starter Features

If you have a license for HP Client Automation Starter, the following management capabilities are available:

- **Hardware and software inventory**  
Hardware and software inventory collection is available for managed HP devices, including BIOS configuration information. The inventory information collected on devices is viewed through a central console. Reporting tools present the data in detailed or graphic views that can be easily filtered to show devices matching particular criteria.
- **Hardware alert reporting**  
Devices managed by the HP Client Automation Starter can be configured

centrally to report hardware alerts, such as fan failure or chassis opening, on the client device or to the central console. Using the HP Client Management Interface (CMI), an administrator can target a system for repairs before other hardware components are affected.

- **Softpaq management**

HP Client Automation Starter allows you to automatically acquire applicable Softpaqs for devices in an environment, determine whether or not a device requires a Softpaq to update the BIOS, device drivers, or HP provided applications, and deploy the Softpaqs to the device, all from a central console. The reporting area of the console provides information on which acquired and applicable Softpaqs have or have not yet been applied to a device. See [Publishing HP Softpaqs](#) on page 223 for additional information.

- **BIOS management**

HP Client Automation Starter allows you to apply a password to protect the BIOS, adjust boot order on a device, enable Wake-on-LAN, or adjust other BIOS configuration settings. HPCAS can determine current BIOS settings for HP devices in the environment and update the BIOS settings to the desired configuration.

- **ProtectTools management**

Configure ProtectTools security settings.

- **Remote management**

Administrators can take control of problem devices with integrated remote control capabilities in the console. Beyond remote control, administrators have additional power management capabilities built into the console, such as the ability to power down or reboot devices, and Wake-On-LAN.

- **Thin client management**

Deploy Operating Systems and software to HP thin client devices running Windows XPe, CE and embedded Linux. Thin client devices are client computers that depend primarily on a central server for processing activities. HP provides many thin client device models.

## HP Client Automation Standard Features

An HP Client Automation Standard license includes all of the functionality available with the Starter license detailed above, as well as the following additional features:

- **OS deployment**

Deploy supported Windows operating systems to PC client devices.



Operating systems can be deployed to bare metal devices (no existing operating system) or to devices currently running an existing supported Windows operating system.

- **Settings migration**

User settings and files can be moved from machine to machine or migrated from OS to OS for an in-place migration on the same device. Migration of settings is supported across product versions. For example, settings can be migrated from Office XP to Office 2003.

- **Software deployment**

Deploy packaged software to managed devices in an environment. Software can be distributed to locally or remotely connected PCs. If a device is on the network, but not powered on when the deployment job is run, it can be powered on as part of the deployment process.

- **Microsoft patch management**

HP Client Automation Standard provides the ability to manage Microsoft patches in an environment. Patches are automatically acquired from Microsoft. After acquisition, managed devices determine patch compliance, and patches can be deployed to devices. After patches are deployed, they are regularly verified to ensure the device is protected against the security threat addressed by the patch.

- **Inventory and software usage collection**

In addition to hardware and software inventory collection, HP Client Automation Standard can collect software usage information. Usage information can be used to determine license compliance or determine which software licenses are required in an environment. Administrators can determine if they have too many or not enough software licenses with HPCAS's usage management tracking and reporting capabilities.

- **Remote content management**

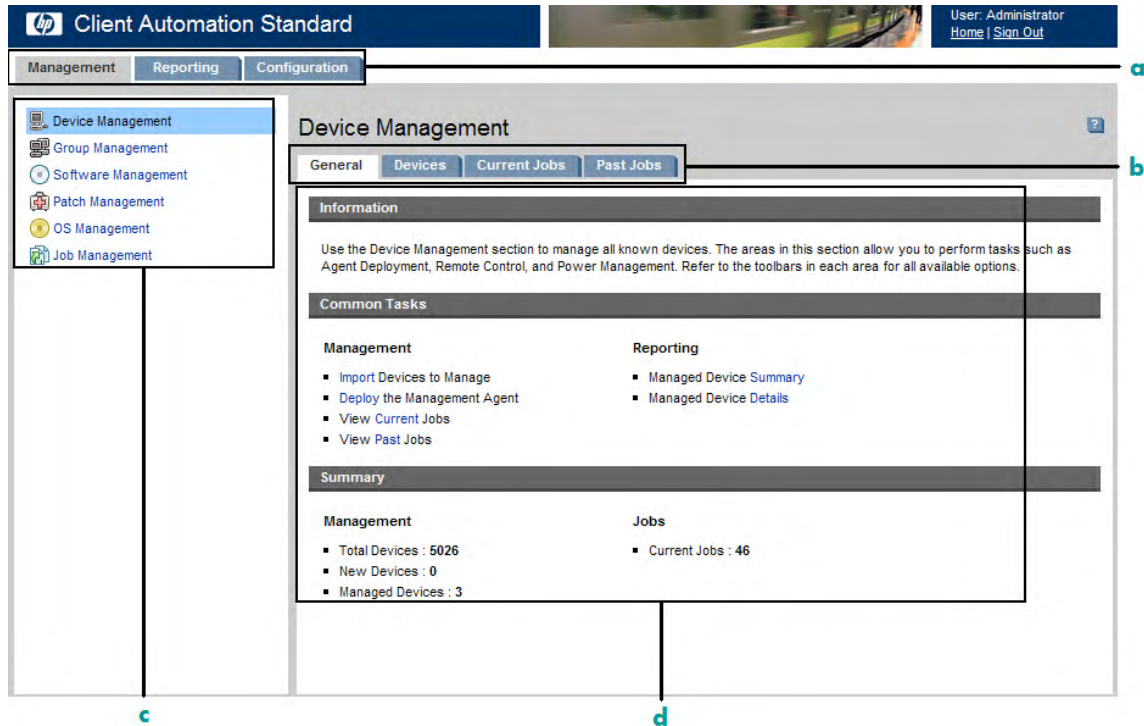
To better facilitate remote offices, HP Client Automation Standard provides the ability to deploy infrastructure servers to deliver resources. This allows for client devices to get their resources from a more local source instead of pulling resources over slower wide area network connections.

## The HPCAS Console

The HPCAS Console is the main web interface used to manage devices, software, operating systems, and patches as well as create and view reports based on those managed devices.

Review the HPCAS Console areas displayed in [Figure 2](#) on page 26.

**Figure 2 HPCAS Console areas**

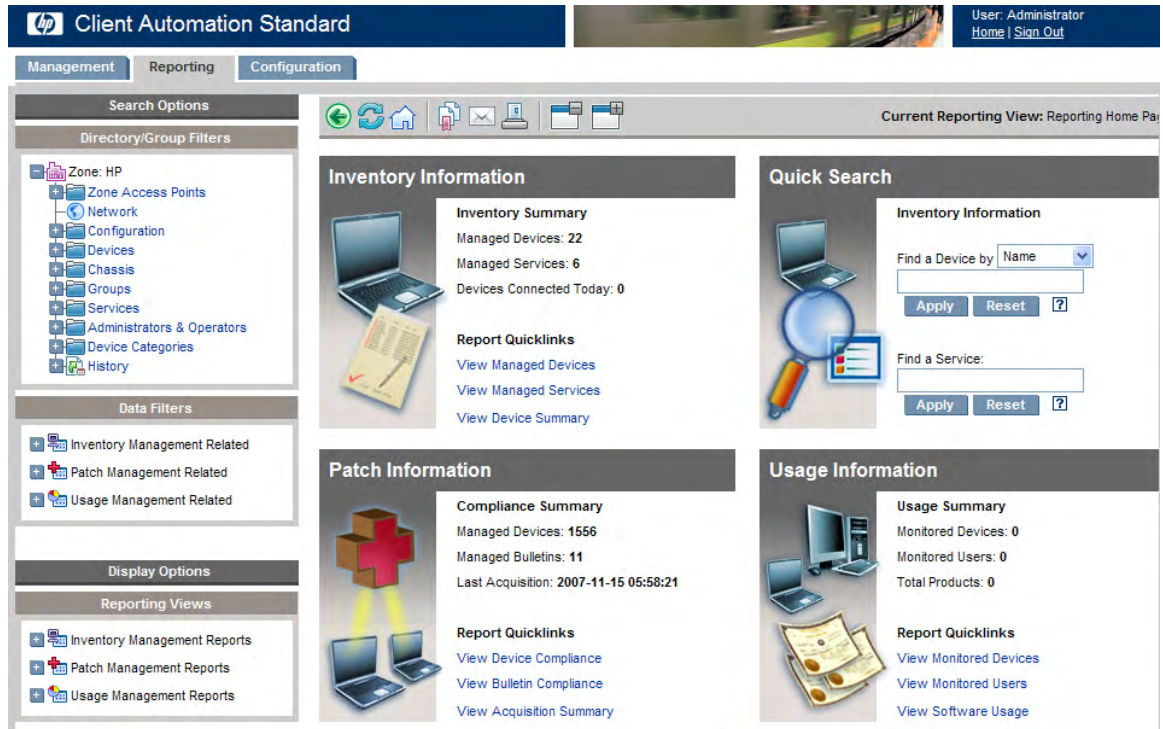


### Legend

- a Console Tabs** - the tabs across the top of the console allowing you to navigate to the three main console areas
- b Workspace Tabs** - tabs displayed within each section
- c Console Tab Sections** - the available sections within a console tab
- d Workspace** - main area where contents of each tab are displayed

The Reporting tab of the console has a slightly different layout than the Management and Configuration tabs. Search and Display options appear on the left and the report query results are displayed in the workspace on the right. The following figure shows an example Reporting tab window.

**Figure 3      Reporting tab**



## Management Agent

The Management Agent is used to manage devices that have been imported into HPCAS. An administrator deploys the Management Agent to a device then entitles and installs software and patches to that device or device's group.

- **Application Self-service Manager**  
When the Management Agent is deployed to a device, the Application Self-service Manager is installed and made available for a user to manage software that has been entitled to that device.

See [Using the Application Self-service Manager](#) on page 231 for more information.

## Installing Software

There are two ways to install software to a managed device.

- 1 Users select the entitled software from the Application Self-service Manager and install it at their discretion. See [Using the Application Self-service Manager](#) on page 231 for more information.
- 2 An administrator entitles and deploys software to a managed device directly from HPCAS without the need for any end-user interaction. See [Software Management](#) on page 81 for more information.

## HP Client Automation Administrator Publisher

The Publisher is used to publish software, operating system images, BIOS configuration settings, or HP Softpaqs into the HPCAS database. Software services can then be entitled and deployed to managed devices within your environment.

► A **service** is any entry in the Software Library, Patch Library, or OS Library. A service **import deck** or **export deck** contains all components necessary to install a particular service (files and folder structures, for example).

The Publisher should be installed to the device from which you plan to select and configure software services. You can install the Publisher using the HP Client Automation Administrator installation file included on the HPCAS installation media, or by using the [HP Client Automation Administrator Publisher](#) service that is available in the Software Library for distribution to a managed device.

See [Using the Publisher](#) on page 213 for more information.

- **HP Client Automation Agent Explorer**  
The Agent Explorer is a component of the HP Client Automation Administrator and is installed along with the Publisher. Use it to troubleshoot and resolve problems. Do *not* use it without direct instructions from HP Support.

## The Image Preparation Wizard

The Image Preparation Wizard prepares and captures operating systems locally on a device. The wizard is part of the Image Preparation Wizard CD ISO that is available on the HPCAS media.

See [Preparing and Capturing OS Images](#) on page 189 for detailed instructions.


## The Settings Migration Manager

Use the Settings Migration Manager on the HPCAS server to define a template for capturing user settings for applications and operating systems on managed devices.

When defined, deploy the Settings Migration Utility service to managed devices. Use the utility to backup and restore settings based on the configuration template defined on the HPCAS server.

See [Settings Migration](#) on page 249 for more information.

## Getting Help

Click the **Help**  button in the upper right corner of any window to open the HPCAS online help.

In addition to the console, the Publisher, Application Self-service Manager and Image Preparation Wizard each contain specific online help based on information in this guide.



## 2 Installing HPCAS

This chapter explains how to install and configure HP Client Automation Starter and Standard and its components. Each of the following sections contains specific installation instructions and requirements for HPCAS, the Publisher, and the Management Agent:

- [System Requirements](#) on page 31
- [Installing HPCAS](#) on page 35
- [Installing the Publisher](#) on page 39
- [Manually Installing the Management Agent](#) on page 41

### System Requirements



HPCAS is recommended for managing software, patches, and inventory for up to 10,000 devices.

### Platform Support

For detailed information about supported platforms for HPCAS Servers and target devices, see the release note document that accompanies this release.

### Web Browsers

HPCAS is supported on the following web browsers:

- Microsoft Internet Explorer 6 and 7

### Server

- Dedicated server with dual processors, minimum 2GHz CPU
- 4 GB RAM

## Database

- Microsoft SQL Server 2000 SP4 or above must be locally installed or remotely accessible from the HPCAS server (SQL Server Personal Edition is recommended only for testing or demonstration purposes).
- SQL Server must be configured to use mixed mode authentication.



If you are installing HPCAS on a Windows 2000 system, assure that the local system has the latest Microsoft Data Access Components installed (this is required to access SQL Server remotely). Visit **[www.microsoft.com](http://www.microsoft.com)** for more information.

## Target Devices

- For detailed information about supported platforms for target devices, see the release notes.
- HP Thin Client devices to be managed should have Windows CE, XPe, or Embedded Linux installed.
- File and Printer Sharing should be enabled.
- For target devices running Windows XP that are not part of an Active Directory, Simple File Sharing must be disabled.
- TPM enabled systems require Infineon Driver version 2.00 or higher.

## Firewall Settings

HPCAS uses several TCP ports for communication to managed devices. If corporate or personal firewall software is in place, then exclusions must be made.

### Target Devices

If the target client device has a personal firewall installed then the following port must be excluded for inbound traffic:

- TCP 3463

The following ports must be excluded to enable remote deployment of the Management Agent:



- TCP 139 and 445
- UDP 137 and 138

Windows Firewall users can select File and Printer sharing to exclude these ports.

In addition, the following program files must be excluded from the firewall.

In `C:\Program Files\Hewlett-Packard\CM\Agent`:

- `RadUIShell.exe`
- `Radexecd.exe`
- `nvdkit.exe`

And in `C:\Program Files\Hewlett-Packard\CM\ManagementAgent`:

- `nvdkit.exe`

## HPCAS Server

If a corporate firewall is installed, then the following ports must be excluded for TCP traffic on the server:

3460, 3464, 3465, 3466, 3467, 3468, 3469, 3470 and 3480

## SQL Server

If SQL Server is installed on a separate server from the HPCAS Server, firewall rules may need to be added to enable communication from the HPCAS Server to SQL Server.

Refer to the following Microsoft KB article for information on opening required ports for SQL Server:

**<http://support.microsoft.com/kb/841251>**

## Infrastructure Servers

The following ports must be excluded if a firewall is enabled on any of the infrastructure servers you will be using. See [Infrastructure Management](#) on page 142 for information on managing Infrastructure Servers in your environment.

- TCP 3463, 139, 445, and 3467
- UDP 137 and 138

Windows Firewall users can select File and Printer sharing to exclude TCP ports 139 and 445 and UDP ports 137 and 138.

## Sygate Firewall Settings

Windows XPe thin client devices ship with Sygate firewall pre-installed. In addition to the settings described in [Target Devices](#) on page 32, Sygate must be configured to allow HPCAS to operate.

- 1 Log on to Windows XPe as Administrator.
- 2 Right-click the Sygate icon in system tray and select **Advanced Rules**.
- 3 On the General tab:
  - Add description **Allow HPCAS All**.
  - Select **Allow this traffic**.
- 4 On the Applications tab, use the Browse button to add the following applications from C:\Program Files\Hewlett-Packard\CM\Agent:
  - Nvdkit
  - Radconct
  - Radpinit
  - Radexecd
  - Radstgrq
- 5 Make sure each item is selected (with a check mark next to each).
- 6 Click **OK** to save the new rule.
- 7 Click **OK** to exit.
- 8 Right-click the Enhanced Write Filter (EWF) icon in system tray and select commit. You are prompted to reboot. This will write your changes to the flash memory.

## VMware Requirements

If you are installing HPCAS to a VMware environment for testing purposes, the following requirements must be met:

- VMware version 6.02 or greater.
- 1.5 GB Memory allocated.

- 8 GB HDD space allocated (additional space may be required for migration).
  - Host OS: Windows 2000 or 2003 server.
  - Guest OS: Windows 2000 or 2003 server.
  - Host system: dual processors (minimum 2 GHz CPU) so VMware can set affinity to one, if needed.
  - Refer to the [System Requirements](#) above for additional HPCAS server requirements.
- HPCAS installed to a VMware environment should be used for testing or evaluation purposes, only.
- If you are installing HPCAS to a VMware environment with a Windows XP host operating system, the installation may hang, Disabling Acceleration in the VMware Advanced Options may allow the installation to continue. Acceleration can be enabled again after the install is complete.

## Installing HPCAS

The next sections describe the steps required for installing and configuring HPCAS. Steps 1 and 2 must be completed in order.


- 1 [Pre-Installation – Database Setup](#) on page 35
- 2 [Installing](#) on page 37
- 3 [Installing the Publisher](#) on page 39

### **Task 1**     [Pre-Installation – Database Setup](#)


Before you can install HPCAS, you must first set up your SQL Server database. To do this, attach the supplied database file (CCMDB\_Data.MDF) to the SQL Server you will be using for HPCAS.

[To attach the HPCAS database using SQL Server 2000](#)

- 1 From the HPCAS media, copy the Database folder to a location that your SQL Server can access.

- 2 Open SQL Server Enterprise Manager, and under the desired SQL Server (for example, local) click to highlight **Databases**.
  - 3 From the File menu, click **Action → All Tasks → Attach Database**.
  - 4 Browse to the `Database` folder that you copied, and select **CCMDB\_Data.MDF**.
    - Configure the database attachment to attach as **CCMDB** with the database owner name **sa** (or the appropriate name assigned by your database administrator).
-  The database owner name may not be **sa** if you are using Windows Authentication.
- The SQL Server name, admin user ID, and password are required during HPCAS installation.


#### To attach the HPCAS database using SQL Server 2005

- 1 From the HPCAS media, copy the `Database` folder to a location that your SQL Server can access.
  - 2 Open SQL Server Management Studio. The **Connect to Server** window opens.
  - 3 In the **Authentication** box, select **SQL Server Authentication** and login as **sa** (or the appropriate name assigned by your database administrator).
  - 4 Click **Connect**.
  - 5 Right-click **Databases** and select **Attach**.
  - 6 Click **Add** and browse to the `Database` folder that you copied, and select **CCMDB\_Data.MDF**.
    - Configure the database attachment to attach as **CCMDB** with the database owner name **sa** (or the appropriate name assigned by your database administrator).
-  The database owner name may not be **sa** if you are using Windows Authentication.
- The SQL Server name, admin user ID and password are required during HPCAS installation.

Now the database is attached. The next section will describe the HPCAS installation in detail.


## Task 2 Installing HPCAS

Install HPCAS to a dedicated server in your environment.

 Before installing HPCAS, you must first set up your SQL Server database. See the previous section for database setup instructions.


### To install HPCAS

- 1 On the HPCAS media, double-click **hpccm.exe**. The Welcome window opens.
- 2 Click **Next**. The License Agreement window opens.
- 3 Read and accept the License Agreement, and click **Next**. The User Information window opens.
- 4 Enter your User Information and the location of your license file, and click **Next**.

 The license file must have the extension `.nvd`.

The ODBC Connection Configuration window opens.

- 5 Configure an ODBC DSN connection to your HPCAS database. Enter the SQL Server hostname, the user account, and the user password and click **Next**. The Target Drive window opens.
- 6 Select the target installation drive, and click **Next**. The Proxy Configuration window opens.
- 7 If you need to use an Internet proxy to access the Internet, click **Yes** to display the Proxy Details and Advanced settings. Otherwise, accept the default **No**, and continue with step 10.
- 8 Fill in the required Proxy Details and Advanced Proxy settings, if required, and click **Next**. The HPCAS Server Hostname window opens.
- 9 Enter the fully qualified hostname to be used by client computers connecting to this server.

 This hostname would typically be set up by your network administrator as a static DNS entry, for example, `HPCAS.acmecorp.com`. This allows client computers to continue to access the HPCAS server in the event of a computer name or IP address change.

- 10 Click **Next**. The Ready to Install the Application window opens.
- 11 If you want to change any of the installation settings click **Back**. When you are ready to install, click **Next**.
- 12 HPCAS is installed. Click **Close** to exit the application.
- 13 If you will be capturing and deploying Windows Vista images with HPCAS, you must copy two utilities to the HPCAS Server. These utilities are found on the Windows Vista media and within the default installation directory of the Windows Automated Installation Kit (WAIK). WAIK is available from the Microsoft web site. It is not included as part of a normal Vista installation.
  - a Create \utilities\Program Files in  
C:\Novadigm\OSManagerServer\OSM\SOS\winpe\
  - b Copy bootsect.exe from \boot on the Windows Vista media to  
C:\Novadigm\OSManagerServer\OSM\SOS\winpe\utilities\  
Program Files\.
  - c Copy imagex.exe from C:\Program Files\Windows AIK\Tools\x86  
to C:\Novadigm\OSManagerServer\OSM\SOS\winpe\utilities\  
Program Files\.

### Launching the HPCAS Console

If you are launching HPCAS locally, you can double-click the **HP Client Automation Console** desktop icon.

Alternatively, you can access the HPCAS Console using a Web browser from any device in your environment (Microsoft Internet Explorer 6 or above is required).

- Go to **<http://HPCAShost:3480/ccm>**

Where *HPCAShost* is the name of the server where HPCAS is installed.

At the Log In page, enter your user name and password and click **Sign In**. By default, the user name is **admin** and the password is **secret**.

- ▶ **Note about Windows 2003 Server:** To allow local access to HPCAS on a device with Windows 2003 Server installed, make sure to check **Bypass proxy server for local address** within the Local Area Network (LAN) Settings for that device.
- ▶ In order to view the Reporting section graphical reports, Java Runtime or Java Virtual Machine is required. Java can be installed from **<http://java.com/en/index.jsp>**.

### Task 3 Installing the Publisher

Install the Publisher to the location from which you will be publishing software to HPCAS.

In addition to the installation file included with the product CD, a Publisher service, [HP Client Automation Administrator Publisher](#), is available in the HPCAS Software Library for distribution to a managed device. To install the Publisher, use one of two methods, which are described in the following sections:

- [To install the Publisher using the installation program](#) on page 39
- [To install the Publisher using the Software Publisher service](#) on page 39

#### To install the Publisher using the installation program

- 1 On the device on which you want to install the Publisher, open the HPCAS media to the `RadAdmin` directory and double-click `setup.exe`.

The Welcome Window opens.



The Publisher is a component of the HP Client Automation Administrator. Refer to the HP web site for additional information about HP Client Automation Enterprise products and services.

- 2 Click **Next** to begin the installation. The End-User License Agreement window opens.
- 3 Read and accept the License Agreement, and click **Next**.
- 4 Select the installation directory and click **Next**.
- 5 Enter the IP address or hostname of your HPCAS server. The default port 3464 should not be changed.
- 6 Click **Next**. The Ready to Install the Application window opens.
- 7 Click **Install** to begin the installation.
- 8 When the installation is complete, click **Finish**.

#### To install the Publisher using the Software Publisher service

- 1 Manage the target device by deploying the Management Agent. See [Deploying the Management Agent](#) on page 60 for details.

- 2 Entitle the Software Publisher service to the device. First add the device to a group and assign entitlement. See [Group Management](#) on page 67 for more information.
- 3 Deploy the [HP Client Automation Administrator Publisher](#) service that is available in the HPCAS Software Library. See [Software Management](#) on page 81 for instructions on deploying software.

After it is deployed, you can use the Publisher to publish software, HP Softpaqs, BIOS settings, and OS image services.

### [Accessing the Publisher](#)

- Access the Publisher using the **Start** menu:

**Start → All Programs → HP Client Automation Administrator → HPCA Administrator Publisher**



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

For additional Publisher information, see [Using the Publisher](#) on page 213 or refer to the Publisher online help.



# Manually Installing the Management Agent

Normally, the Management Agent is deployed to target devices using the HPCAS console (see [Deploying the Management Agent](#) on page 60 for more information). To manage devices that are not always connected to the network, you can install the Management Agent manually. A separate installation file is included with the HPCAS media.

After the Management Agent is installed, client devices are added to the HPCAS database automatically.

► The Management Agent cannot be deployed to thin client devices and must be installed manually. See [Installing the Management Agent on Thin Clients](#) on page 41 for installation instructions.

To install the Management Agent manually

- 1 Use a command line and go to the `RadAgent` directory of the HPCAS media.
- 2 Type `setup.cmd host`, where `host` is the IP address or hostname of your HPCAS server.
- 3 Press **Enter**. The Management Agent is installed and the device is ready for management using HPCAS.

## Installing the Management Agent on Thin Clients

In addition to devices not always connected to the network, you will need to manually install the Management Agent to any thin client devices you want to manage.

### Linux-based Thin Clients

Installation of the HPCAS Management Agent requires minimum free space of 3 MB on the `/mnt` file system. Certain thin client models and related images do not have enough space to install the agent. Currently, models that have only a 32 MB flash memory cannot install the agent locally. See notes on running from an NFS share below, and restrictions on using Local Service Boot (LSB) for OS deployment.

## To install the Management Agent on a Linux-based thin client

- 1 Login to the target thin client device as root.
- 2 Create a new directory called `/mnt/opt/OVCM`.
- 3 Copy the contents of `ThinClient.tar` (located on the HPCAS media in the `/ThinClient/Linux` directory) to `/mnt/opt/OVCM`.

Depending on your device model, you may have to un-tar these files 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 (would require approximately 7-8 MB free). After un-tarring, you can delete the `ThinClient.tar`.

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

```
./install -i HPCAS_Server
```

Where *HPCAS\_Server* is the hostname or IP address of the HPCAS server.

The Management Agent is installed.



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



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

## Running the Agent from an NFS Share

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

To run the agent remotely from an NFS share:

- 1 Update the install script and modify the MEDIA\_RAM\_ROOT and INFRA\_MEDIA\_ROOT variables to point to the NFS directory.
- 2 Create the directory /mnt/opt/OVCM and place the install script into this location, and place the rest of the installation package (thinclient.tar) into the NFS directory.
- 3 Run install as described in step 4 above.

To remove the Management Agent from a Linux-based thin client

Use the **uninstall** script to remove the Management Agent.

- 1 Login to the device as root.
- 2 Go to /tmp/OVCM/IDMSYS.
- 3 Type ./uninstall and hit **Enter**.

The Management Agent is removed.

## Windows XPe

To install the Management Agent to Windows XPe

- 1 Access the HPCAS media from the Windows XPe Thin Client device.
- 2 On the HPCAS 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 HPCAS server.

The Management Agent is installed.

To remove the Management Agent from Windows XPe

Use the installation program **setup.exe** to remove the Management Agent from Windows XPe.

- 1 Double-click **setup.exe**
- 2 Select **Remove**.
- 3 Click **OK**.

The Management Agent is removed.

## Windows CE

To install the Management Agent to Windows CE

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

The Management Agent is installed.

To remove the Management Agent from Windows CE

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

## Removing HPCAS

Use the HPCAS installation program to remove HPCAS from your server.

If you use the Windows Control Panel applet **Add/Remove Programs** to remove HPCAS, some files and folders will be left on the server and must be removed manually (the directory `C:\Novadigm` and any files that were added or changed since the initial installation).

To remove HPCAS from your server

- 1 On the HPCAS media, double-click **hpccm.exe**
- 2 Select **Remove** and click **OK**.

HPCAS is removed from your server.

## Configuring PXE for OS Deployment

If you will be using PXE to deploy operating system images, use the following instructions to configure your DHCP and TFTP servers.



HPCAS assumes a TFTP server and DHCP server already exist in your environment. These are not included with the HPCAS media.

### To configure PXE for OS deployment

- Configure your DHCP server to use a Boot File (DHCP Option 067) and a Boot Server (DHCP Option 066).
  - The Boot file used in HPCAS is `rombl.0`
  - The Boot Server must point to the IP address running the TFTP Server.
- Configure the TFTP server to serve the boot files.
  - Copy the contents of the `\OSManagement\PXE\` directory from the HPCAS media to your TFTP server.
  - In the newly copied `\linux.cfg` directory, edit the file named `default` to point to your HPCAS server. Note that this configuration file must use the IP address and not the hostname of your server. Here is an example default configuration file.

```
[OS Manager]
DFLTSVOS=_SVC_LINUX_
ISVR=192.168.1.11:3469
[_SVC_LINUX_]
KERNEL=bzImage
APPEND=initrd=rootfs.gz root=/dev/ram0 rw quiet
pci=nommconf vga=0x311 splash=silent
[_SVC_PEX86_]
PEBCD=rombl.bcd
PEAPPEND=initrd=winpe.wim
```

In the example above, the HPCAS server IP address is 192.168.1.11 and the port number used for OS management is 3469.



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.

For information about PXE industry standards, see:  
**<ftp://download.intel.com/design/archives/wfm/downloads/pxespec.pdf>**

## 3 Getting Started

Now that you have installed and configured HPCAS, you are ready to start using the web-based console to manage your Windows client environment. The next sections get you started using HPCAS and introduce you to the essential tasks you will need to begin.

- [Logging In](#) on page 47
- [Quick Start Tasks](#) on page 47

### Logging In

Access HPCAS using the desktop icon, or by using a browser from any device in your environment with network access to the HPCAS server.

- Go to **http://HPCAShost:3480/ccm**, where *HPCAShost* is the name of the server where HPCAS is installed.

At the Log In page, enter your user name and password and click **Sign In**. By default, the user name is **admin** and the password is **secret**.

To learn how to change the password and add additional users see [Configuration](#) on page 137.

- The HPCAS console may open additional browser instances when you are running wizards or displaying alerts. To access these wizards and alerts, be sure to include HPCAS as an Allowed Site in your browser's pop-up blocker settings.
- For security reasons, HPCAS logs out the current user automatically after 20 minutes of inactivity, after which time you will need to log in again to continue using the console.

### Quick Start Tasks

Use the quick start tasks described in this section to begin managing your Windows client environment right away.



Some tasks in this section require HP Client Automation Standard.

When you have completed these tasks, you will:

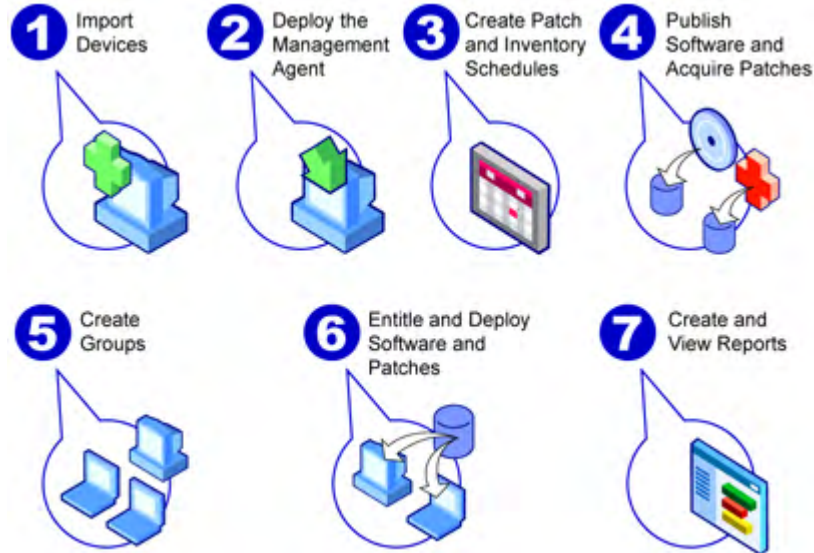
- have managed devices by importing them into HPCAS and deploying the Management Agent.
- have configured the schedules needed for inventory and patch management.
- know where to begin to publish software and acquire patches.
- have been introduced to creating device groups then deploying software and patches to devices in those groups.
- know where to create reports for all managed devices in your environment.

The following sections discuss these tasks and point you to related sections for additional information:

- 1 [Import Devices](#) on page 49
- 2 [Deploy the Management Agent](#) on page 49
- 3 [Configure Schedules](#) on page 50
- 4 [Publish Software and Acquire Patches](#) on page 51
- 5 [Create Groups](#) on page 52
- 6 [Entitle and Deploy Software or Patches](#) on page 52
- 7 [Generate and View Reports](#) on page 53



**Figure 4 Quick Start tasks at a glance**



### **Task 1** Import Devices

In order to collect inventory information or deploy software and patches, you first need to make HPCAS aware of the devices in your environment by importing them.

- From the Device Management General tab, click **Import** to launch the [Import Device Wizard](#).
- Follow the steps in the wizard on page 168 to import devices.

► Most tasks create a job that can be monitored in the Current Jobs and Past Jobs tabs or in the Job Management section.

When devices have been imported, [Deploy the Management Agent](#) to manage software, patches, and inventory.

### **Task 2** Deploy the Management Agent

When devices are imported, deploy the Management Agent.

- From the Device Management General tab, click **Deploy** to launch the [Agent Deployment Wizard](#).

- Follow the steps in the wizard on page 169 to deploy the Management Agent to your imported devices.



Deploying the Management Agent to Windows Vista devices.

Access to the Administrative share (C\$) on Windows Vista devices is disabled for locally defined administrators. Therefore, Windows Vista devices should be part of a domain, and the domain administrator's credentials should be specified during Management Agent deployment through the HPCAS console. If the devices are not part of a domain, additional steps are required to allow access for local administrators. See the following link on Microsoft's support web site for detailed steps:

**<http://support.microsoft.com/kb/947232/en-us>**


After making these changes, reboot the device.

Now that you have begun to manage devices, [Configure Schedules](#) for inventory collection, patch compliance scanning and patch acquisition.

### **Task 3**    [Configure Schedules](#)

To initiate inventory and patch acquisition schedules, use the [Software/Hardware Inventory Wizard](#) and [Configuration](#) tabs.

[To configure the inventory schedule](#)

- From the [Devices](#) tab in the Device Management area, select managed devices (or select a Group from the Group Management, [Groups](#) tab).
- Click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory** to launch the [Software/Hardware Inventory Wizard](#).
- Follow the steps in the wizard on page 171 to define software and hardware inventory collection for your devices and groups.


[To configure patch acquisition schedule and settings](#)

- Use the [Configuration](#) tab, [Patch Management](#) section to configure patch acquisition settings and schedule.
  - Use the Schedule tab to enter a schedule for patch acquisitions.
  - In the Settings tab, enter the required Windows patch and HP Softpaq acquisition settings.



Microsoft Patch Management is available with HP Client Automation Standard.

#### To configure a patch compliance discovery schedule

- From the [Devices](#) tab in the Device Management area, select managed devices.
- Click the **Inventory Collections**  toolbar button, then select **Discover Patch Compliance** to launch the [Patch Compliance Discovery Wizard](#).
- Follow the steps in the wizard on page 171 to create a patch compliance schedule for your devices and groups.

When schedules are configured, you can [Publish Software and Acquire Patches](#).


### **Task 4**    [Publish Software and Acquire Patches](#)

Before you can deploy software and patches to managed devices, you must populate the Software Library and Patch Library.

- Use the Publisher to publish software into the HPCAS database.
  - Launch the Publisher on the machine from which you plan to configure and publish software services. Refer to the Publisher online help or [Chapter 9, Using the Publisher](#) for more information.



Publishing software and operating systems is available with HP Client Automation Standard. With HP Client Automation Starter, you can publish HP Softpaqs and BIOS settings or software and OS images only for thin client devices.

- Populate the Patch Library by acquiring patches from HP and Microsoft sources.
    - From the Management tab, Patch Management section, click **Acquire**. Patches are downloaded and added to the Patch Library. HPCAS automatically downloads patches according to the acquisition schedule configured in the previous step, [Configure Schedules](#).
-  Patches should be acquired initially to an HPCAS Server in a non-production lab environment for evaluation to prevent possible performance issues.

When software and patches are available in each library, [Create Groups](#) to entitle software and patches for deployment.

## Task 5 Create Groups

To deploy software or patches, you must create a group that includes the target devices, and then entitle software or patches to that group.

- From the Group Management General tab, click **Create** a New Static Group. This will launch the [Group Creation Wizard](#). Follow the steps in the wizard on page 174 to create a static group.
- HPCAS also supports dynamic device groups that are based on discovered devices (discovery group) or on selected inventory criteria (reporting groups). These groups are also created using the Group Creation Wizard. See [Group Management](#) on page 67 and [Reporting](#) on page 121 for more information.



When the group has been created, [Entitle and Deploy Software or Patches](#) to the devices in the group.

## Task 6 Entitle and Deploy Software or Patches

In the Group Management section, Groups tab, click the Group description to open the Group Details window. From here, you can entitle and deploy software or patches.



► HP Client Automation Standard is required to deploy software and patches. HP Client Automation Starter allows for the deployment of BIOS settings and HP Softpaqs.

### To entitle and deploy software

- Use the [Group Details](#), Software tab to entitle software.
  - Click the **Add Software Entitlement**  toolbar button to select software services and make them available to that group. Entitled software is displayed in the Software tab list and is available to end users in the Application Self-service Manager, but is not automatically deployed. This enables you to create a managed software catalog and allow users to determine what optional software to deploy at what time.
  - To deploy software, select the software to deploy, then click the **Deploy Software**  toolbar button. This opens the [Software Deployment Wizard](#). Follow the steps in the wizard on page 177, to

deploy software to devices in that group. Deployed software is automatically installed on end user devices.

#### To entitle and deploy patches

- Use the [Group Details](#), Patches tab to entitle and deploy patches.
  - Click the **Add Patch Entitlement**  toolbar button to select patches and make them available to that group. Entitled patches are then displayed within the Patches tab list.
  - To deploy patches, select the patches to deploy, then click the **Deploy Patches**  toolbar button. This opens the [Patch Deployment Wizard](#). Follow the steps in the wizard on page 180 to deploy patches to devices in that group.
    - Patch compliance and enforcement can be configured using the [Patch Deployment Wizard](#).
    - Entitled patches are not shown in the Application Self-service Manager catalog.

You have now successfully used HPCAS to deploy software and patches. Learn about creating reports by following the instructions in the section, [Generate and View Reports](#) below.


### Task 7    [Generate and View Reports](#)

Use the Reporting tab to generate and view reports based on managed device information.

- Follow the instructions in [Reporting](#) on page 121 to generate device reports.

To generate a quick example report, click **View Managed Devices** in the **Inventory Information** area to display a list of all devices that have the Management Agent installed.

When a list of devices is created, you can use the options on the left or click any of the device column details to apply more filters.

When a report is generated, click the **Create a New Dynamic Reporting Group**  toolbar button to create a dynamic group of devices in the report. This will open the [Group Creation Wizard](#). Follow the steps in the wizard on page 174 to create the Reporting Group.



## 4 Management

The Management tab contains the tools you will use to manage your environment. The next sections describe the management areas that you can control:

- [Device Management](#) on page 56
- [Group Management](#) on page 67
- [Software Management](#) on page 81
- [Patch Management](#) on page 91
- [OS Management](#) on page 101
- [Job Management](#) on page 115

# Device Management

Use the Device Management section to import devices, deploy the Management Agent, discover inventory, manage patches, manage device power options, control devices remotely, collect application usage information, and view reports based on all managed devices.

The Device Management tabs are described in the following sections:

- [General](#) on page 56
- [Devices](#) on page 57
- [Current Jobs](#) on page 65
- [Past Jobs](#) on page 66

## General

Use the General tab to add devices, deploy management agents, view current and past Agent Deployment jobs, and view reports about your managed devices.

The Summary section of the workspace shows the number of devices in your database, the number of managed devices (devices that have a management agent installed), and the total number of current jobs.

### To import a device

- In the Common Tasks area, click **Import**. This will launch the [Import Device Wizard](#).

Follow the steps in the wizard on page 168 to add new devices to HPCAS.

### To deploy the Management Agent

- In the Common Tasks area, click **Deploy**. This will launch the [Agent Deployment Wizard](#).

Follow the steps in the wizard on page 169 to deploy the Management Agent to devices in your database.



To deploy the Management Agent to remote devices you need access to administrative shares. Windows XP includes a security feature, Simple File Sharing (SFS) which blocks access to these shares. SFS is enabled by default for Windows XP devices that are part of a



workgroup, and disabled automatically for devices that are joined to an Active Directory domain. If your target devices are running Windows XP and they are not part of an Active Directory domain, then you must turn off SFS to allow installation of the Management Agent. The following Microsoft knowledge base article provides more details on how to configure SFS:

**<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q304040>**

- The Management Agent cannot be remotely deployed to thin client devices and must be installed manually using the installation programs included in the `\ThinClient` directory on the HPCAS media.
- The Management Agent is deployed to Windows Vista and Windows Server 2008 devices in silent mode only.

## Devices

The Devices tab contains a table of all devices that have been imported into HPCAS.

- When HPCAS is installed, the host server is added automatically to the Devices list. This device definition is required by HPCAS and cannot be removed.

Newly imported devices (imported within the last seven days) can be recognized by the word 'new' in parentheses (*new*) to the right of the device name.

- Not all device information is available until a Management Agent is deployed.

Use the Devices toolbar to import devices, deploy or remove the Management Agent, discover inventory, manage patches, manage device power options, control devices remotely, discover application usage, and remove devices from the database.


Click any column heading in the device list to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.

- If computer names in your environment contain more than 15 characters, you may experience unexpected results when using HPCAS to deploy the Management Agent or create groups. HP








recommends that computer names contain no more than 15 characters. For more information, refer to the Microsoft Knowledge Base article:



<http://support.microsoft.com/default.aspx?scid=kb;en-us;188997>

Use the **Search** function to narrow the list of devices. The first search box will always contain the column headings available depending on which section of the console you are currently in. The second box contains search parameters you can use to customize your query.

**Filtered Results**  is displayed at the bottom of the table when you are viewing your query results.

**Table 2      Devices toolbar tasks**

<b>Toolbar Button</b>	<b>Description</b>
	<b>Refresh Data</b> – Refresh the Device list.
	<b>Export to CSV</b> – create a comma-separated list that you can open or save.
	<b>Import Devices to Manage</b> – Launches the <a href="#">Import Device Wizard</a> .
	<b>Deploy the Management Agent</b> – Launches the <a href="#">Agent Deployment Wizard</a> .
	<b>Remove the Management Agent</b> – Launches the <a href="#">Agent Removal Wizard</a> .
	<b>Inventory Collections:</b> <b>Discover Software/Hardware Inventory</b> – Launches the <a href="#">Software/Hardware Inventory Wizard</a> . <b>Discover Patch Compliance</b> – Launches the <a href="#">Patch Compliance Discovery Wizard</a> . <b>Discover Application Usage</b> – Launches the <a href="#">Application Usage Collection Wizard</a> .
	<b>Power Management</b> – Launches the <a href="#">Power Management Wizard</a> .


Toolbar Button	Description
	<b>Remote Control</b> – Launches the Remote Control interface window.
	<b>Delete Devices</b> – Removes a Device from the Device list. Note that removing a device from the Device List does not remove device reporting data. Reporting data must be removed using the Configuration tab. See <a href="#">Maintenance</a> on page 166 for details.

The following tasks are available from the Devices tab.

- [Importing Devices](#) below
- [Deploying the Management Agent](#) on page 60
- [Removing the Management Agent](#) on page 60
- [Discovering Software/Hardware Inventory](#) on page 61
- [Discovering Patch Compliance](#) on page 61
- [Discovering Application Usage](#) on page 61
- [Remote Control](#) on page 62
- [Power Management](#) on page 63
- [Removing Devices](#) on page 63
- [Device Details](#) on page 64

## Importing Devices

The [Import Device Wizard](#) allows you to manually import devices by name or IP address or to discover devices contained within either Active Directory or another LDAP-compliant directory, or within a network domain.

- To import one or more devices into HPCAS, click **Import Devices to Manage**  toolbar button. This will launch the [Import Device Wizard](#).

Follow the steps in [Import Device Wizard](#) on page 168 to add new devices to HPCAS.

## Deploying the Management Agent from the Devices Tab


Use the [Agent Deployment Wizard](#) to deploy the Management Agent to devices in your environment.



Deploying the Management Agent to Windows Vista devices.

Access to the Administrative share (C\$) on Windows Vista devices is disabled for locally defined administrators. Therefore, Windows Vista devices should be part of a domain, and the domain administrator's credentials should be specified during Management Agent deployment through the HPCAS console. If the devices are not part of a domain, you must perform additional steps to allow access for local administrators. See Microsoft's support web site for details.


### To deploy the Management Agent

- 1 Select the check box in the first column to select the devices you want to manage.
- 2 Click the **Deploy the Management Agent**  toolbar button to launch the [Agent Deployment Wizard](#).
- 3 Follow the steps in [Agent Deployment Wizard](#) on page 169 to deploy the Management Agent to the selected devices.

## Removing the Management Agent

Use the [Agent Removal Wizard](#) to remove the Management Agent from devices in your HPCAS database.


### To remove the Management Agent

- 1 Select the check box in the first column to select the devices from which you want to remove the Agent.
- 2 Click the **Remove the Management Agent**  toolbar button to launch the [Agent Removal Wizard](#).
- 3 Follow the steps in [Agent Removal Wizard](#) on page 170 to remove the Management Agent from the selected devices.

## Discovering Software/Hardware Inventory

Use the Software/Hardware Inventory Wizard to discover inventory for devices in your HPCAS database.

### To discover software and hardware inventory

- 1 Select the check box in the first column to select the devices for which you want to discover inventory.
- 2 Click the **Inventory Collections**  toolbar button and select **Discover Software/Hardware Inventory** to launch the [Software/Hardware Inventory Wizard](#).
- 3 Follow the steps in [Software/Hardware Inventory Wizard](#) on page 171 to discover inventory for the selected devices.

## Discovering Patch Compliance

Use the Patch Compliance Discovery Wizard to discover compliance for Devices in your HPCAS database.

### To discover and enforce patch compliance

- 1 Select the check box in the first column to select the devices that you want to target for patch compliance discovery.
- 2 Click the **Inventory Collections**  toolbar button and select **Discover Patch Compliance** to launch the [Patch Compliance Discovery Wizard](#).
- 3 Follow the steps in [Patch Compliance Discovery Wizard](#) on page 171 to discover patch compliance for the selected devices.
- 4 Use the [Reporting](#) tab to view patch compliance reports for the selected devices.


## Discovering Application Usage

Use the [Application Usage Collection Wizard](#) to discover application usage for devices in your HPCAS database. The wizard installs the Collection Agent, which then returns usage data defined by filters you create and enable. Also, if required, usage data can be obfuscated to ensure privacy. See the [Reporting](#) section of the Configuration tab on page 159 for more information.

Usage data is returned one time for individual devices. Recurring usage data collection is available for groups only. See [Discovering Application Usage Data](#) on page 73 for information on collecting usage data for groups.

► HP Client Automation Standard is required for collecting application usage data.

#### To discover application usage


- 1 Select the check box in the first column to select the devices that you want to target for application usage discovery.
- 2 Click the **Inventory Collections**  toolbar button and select **Discover Application Usage** to launch the [Application Usage Collection Wizard](#).
- 3 Follow the steps in [Application Usage Collection Wizard](#) on page 172 to discover application usage for the selected devices.
- 4 Use the [Reporting](#) tab to view usage reports for the selected devices.

## Remote Control

Use the Remote Control interface to launch a remote session with any device. The interface allows you to connect to devices that have either RDP or VNC installed and enabled. HPCAS will detect whether VNC or RDP is installed on the remote system by connecting to ports 5800 and 3389, respectively. If a connection is made on either port, HPCAS will assume one of these programs is installed and running and present that option as an available remote connection method.

► In order to use VNC, Sun Java Plugin for Internet Explorer must be installed. To install Java, go to <http://java.com/en/index.jsp>.

#### To launch a remote session


- 1 Select the device from the list, then click the **Remote Control**  toolbar button to launch the Remote Control interface window.
- 2 Select the Remote Control Method from the available options. Only the programs detected by HPCAS are available.
  - **Windows Remote Desktop** – RDP (Remote Desktop Protocol) is a multichannel capable protocol available on Windows client devices. You can use RDP to connect remotely to a device with RDP enabled

(for example, Windows XP). HPCAS detects this program by connecting to port 3389 on the remote device.

- **VNC Client** – VNC (Virtual Network Computing) is a desktop sharing system used to remotely control another computer. Use VNC to remotely connect to client devices that have VNC installed and enabled.
- 3 If you select a Windows Remote Desktop, you must also select the **Resolution** for the remote session window.
  - 4 Click **Connect**. The remote session opens in a new window.
  - 5 Click **Close** to exit the wizard.
  - 6 When you are finished with the remote session, close the window to disconnect from the device.
- ▶ When using Windows Remote Desktop, you may be prompted to install an ActiveX control. This is required for Windows Remote Desktop to function properly. You are also prompted to connect local drives. This is not required.
- ▶ The VNC Server installed on the managed device must support the VNC Java applet running on port 5800. To verify this, open a browser window to **http://hostname:5800**. If the applet is installed, the login page opens.

## Power Management

Use the Power Management wizard to turn on, turn off, or restart a device.


- Select the device you want to manage, and then click the **Power Management**  toolbar button to launch the **Power Management Wizard**.


Follow the steps in **Power Management Wizard** on page 173 to create a Power Management job for the selected devices.

## Removing Devices

Use the Devices toolbar to remove devices from your HPCAS database.

### To remove devices from HPCAS

- 1 Select the check boxes in the first column to choose the devices that you want to remove.
- 2 Click the **Delete Device(s)**  toolbar button to remove the devices from HPCAS.

 Note that removing a device from the Device List does not remove device reporting data. Reporting data must be removed using the Configuration tab. See [Maintenance](#) on page 166 for details.

## Device Details

On the Devices tab, click any device name to open the Device Details window. The Device Details window presents the configuration model from the perspective of the selected device.

Use the Device Details window to:

- view device properties
- view and modify device group membership
- view entitlements
- view a reporting summary
- deploy the Management Agent
- create device management jobs


The following areas are available from the Device Details window.

### General

The General tab displays common tasks available for the device. To access more configuration tasks click any of the other management area tabs.

### Properties

The Properties tab displays information including the device name, operating system, serial number, IP address, agent status, last logged on user and created and modified dates. Not all information is available until the Management Agent has been deployed.

 The Last Logged on User reports the user account that last logged on to the device via a console login. If multiple users are logged on,



only the last to log on is recorded. The last logged on user will not be updated by a Remote Desktop Connection login or by switching between logged on users.

Additional device information that may be useful during troubleshooting is available in the **Advanced Properties** section. To view this information, click the icon on the right-side of the Advanced Properties title bar to expand the section.

### Groups

The Groups tab displays all groups to which the current device belongs.

### OS

The OS tab displays all operating systems entitled to the device based on the device's group membership. Use the toolbar provided to deploy OS images.

### Software

The Software tab lists all entitled software, based on group membership. Use the toolbar buttons to deploy or remove software on the current device.

### Patches

The Patches tab displays all entitled patches, based on group membership. Use the toolbar to deploy a patch to the current device.



After a patch is deployed it cannot be removed.

### Reporting

The Reporting tab contains summary reports specific to the device you are viewing. For detailed reports, use the [Reporting](#) tab in the main HPCAS console.

## Current Jobs

Current Jobs displays all active or scheduled Device Management jobs. Device Management jobs target individual devices and can be used to either deploy or remove a Management Agent or administer software to devices in the HPCAS database.

Click any column heading to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.

For information about [Job Controls](#) and [Job Status](#), see Job Management, [Current Jobs](#) section on page 115.

## Past Jobs

Past Jobs displays all completed Device Management jobs.

Click any column heading to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.



Completed jobs are moved to the Past Jobs list one minute after completion.

# Group Management

Use the Group Management section to create and manage device groups. Creating device groups eases management and is required to deploy software and patches to managed devices.

The Group Management tabs are described in the following sections:

- [General](#) on page 67
- [Groups](#) on page 68
- [Current Jobs](#) on page 79
- [Past Jobs](#) on page 80

## General

Use the General area to create new groups, manage existing groups, and view current and completed group management jobs.

Groups can consist of both managed and unmanaged devices.

[To create a new static group](#)

- In the Common Tasks area, click **Create a New Static Group**. This will launch the [Group Creation Wizard](#).

Follow the steps in [Group Creation Wizard](#) on page 174 to create a new device group for software and patch deployment.

[To create a new Dynamic Discovery Group](#)

- In the Common Tasks area, click **Create a New Dynamic Discovery Group**. This will launch the [Group Creation Wizard](#).

Follow the steps in [Group Creation Wizard](#) on page 174 to create a new device discovery group.

[To create a new Dynamic Reporting Group](#)

- Use the Reporting tab to define a query, then click the **Create a Dynamic Reporting Group** toolbar button to begin the [Group Creation Wizard](#). See [Creating Dynamic Reporting Groups](#) on page 136, for more information.

The next section, [Group Types](#), on page 68 describes the different types of groups available within HPCAS.

## Group Types

HPCAS uses the following group types to manage devices.

### Internal

Internal Groups are provided by HPCAS. For example, the All Devices group contains all imported devices, by default.

### Static

Create static groups by selecting individual devices. To add or remove devices from a static group, you must modify the group membership manually using the [Group Details](#) window.

### Discovery

A discovery group contains a dynamic list of devices, either managed or unmanaged, from an external source (LDAP, network discovery) according to the parameters you set during the Group Creation Wizard. Discovered devices are automatically added to the HPCAS device list.

### Reporting

Create a reporting group from a list of devices returned in a report query. Reporting groups are updated automatically using a group management job. See [Creating Dynamic Reporting Groups](#) on page 136 for more information.


The following Reporting groups are included with HPCAS by default:

- **All Windows Vista Devices**
- **All Windows XP Professional Devices**
- **All Windows 2000 Professional Devices**
- **All TPM Capable Devices**

These groups refresh daily and will automatically add new managed devices they find that meet the dynamic group requirements.







## Groups



The Groups tab lists all created groups. Newly created groups (created within the last seven days) display the word ‘new’ in parentheses (*new*) to the right of the group name.

- Click the description link for any group to view specific group information.
- Click a column heading to sort the group list.
- Use the toolbar buttons to create inventory, patch, and power management jobs for devices in any group.
- Use the **Search** function to narrow the list of devices. The first search box always contains the column headings available depending on which section of the console you are currently in. The second box contains search parameters you can use to customize your query. **Filtered Results**  is displayed at the bottom of the table when you are viewing your query results.

The groups you create can determine which devices receive what software or patches based on either device inventory, location, or any other criteria you define. Make sure to plan group creation before you add any devices.

**Table 3      Groups toolbar tasks**

Toolbar Button	Description
	<b>Refresh</b> – Refresh the Groups list.
	<b>Export to CSV</b> – create a comma-separated list that you can open or save.
	<b>Create a New Group</b> – Launches the <a href="#">Group Creation Wizard</a> .
	<b>Deploy the Management Agent</b> – Launches the <a href="#">Agent Deployment Wizard</a> .
	<b>Remove the Management Agent</b> – Launches the <a href="#">Agent Removal Wizard</a> .
	<b>Inventory Collections:</b> <b>Discover Software/Hardware Inventory</b> – Launches the <a href="#">Software/Hardware Inventory Wizard</a> . <b>Discover Patch Compliance</b> – Launches the <a href="#">Patch Compliance Discovery Wizard</a> . <b>Discover Application Usage</b> – Launches the <a href="#">Application Usage Collection Wizard</a> .


Toolbar Button	Description
	<b>Power Management</b> – Launches the <a href="#">Power Management Wizard</a> .
	<b>Delete Groups</b> – Removes a Group from the Groups list.

The following tasks are available from the Groups tab.

- [Creating a Group](#) on page 70
- [Deploying the Management Agent](#) on page 71
- [Removing the Management Agent](#) on page 71
- [Discovering Software/Hardware Inventory](#) on page 72
- [Discovering Patch Compliance](#) on page 72
- [Discovering Application Usage Data](#) on page 73
- [Power Management](#) on page 73
- [Removing Groups](#) on page 73
- [Group Details](#) on page 74
- [Group Details Window Tasks](#) on page 76
- [Adding and Removing Devices from Static Groups](#) on page 77
- [Adding and Removing Software Entitlement from Groups](#) on page 77
- [Deploying, Removing, and Synchronizing Software from Groups](#) on page 78
- [Adding and Removing Patch Entitlement from Groups](#) on page 78
- [Deploying Patches to Groups](#) on page 79


## Creating a Group

To create a Static Group

- Click the **Create a New Group**  toolbar button, then select **Create a New Static Group**. This will launch the [Group Creation Wizard](#). You can create groups for both managed and unmanaged devices.

Follow the steps in [Group Creation Wizard](#) on page 174 to create a new static device group for software and patch deployment.

To create a [Dynamic Discovery group](#)


- Click the **Create a New Group**  toolbar button, then select **Create a New Dynamic Discovery Group**. This will launch the [Group Creation Wizard](#).

Follow the steps in [Group Creation Wizard](#) on page 174 to create a new Dynamic Discovery group for software and patch deployment.

## Deploying the Management Agent to a Group

Use the Agent Deployment Wizard to deploy the agent to a group.

To deploy the [Management Agent](#) to a group of devices

- 1 Select the check box in the first column to select the group you want to either manage or redeploy the Management Agent to.
- 2 Click the **Deploy the Management Agent**  toolbar button to launch the [Agent Deployment Wizard](#).
- 3 Follow the steps in the wizard on page 169 to deploy the Management Agent to the selected groups.


➤ Deploying the Management Agent requires device authentication information (user name and password with administrator access). To deploy the Agent to a group, all devices within that group must share the same authentication information.

➤ The Management Agent cannot be remotely deployed to Thin Client devices and must be installed manually using the installation programs included in the `\ThinClient` directory on the HPCAS media.

## Removing the Management Agent from a Group

Use the Agent Removal Wizard to remove the Agent from a group of devices.


To remove the Management Agent from a group of devices

- 1 Select the check box in the first column to choose the groups from which you want to remove the Agent.
- 2 Click the **Remove the Management Agent**  toolbar button to launch the [Agent Removal Wizard](#).
- 3 Follow the steps in [Agent Removal Wizard](#) on page 170 to remove the Management Agent from all devices within the selected Groups.

## Discovering Software/Hardware Inventory for a Group

Use the Software/Hardware Inventory Wizard to discover inventory for a group of devices.

To discover software and hardware inventory for a group of devices

- 1 Select the check box in the first column to select the groups for which you want to discover inventory.
- 2 Click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory** to launch the [Software/Hardware Inventory Wizard](#).
- 3 Follow the steps in [Software/Hardware Inventory Wizard](#) on page 171 to discover inventory for the devices within each selected Group.
- 4 Use the [Reporting](#) tab to view inventory reports for the selected groups.

## Discovering Patch Compliance a Group

Use the Patch Compliance Discovery Wizard to discover patch compliance for a group of devices.

To discover patch compliance for a group of devices

- 1 Select the check box in the first column to select the groups for which you want to target for patch compliance discovery.
- 2 Click the **Inventory Collections**  toolbar button, then select **Discover Patch Compliance** to launch the [Patch Compliance Discovery Wizard](#).
- 3 Follow the steps in [Patch Compliance Discovery Wizard](#) on page 171 to discover and enforce patch compliance for the devices within the selected Groups.



- 4 Use the [Reporting](#) tab to view patch compliance reports for the selected groups.


## Discovering Application Usage Data a Group

Use the [Application Usage Collection Wizard](#) to discover application usage for devices in your HPCAS database. The wizard installs the Collection Agent, which then returns usage data defined by filters you create and enable. Also, if required, usage data can be obfuscated to ensure privacy. See the [Reporting](#) section of the Configuration tab on page 159 for more information.



HP Client Automation Standard is required for collecting application usage data.

### To discover application usage

- 1 Select the check box in the first column to select the groups that you want to target for application usage discovery.
- 2 Click the **Inventory Collections**  toolbar button, and select **Discover Application Usage** to launch the [Application Usage Collection Wizard](#).
- 3 Follow the steps in [Application Usage Collection Wizard](#) on page 172 to discover application usage for the selected groups.
- 4 Use the [Reporting](#) tab to view usage reports for the selected groups.

## Power Management

Use the Power Management wizard to turn on, turn off, or restart a device.


- Select the Group you want to manage and click the **Power Management**  toolbar button to launch the [Power Management Wizard](#).

Follow the steps in [Power Management Wizard](#) on page 173 to create a Power Management job for the selected Group.

## Removing Groups

Use the Groups toolbar to remove groups from HPCAS.

To remove Groups from HPCAS

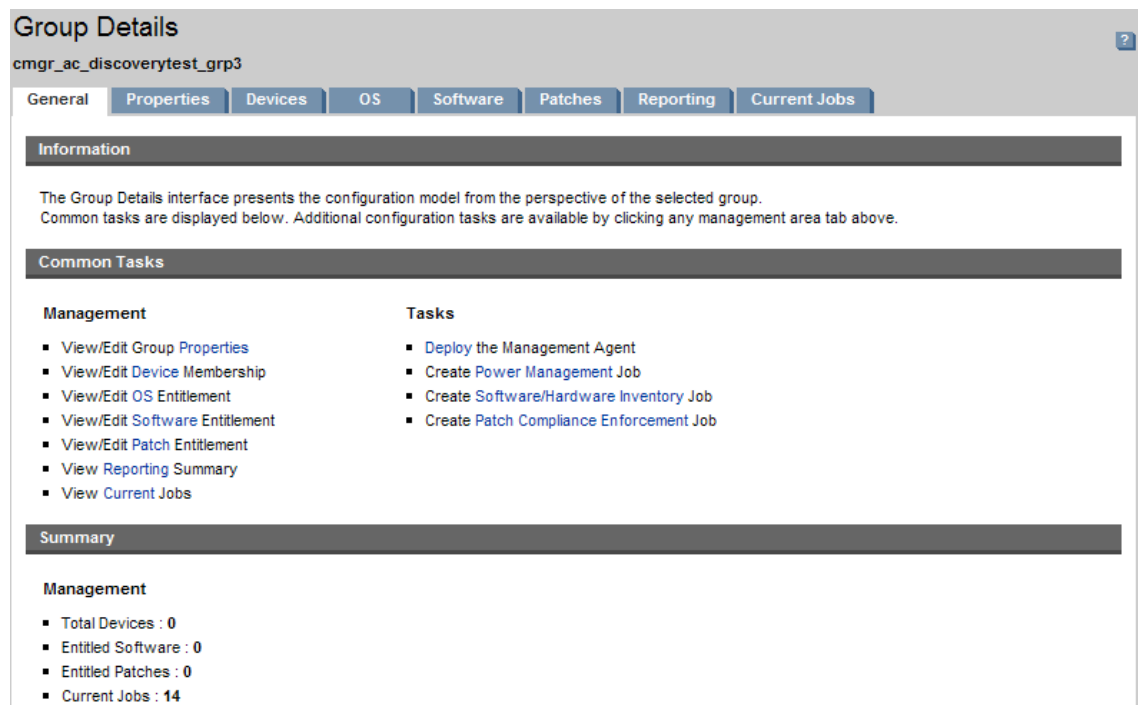
- 1 Select the check box in the first column to select the groups you want to remove.
- 2 Click the **Delete Groups(s)**  toolbar button to remove the Group from HPCAS.

## Group Details

Click any Group name to open the Group Details window. This window presents the configuration model from the perspective of the selected group.

Use the Group Details window to view group properties, view and modify device membership, view or modify entitlements, view a reporting summary, or create group management jobs. The following areas are available:

**Figure 5 Group Details window**



## General

The General tab displays common tasks available for the group. Click any of the other management area tabs to access additional configuration tasks.

## Properties

The Properties tab displays the group type, name and description as well as additional properties for dynamic groups.

### Group Type

**Static:** update device membership manually using the Group Details, Devices section.

**Reporting** and **Discovery:** to update group membership, use the job controls under the Current Jobs tab to run the discovery job.

**Internal:** group membership cannot be altered.

Click **Save** to commit any changes to the Group Properties section.

If you are viewing a dynamic reporting group, you will be able to view the criteria that were used to originally create the group in the **Reporting Filter Criteria** section. This information is read only. If you want to change the criteria, you will need to create a new dynamic reporting group. Note that the filter criteria are only viewable for groups with recurring schedules or a Run After schedule that has not yet run. For groups with Run Once schedules that have already run, “No filter information is available” is displayed.

If you are viewing a dynamic discovery group, you can view the dynamic group properties in the **Discovery Properties** section.

## Devices

Devices listed in the Devices tab are current members of the group.

- You must manually edit device membership of a Static group.
- Use the job controls under the Current Jobs tab to modify the membership refresh schedule for Dynamic Reporting or Discovery groups.


## OS

Operating system images listed in the OS tab are entitled to the group. Use the toolbar buttons to complete group-specific OS entitlement and deployment tasks.

## Software

Software listed in the Software tab is entitled to the group. Adding or removing software entitlements affects all existing device members as well as any devices added to the group in the future.


Use the toolbar buttons to add or remove entitlement, synchronize software, or deploy or remove software from devices in the group.

 Removing a software entitlement does not automatically remove the software from devices in the group. To remove software, select the target devices and use the Remove Software button. After removing the software, you can remove the entitlement to ensure that the software is no longer available.

## Patches

The Patches tab displays all patches entitled to the group.

Use the toolbar buttons to add or remove patch entitlement for the group or to deploy a patch to devices in the group.

 After a patch is deployed it cannot be removed from a device.

## Reporting

The Reporting tab contains summary reports specific to the group. For detailed reports, use the Reporting tab in the main HPCAS console.

## Current Jobs

The Current Jobs tab displays all currently active or scheduled jobs for the group. Use the toolbar buttons to administer any of the available jobs.

## Group Details Window Tasks

Use the Group Details window to complete the following tasks:


- [Adding and Removing Devices from Static Groups](#) on page 77
- [Adding and Removing Software Entitlement from Groups](#) on page 77
- [Deploying, Removing, and Synchronizing Software from Groups](#) on page 78
- [Adding and Removing Patch Entitlement from Groups](#) on page 78

- [Deploying Patches to Groups](#) on page 79


## Adding and Removing Devices from Static Groups

Use the [Group Details](#) window to update static group membership.

To add devices to a static group

- 1 In the Group Details window, click the **Devices** tab.
- 2 Click **Add Device(s)** .
- 3 In the window that opens, select the devices you want to include in the group and click **Add Devices**.


To remove devices from a static group

- 1 In the Group Details window, click the **Devices** tab.
- 2 Select the devices you want to remove from the group and click **Remove Device(s)** .


## Adding and Removing Software Entitlement from Groups

Use the [Group Details](#) window to add or remove software entitlement for devices in a group.

To entitle software to a group

- 1 In the Group Details window, click the **Software** tab.
- 2 Click **Add Entitlement** . The Software Entitlement window opens.
- 3 Select the software you want to entitle to the group and click **Add Entitlement**.

To remove software entitlement from a Group

- 1 In the Group Details window, click the **Software** tab.
- 2 Select the software you want to remove entitlement for from the group, and then click **Remove Entitlement** .


## Deploying, Removing, and Synchronizing Software from Groups

Use the [Group Details](#) window to deploy, remove, or synchronize software for devices in a group.


### To deploy software to a group

- 1 In the Group Details window, click the **Software** tab.
- 2 Select the software you want to deploy and click the **Deploy Software**  toolbar button.
- 3 To deploy the software to the managed devices within the group, follow the steps in [Software Deployment Wizard](#) on page 177.

### To remove software from a group

- 1 In the Group Details window, click the **Software** tab.
- 2 Select the software you want to remove from the managed devices within the group and click the **Remove Software**  toolbar button.
- 3 To remove the software from the managed devices within the group, follow the steps in [Software Removal Wizard](#) on page 182.

### To synchronize software


- 1 In the Group Details window, click the **Software** tab.
- 2 Click the **Synchronize Software**  toolbar button to launch the [Software Synchronization Wizard](#), which will ensure that all entitled software is installed to group members and that any new group members receive entitled software.
- 3 Follow the steps in [Software Synchronization Wizard](#) on page 179 to set a software synchronization schedule for the group.

## Adding and Removing Patch Entitlement from Groups

Use the [Group Details](#) window to add or remove patch entitlement for devices in a group.

### To entitle patches to a group


- 1 In the Group Details window, click the **Patches** tab.

- 2 Click the **Add Entitlement**  toolbar button. The Patch Entitlement window opens.
- 3 Select the patches you want to entitle to the group and click **Add Entitlement**.



Only patches that have not yet been entitled are shown in the Patch Entitlement window. Patches that have already been entitled to the group are not shown.


#### To remove patch entitlement from a group

- 1 In the Group Details window, click the **Patches** tab.
- 2 Select the patches you want to remove entitlement for from the group, then click the **Remove Entitlement**  toolbar button.

## Deploying Patches to Groups

Use the [Group Details](#) window to deploy patches to devices in a group.

#### To deploy patches to a group

- 1 In the Group Details window, click the **Patches** tab.
- 2 Select the patches you want to deploy and click the **Deploy Patches**  toolbar button. The [Patch Deployment Wizard](#) opens.
- 3 Follow the steps in the wizard on page 180 to deploy the patches to the managed devices within the group.



After a patch is deployed, it cannot be removed from a device.

## Current Jobs

Current Jobs displays all active or scheduled Group Management jobs. Group Management jobs target specific groups and are used to administer software to devices in those groups or to refresh the devices in the Dynamic Reporting or Discovery groups that you have created.

Click any column heading to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.

For information about the [Job Controls](#) and [Job Status](#), see [Current Jobs](#) on page 115.

## Past Jobs

Past Jobs displays all completed Group Management jobs. Click the description of any job to display more details about that job's status.



Completed jobs are moved to the Past Jobs list one minute after they are finished.



# Software Management

Use the Software Management section to manage software services and software management jobs. Software is entitled to groups of managed devices then either deployed by the administrator using the HPCAS, or installed by the end user using the Application Self-service Manager.

The Software Management tabs are described in the following sections:

- [General](#) on page 81
- [Software](#) on page 82
- [Current Jobs](#) on page 89
- [Past Jobs](#) on page 89

► HP Client Automation Standard is required to deploy software. With HP Client Automation Starter you can deploy BIOS settings and HP Softpaqs only.

## General

Use the General tab to learn how to publish software, entitle and deploy software to managed devices, view current and past Software Management jobs and view software detail and summary reports.

The Summary section displays how many software services are currently available in the HPCAS database as well as the number of current Software Management jobs.

### To publish software

- Use the Publisher to publish software into HPCAS. Published Software is displayed in the [Software](#) Library.

Install the Publisher on the machine from which you will be selecting and configuring software services. See [Installing the Publisher](#) on page 39 for installation instructions. See Chapter 9, [Using the Publisher](#) for information about how to publish software into HPCAS.

### To entitle and deploy software

- 1 In the Common Tasks area, click **Deploy**. This will launch the [Software Deployment Wizard](#).

- 2 Follow the steps in the wizard on page 177 to entitle and deploy software to managed devices.

## Software

The Software tab displays all software that has been published into HPCAS.

Use the tools provided to refresh software data, deploy software to managed devices, or remove software from the library. You can also import and export software to and from the Software Library.

HPCAS contains the following software services by default:

- **CCM\_PUBLISHER** – HP Client Automation Administrator Publisher. An alternative installation method for the Publisher, use this service to deploy the Publisher to a device from which you will capture and publish software, publish OS images, BIOS settings, or HP Softpaqs.
- **CCM\_TPM\_ENABLEMENT** – TPM Enablement. This service initializes the use and ownership of the TPM chip on compatible HP devices using the settings you configure in the Configuration tab, Hardware Management section. See [Configuring TPM](#) on page 158 for configuration options. Installing this service performs the following tasks:
  - Enables the TPM chip in the BIOS
  - Sets the specified BIOS Administrator password
  - Sets up ownership of TPM and the owner password
  - Initializes the emergency recovery token and path
  - Sets the password reset token and path and the backup archive path

After the TPM Enablement service is deployed, the device is ready for user-level initialization (performed by the end user through the HP ProtectTools Security Manager interface).










In order to enable and initialize the TPM security chip, the HP ProtectTools software must first be installed on the device. Some device models have this software pre-installed while for others you will need to either download or purchase the software separately. For more information, review the HP documentation for your particular device model.

- **CCM\_SMM** – Settings Migration Manager. This service installs the Settings Migration Manager Utility which allows for backup and restore

of user settings on individual devices. See [Settings Migration](#) on page 249 for information on using Settings Migration Manager.

► These default services cannot be deleted from the Software Library.

**Table 4      Software toolbar tasks**

Toolbar Button	Description
	<b>Refresh Data</b> – Refresh the Software Library.
	<b>Export to CSV</b> – create a comma-separated list that you can open or save.
	<b>Deploy Software</b> – Launches the <a href="#">Software Deployment Wizard</a> .
	<b>Add Group Entitlement</b> – Launches the <a href="#">Service Entitlement Wizard</a> .
	<b>Import Service</b> – Launches the <a href="#">Service Import Wizard</a> .
	<b>Export Service</b> – Launches the <a href="#">Service Export Wizard</a> .
	<b>Delete Software</b> – Remove Software from the library.


The following tasks are available from the Software tab.

- [Deploying Software](#) on page 83
- [Adding Group Entitlement](#) on page 84
- [Importing a Service](#) on page 84
- [Exporting a Service](#) on page 85
- [Removing Software from HPCAS](#) on page 85
- [Software Details](#) on page 85

## Deploying Software

Use the Software Deployment Wizard to deploy software to groups or devices.


To entitle and deploy software

- 1 Select the software for deployment and click the **Deploy Software**  toolbar button. This will launch the [Software Deployment Wizard](#).
- 2 Follow the steps in [Software Deployment Wizard](#) on page 177 to entitle and deploy software to managed devices.

## Adding Group Entitlement

Software available in the library can be entitled to groups of devices.

To add group entitlement


- 1 Select the check box in the first column to select the software for group entitlement.
- 2 Click the **Add Group Entitlement**  toolbar button to launch the [Service Entitlement Wizard](#).
- 3 Follow the steps in [Service Entitlement Wizard](#) on page 181 to entitle the selected software to groups of devices that you will select using the wizard.

## Importing a Service

HPCAS can import software services to the Software Library. To import a service, the service import deck must be located within the `ChangeControl` directory on your HPCAS server (C:\Novadigm\ChangeControl, by default).

Importing a service is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to your `ChangeControl` directory on your production HPCAS server. Then use the Import Service wizard to import that service to your production Software Library and deploy the software to managed devices.


To import a service

- 1 Click the **Import Service**  toolbar button to launch the [Service Import Wizard](#).
- 2 Follow the steps in the wizard on page 178 to import the service to the Software Library.

## Exporting a Service

Published software services can be exported to the `ChangeControl` directory on your HPCAS server. Exported services are available for import to any other HPCAS server libraries (within a testing environment, for example).


### To export a service

- 1 Select the check box in the first column to select the software to export as a service.
- 2 Click the **Export Service**  toolbar button to launch the [Service Export Wizard](#).
- 3 Follow the steps in [Service Export Wizard](#) on page 178 to export the service to the `ChangeControl` directory on your HPCAS server machine.

## Removing Software from HPCAS

Use the Software toolbar to remove software from the HPCAS database.

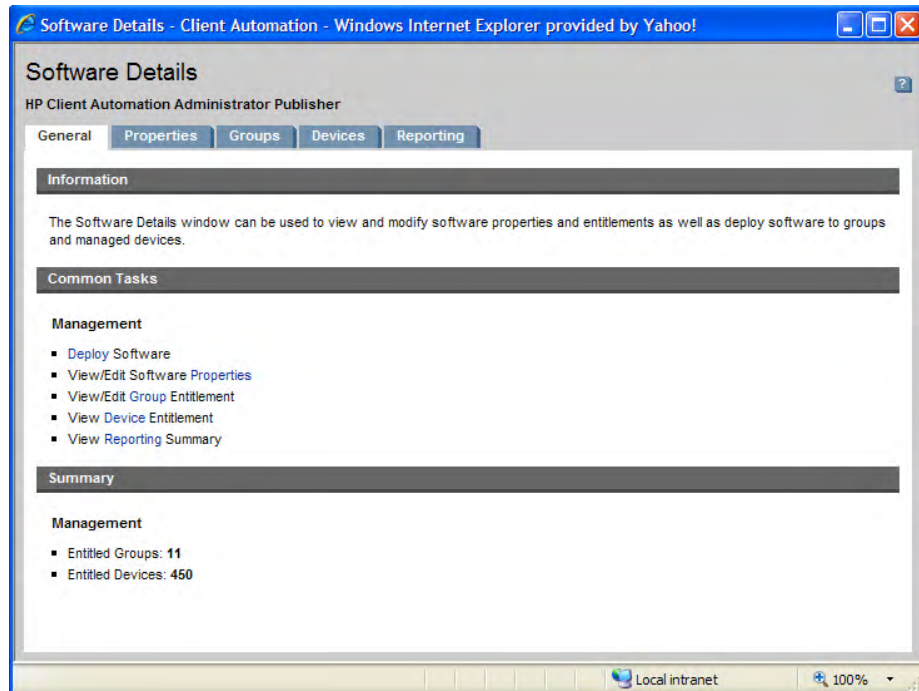
### To remove software from the Software Library

- 1 Select the software you want to remove.
- 2 Click the **Delete Software**  toolbar button.

## Software Details

Click any Software name to open the Software Details window. Use the Software Details window to view software service properties, view or modify entitlements, deploy or remove software, or view a reporting summary.

**Figure 6     Software Details window**



## General

The General tab displays common tasks available for the software. To access more configuration tasks click any of the other management area tabs.

## Properties

Use the Properties tab to change the software details, including the catalog group and administrative functions.

- **Description**  
Enter a detailed description for the software. This is a required field.
- **Software Category**  
Type a category for the software. The Software Category is displayed in the Software Library and is available as a sort option.
- **Catalog Visibility**  
Select whether to display the software in the catalog on the managed

device. Displaying software in the catalog allows the end user to install or remove the software.





- **Reboot Settings**  
Select whether to reboot the managed device after the software is installed, and whether or not to prompt the end user.
- **Author**  
The software author (for example, Hewlett- Packard).
- **Vendor**  
The software vendor (for example, Hewlett- Packard).
- **Web Site**  
The software Web site (for example, **www.hp.com**).
- **Install Command Line**  
Command to run after the software is deployed to a device.
- **Pre-uninstall Command Line**  
Command to run before software is removed from a device. For example, some registry keys may need to be removed prior to running the software removal command.
- **Un-install Command Line**  
Command to run after the software is removed from a device.







Make sure to click **Save** after making any changes to the software details.

## Groups

The Groups tab displays all groups that have been entitled for the selected software. Use the toolbar buttons to alter entitlement or the installed state of the software on managed devices within each group.




- To **entitle** additional groups, click the **Add Software Entitlement**  toolbar button.
- To **remove entitlement** from a group, select the group then click the **Remove Software Entitlement**  toolbar button.
- To **deploy** the selected software to a specific group, select the group and click the **Deploy Software**  toolbar button. This launches the [Software Deployment Wizard](#). Follow the steps in the wizard on page 177 to deploy the selected software.
- To **remove** the software from a specific group, first select the group and click the **Remove Software**  toolbar button. This launches the [Software](#)

**Removal Wizard.** Follow the steps in the wizard on page 182 to remove the software from managed devices within that group.

- To **discover software and hardware inventory** for a group of devices, first select the group, click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory**. This launches the **Software/Hardware Inventory Wizard**. Follow the steps in the wizard on page 171 to discover software and hardware inventory.
- To **discover and enforce patch compliance** for a group of devices, select the group, click the **Inventory Collections**  toolbar button, then select **Discover & Enforce Patch Compliance**. This launches the **Patch Compliance Discovery Wizard**. Follow the steps in the wizard on page 171 to discover and enforce patch compliance.
- To **discover application usage** for a group of devices, select the group, click the **Inventory Collections**  toolbar button then select **Discover Application Usage**. This launches the **Application Usage Collection Wizard**. Follow the steps in the wizard on page 172 to discover application usage data.
- To **turn on, turn off, or reboot** a group of devices select the group, then click the **Power Management**  toolbar button. This launches the **Power Management Wizard**. Follow the steps in the wizard on page 173 to manage the devices.




## Devices

The Devices tab displays all devices that have been entitled for the selected software. Deploy or remove software from a specific device using the toolbar at the top of the list.

- To **deploy** the selected software to a specific device, select the device and click the **Deploy Software**  toolbar button. This launches the **Software Deployment Wizard**. Follow the steps in the wizard on page 177 to deploy the selected software.
- To **remove** the software from a specific device, first select the device and click the **Remove Software**  toolbar button. This launches the **Software Removal Wizard**. Follow the steps in the wizard on page 182 to remove the software from managed devices within that group.
- To **discover software and hardware inventory** for devices, first select the devices, click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory**. This launches the



[Software/Hardware Inventory Wizard](#). Follow the steps in the wizard on page 171 to discover software and hardware inventory.

- To **discover and enforce patch compliance** for devices, select the devices, click the **Inventory Collections**  toolbar button, then select **Discover & Enforce Patch Compliance**. This launches the [Patch Compliance Discovery Wizard](#). Follow the steps in the wizard on page 171 to discover and enforce patch compliance.
- To **discover application usage** for devices, select the devices, click the **Inventory Collections**  toolbar button, then select **Discover Application Usage**. This launches the [Application Usage Collection Wizard](#). Follow the steps in the wizard on page 172 to discover application usage data.
- To **turn on, turn off, or reboot** devices, select the devices then click the **Power Management**  toolbar button. This launches the [Power Management Wizard](#). Follow the steps in the wizard on page 173 to manage the devices.

## Reporting

The Reporting tab contains summary reports specific to the software you are viewing. For detailed reports, use the [Reporting](#) tab in the main HPCAS console.

## Current Jobs

Current Jobs displays all currently active or scheduled Software Management jobs. Software Management jobs are used to entitle and deploy or remove software from managed devices in your HPCAS database.

Click any column heading to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.

For information about the [Job Controls](#) and [Job Status](#), see [Current Jobs](#) on page 115.

## Past Jobs

Past Jobs displays all completed software management jobs.

Click any column heading to change the sort order, or use the navigation buttons at the top of the table to jump to a specific section.



Completed jobs (from the Current Jobs tab) are moved to the Past Jobs list one minute after they are finished.

# Patch Management

Use the Patch Management area to manage patches, HP Softpaqs, and patch management jobs.

Acquired patches and HP Softpaqs are entitled to groups of managed devices, then deployed by the administrator using HPCAS. Also, entitled patches and Softpaqs are deployed automatically based on the compliance schedule you set. See [Patch Management — Configuration](#) on page 151. Softpaqs that are published using the Publisher are contained in the Software Library, while acquired Softpaqs are contained in the Patch Library.

The Patch Management tabs are described in the following sections:

- [General](#) on page 93
- [Patches](#) on page 94
- [Current Jobs](#) on page 99
- [Past Jobs](#) on page 99

► HP Client Automation Standard is required for Microsoft patch management.

## [Microsoft Update Catalog: Minimum OS and Service Pack Requirements](#)

Refer to Microsoft's web site for specific information concerning the minimum operating system and service pack requirements for Microsoft Update Catalog and Windows Update technologies leveraged by HPCAS Patch Management. As of this writing, the supported OS Versions and languages can be viewed from the Microsoft Update Home page at this link:

**<http://update.microsoft.com/microsoftupdate/v6/default.aspx>**

► Windows Installer Version 3.1 is required on Agent machines because newer Microsoft security patches require this to install more recent security patches. For additional information on Windows Installer 3.1, see the following Microsoft article:  
**<http://support.microsoft.com/kb/893803/en-us>**.


## [Important Information about Microsoft Automatic Updates](#)

Automatic Updates is a feature of Windows that enables users to initiate a scan of their system for needed patches. It also allows for the download and

installation of the patches. This feature currently supports the following configuration options:

- 1 Download updates for me, but let me choose when to install them.
- 2 Notify me but don't automatically download or install them.
- 3 Turn off Automatic Updates.

Automatic Updates and HPCAS Patch Management use an underlying Windows component, Windows Update Agent (WUA), to scan a device and install updates. To avoid a problem situation where WUA may be in use by another patch management product, configure Automatic Updates as described below when using Patch Management to distribute and install updates. Microsoft is expected to correct this problem.

 You are strongly advised to use the option **Turn off Automatic Updates**.

Be aware of the consequences associated with each of these options.

If you set Automatic Updates to **Notify me but don't automatically download or install them**, it is imperative that users do not initiate the Automatic Updates download process while the Agent is scanning or installing updates. If the Automatic Updates process is initiated manually, it could result in *either* process failing to download and install updates on the managed device. This behavior is not specific to Patch Management. It is also exhibited when other patch management products attempting to use WUA, and WUA is already in use. At the time of this writing, relevant Microsoft Knowledge Base articles include:

- Microsoft KB Article 910748, <http://support.microsoft.com/kb/910748>
- Microsoft KB Article 931127, <http://support.microsoft.com/kb/931127>
- If you have virus scanners installed and enabled in your enterprise, please see Microsoft KB Article 922358 which documents a need to exclude the folder %Windir%\SoftwareDistribution from virus scans. While this Microsoft document references specific Microsoft patch management technologies, the same Windows Update Agent limitation can occur in an enterprise using HPCAS Patch Management, which leverages Windows Update Agent technologies. Please review Microsoft KB Article 922358, <http://support.microsoft.com/kb/922358>
- If you set Automatic Updates to **Turn off Automatic Updates**, it is possible that you will not be informed of all updates available because HPCAS does not support a product that Automatic Updates does.

WUA uses the Automatic Updates Windows service, which must be set to either **Automatic** or **Manual** on target devices. The Automatic Updates service can be in a stopped state since WUA will start it as needed.

See the following Microsoft articles for more information about Automatic Updates:

*How to configure and use Automatic Updates in Windows XP.* At the time of this writing, the url is <http://support.microsoft.com/kb/306525/>.

*How to configure and use Automatic Updates in Windows 2000.* At the time of this writing, the url is <http://support.microsoft.com/kb/327850/>.

## General

Use the General tab to acquire and deploy patches, view current and completed Patch Management Jobs and view patch compliance detail and summary reports.

The Summary section shows you how many patches are currently available in the HPCAS database and the number of current Patch Management jobs.

Patches and Softpaqs are acquired from HP and Microsoft sources based on information entered in the Configuration section. See [Patch Management — Configuration](#) on page 151 for more information.

### To acquire patches

- 1 In the Common Tasks area click **Acquire**.
- 2 Patches are downloaded and added to the Patch Library. HPCAS will automatically download additional patches according to the acquisition schedule you configured.

Patches are deployed to managed devices from only the HPCAS console, they are not available in the Application Self-service Manager software catalog.

### To deploy patches

- 1 In the Common Tasks area, click **Deploy** Patches to launch the [Patch Deployment Wizard](#).
- 2 Follow the steps in the wizard on page 180 to deploy patches to devices in selected groups.

## Patches

Patches listed in the Patch Library are available for entitlement and deployment to your managed devices. The library contains the acquired patches and Softpaqs based on the acquisition settings you set in the Configuration tab, [Patch Management](#) section.

**Table 5 Patch Library toolbar tasks**

Toolbar Button	Description
	<b>Refresh Data</b> – Refresh the Patch Library.
	<b>Export to CSV</b> – create a comma-separated list that you can open or save..
	<b>Deploy Patches</b> – Launches the <a href="#">Patch Deployment Wizard</a> .
	<b>Add Group Entitlement</b> – Launches the <a href="#">Service Entitlement Wizard</a> .
	<b>Import Service</b> – Launches the <a href="#">Service Import Wizard</a> .
	<b>Export Service</b> – Launches the <a href="#">Service Export Wizard</a> .
	<b>Delete Patch</b> – Remove Patch from the library. When a patch is removed, all entitlements to that patch are also removed (the patch is not removed from devices).


The following tasks are available from the Patches tab.

- [Deploying Patches](#) on page 94
- [Adding Group Entitlement](#) on page 95
- [Importing a Service](#) on page 95
- [Exporting a Service](#) on page 96
- [Patch Details](#) on page 96

## Deploying Patches

Patches available in the Patch library can be deployed to managed devices.


### To deploy patches

- 1 Select the check box in the first column to select the patch for deployment.
- 2 Click the **Deploy Patches**  toolbar button to launch the [Patch Deployment Wizard](#).
- 3 Follow the steps in the wizard on page 180 to deploy patches to devices in managed devices.

## Adding Group Entitlement

Patches available in the Patch library can be entitled to groups of devices. Entitlement can allow patch compliance to be enforced using the schedule configured in the [Patch Deployment Wizard](#).

### To add group entitlement


- 1 Select the check box in the first column to select the patch for group entitlement.
- 2 Click the **Add Group Entitlement**  toolbar button to launch the [Service Entitlement Wizard](#).
- 3 Follow the steps in the wizard on page 181 to entitle the selected patches to groups of devices that you will select using the wizard.

## Importing a Service

HPCAS can import patch services to the Patch Library. To import a service, the service import deck must be located within the `ChangeControl` directory on your HPCAS server (C:\Novadigm\ChangeControl by default).

Importing a service is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to your `ChangeControl` directory on your production HPCAS server. Then use the Import Service wizard to import that service to your production Patch Library and deploy the patch to managed devices.

### To import a service


- 1 Click the **Import Service**  toolbar button to launch the [Service Import Wizard](#).

- 2 Follow the steps in the wizard on page 178 to import the service to the Patch Library.

## Exporting a Service

Published patch services can be exported to the `ChangeControl` directory on your HPCAS server. Exported services are available for import to any other HPCAS server libraries (within a testing environment, for example).

### To export a service

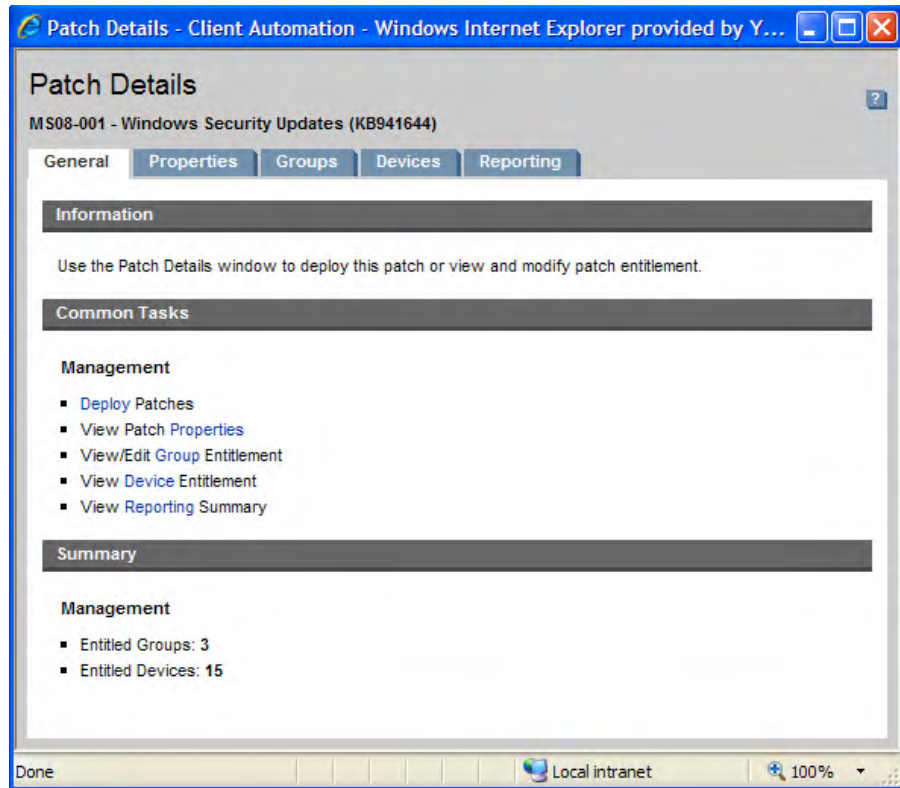
- 1 Select the check box in the first column to select the patch to export as a service
- 2 Click the **Export Service**  toolbar button to launch the [Service Export Wizard](#).
- 3 Follow the steps in the wizard on page 178 to export the service to the `ChangeControl` directory on your HPCAS server machine

## Patch Details

Click any Patch description to open the Patch Details window. Use the Patch Details window to view patch service properties, view and modify entitlements, or view a reporting summary. The following areas are available:



**Figure 7 Patch details window**



### General








The General tab displays common tasks available for the patch service. To access more configuration tasks click any of the other management area tabs.

### Properties

The Properties tab displays the bulletin number, description and type of bulletin, posted and revised dates, and a vendor information link.


### Groups

The Groups tab displays all groups that have been entitled for the selected patch. Use the toolbar buttons to alter entitlement or the installed state of the patch on managed devices within each group.

- To **entitle** additional groups, click **Add Group Entitlement**  toolbar button.
- To **remove entitlement** from a group, select the group then click the **Remove Group Entitlement**  toolbar button.
- To **deploy** the selected patch to a specific group select the group, and then click the **Deploy Patches**  toolbar button. This launches the [Patch Deployment Wizard](#). Follow the steps in the wizard on page 180 to deploy the selected patch.
- To **discover software and hardware inventory** for a group of devices, first select the group, click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory**. This launches the [Software/Hardware Inventory Wizard](#). Follow the steps in the wizard on page 171 to discover software and hardware inventory.
- To **discover and enforce patch compliance** for a group of devices, select the group, click the **Inventory Collections**  toolbar button then select **Discover & Enforce Patch Compliance**. This launches the [Patch Compliance Discovery Wizard](#). Follow the steps in the wizard on page 171 to discover and enforce patch compliance.
- To **discover application usage** for a group of devices, select the group, click the **Inventory Collections**  toolbar button then select **Discover Application Usage**. This launches the [Application Usage Collection Wizard](#). Follow the steps in the wizard on page 172 to discover application usage data.
- To **turn on, turn off, or reboot** a group of devices, select the group then click the **Power Management**  toolbar button. This launches the [Power Management Wizard](#). Follow the steps in the wizard on page 173 to manage the devices.


## Devices

Devices listed in the Devices tab have been entitled to the selected patch. Deploy the patch to a specific device using the toolbar buttons.

- To **deploy** the selected patch to a specific device, select the device and click the **Deploy Patches**  toolbar button. This launches the [Patch Deployment Wizard](#). Follow the steps in the wizard on page 180 to deploy the selected software.



After a patch is deployed it cannot be removed.

- To **discover software and hardware inventory** for devices, first select the devices, click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory**. This launches the [Software/Hardware Inventory Wizard](#). Follow the steps in the wizard on page 171 to discover software and hardware inventory.
- To **discover and enforce patch compliance** for devices, select the devices, click the **Inventory Collections**  toolbar button then select **Discover & Enforce Patch Compliance**. This launches the [Patch Compliance Discovery Wizard](#). Follow the steps in the wizard on page 171 to discover and enforce patch compliance.
- To **discover application usage** for devices, select the devices, click the **Inventory Collections**  toolbar button, then select **Discover Application Usage**. This launches the [Application Usage Collection Wizard](#). Follow the steps in the wizard on page 172 to discover application usage data.
- To **turn on, turn off, or reboot** devices select the devices, then click the **Power Management**  toolbar button. This launches the [Power Management Wizard](#). Follow the steps in the wizard on page 173 to manage the devices.

## Reporting

The Reporting tab contains summary reports specific to the patch you are viewing. For detailed reports, use the [Reporting](#) tab in the main HPCAS console.

## Current Jobs

Patch Management jobs are used to deploy security patches to devices in your environment. Current Jobs shows a list of active or scheduled jobs. Click the description of any job to display more details regarding the job's status.

Use the toolbars to administer currently scheduled or active jobs.

For information about the [Job Controls](#) and [Job Status](#), see [Current Jobs](#) on page 115.

## Past Jobs

Past Jobs displays all completed Patch Management jobs. Click the description of any job to display more details regarding the job's status.



Completed jobs are moved to the Past Jobs list one minute after they are finished.

# OS Management

Use the OS Management section to manage the operating systems (OSs) used by your client devices. The areas in this section allow you to perform tasks such as OS Deployment, Service Import and Export and Entitlement.

The following sections describe each OS Management tab:

- [General](#) on page 101
- [Operating Systems](#) on page 102
- [Current Jobs](#) on page 113
- [Past Jobs](#) on page 114



HP Client Automation Standard is required for OS management.

## General

Use the General tab to find information about publishing operating systems, entitle and deploy operating systems to managed devices, view current and past OS Management jobs, and view operating system detail and summary reports.

The Summary section shows you how many operating system services are currently available in the HPCAS database and the number of current OS Management jobs.

### [To capture and publish OS images](#)

For OS images to be available in the OS Library, they must be published to HPCAS. Use the Image Preparation Wizard to Capture OS images, then use the Publisher to publish them to HPCAS.

- Use the Image Preparation Wizard to prepare and capture OS images. See [Preparing and Capturing OS Images](#) on page 189 or the Image Preparation Wizard online help for image preparation and capture details.
- Use the Publisher to publish operating system images to HPCAS. Published operating system services are displayed in the Operating System tab. See [Using the Publisher](#) on page 213 or the Publisher online help for information about publishing operating systems.

To deploy OS images

- 1 In the Common Tasks area, click **Deploy**. This launches the [OS Deployment Wizard](#).
- 2 Follow the steps in the wizard on page 183 to entitle and deploy an operating system to managed devices.

For additional information about deploying operating systems, including requirements for target devices and deployment scenarios, see [Deploying Operating Systems](#) on page 103.






## Operating Systems


On the Operating Systems tab you can view all available operating systems that have been published into HPCAS.

Use the tools provided to refresh operating system service data, deploy operating systems to managed devices, or remove operating systems from the library. You can also import and export operating system services to and from the Operating System Library.

Newly published services (published within the last seven days) can be recognized by the word ‘new’ in parentheses (*new*) to the right of the description.

**Table 6 OS Library toolbar tasks**

Toolbar Button	Description
	<b>Refresh Data</b> – Refresh the OS Library.
	<b>Export to CSV</b> – create a comma-separated list that you can open or save.
	<b>Deploy Operating System</b> – Launches the <a href="#">OS Deployment Wizard</a> .
	<b>Add Group Entitlement</b> – Launches the <a href="#">Service Entitlement Wizard</a> .
	<b>Import Service</b> – Launches the <a href="#">Service Import Wizard</a> .
	<b>Export Service</b> – Launches the <a href="#">Service Export Wizard</a> .


Toolbar Button	Description
	<b>Delete Operating System</b> – Remove Operating System from the library.

The following tasks are available from the Operating System tab.

- [Deploying Operating Systems](#) below
- [Deploying an OS Image using Local Service Boot \(LSB\)](#) on page 107
- [Deploying an OS Image using PXE](#) on page 108
- [Deploying an OS Image using the Service CD](#) on page 109
- [Adding Group Entitlement](#) on page 110
- [Importing a Service](#) on page 110
- [Exporting a Service](#) on page 111
- [Removing Operating Systems from the Library](#) on page 111
- [OS Details](#) on page 111

## Deploying Operating Systems

To entitle and deploy an operating system

- 1 Select the operating system service to deploy, then click the **Deploy Operating System**  toolbar button. This will launch the [OS Deployment Wizard](#).
- 2 Follow the steps in the wizard on page 183 to entitle and deploy an operating system to managed devices.

Operating systems are deployed in either attended or unattended mode. See the Configuration tab, [OS Management](#) section on page 155 to select the deployment mode.

See the sections below for deployment scenarios and target device requirements for OS deployment.

### Deployment Scenarios

Deploying an operating system to devices in your environment depends on a number of variables. The following table describes multiple OS image

deployment scenarios and instructions for deploying an operating system to those devices.

**Table 7      OS Deployment Scenarios**

Device State	Instructions for deployment
Managed (Agent installed)	<p>If the device is already managed:</p> <ul style="list-style-type: none"><li>• Add the device to a group.</li><li>• Entitle an operating system to the group (if not already entitled).</li><li>• Deploy the OS using the OS Deployment Wizard.</li></ul> <p>Note: If you use LSB during the OS deployment process, you will not need to make preparations for PXE or the Service CD.</p>
Un-managed (Agent not installed)	<p>If the unmanaged device has an OS installed:</p> <ul style="list-style-type: none"><li>• Deploy the Management Agent to the device.</li><li>• See instructions for Managed device above.</li></ul> <p>If unmanaged device does <i>not</i> have an OS installed:</p> <ul style="list-style-type: none"><li>• See the instructions below for deploying an OS to a bare-metal device.</li></ul>



Device State	Instructions for deployment
Bare-metal (no OS installed)	<p>If the device was previously managed (for hard drive recovery, for example):</p> <ul style="list-style-type: none"> <li>• Group membership and any OS entitlement should still be valid. Deploy the OS using PXE or the Service CD.</li> </ul> <p>If the device was not previously managed:</p> <ul style="list-style-type: none"> <li>• Boot the device with PXE or the Service CD.</li> <li>• A device is added to HPCAS using a variation on the MAC address as device name.</li> <li>• Add the new device to a group with OS entitlement.</li> </ul> <p>Note: If an OS is attached to the All Devices group, the OS is installed automatically. If multiple OSs are attached to All Devices, then a choice of OS to install is presented.</p> <ul style="list-style-type: none"> <li>• The device is rebooted and the Service CD or PXE will continue with the OS deployment.</li> </ul> <p>Note: LSB cannot be used for deploying an OS to a bare-metal device.</p>

### Requirements for Target Devices

The target device is a workstation on which you want to install, replace, or update an operating system. The following requirements must be met.:

- Must meet the minimum hardware and BIOS requirements published by Microsoft (for Windows operating systems) or the machine manufacturer for running the OS to be deployed by HPCAS.
- Target devices must be able to contact a DHCP server and obtain an IP address.
- If you want to report on, or make use of the machine'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 machine will be the MAC address.
- Have an English, French, or German keyboard.
- Have 128 MB of RAM or more.

- 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. Some network cards are PXE-capable, but only actually support PXE with the addition of a network boot ROM. These cards must have the network boot ROM installed. Some older 3Com cards require a firmware upgrade to MBA 4.3 and PXE stack version 2.2.
  - Be sure that the target devices have the same or a compatible HAL (Hardware Abstraction Layer) as the reference machine in order to use Microsoft Sysprep. Machines with the same version of HAL.DLL share the same Hardware Abstraction Layer. For more information on determining a machine's HAL, see:

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

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

- Must have an IDE or SCSI (Adaptec only) boot drive interface.
- Match the reference machine's ACPI characteristics (i.e., ACPI vs. non-ACPI, which is represented in the HAL) and boot drive interface.
- Be compatible with the programmable interrupt controller capabilities represented in the HAL captured on the reference machine (i.e., an Advanced Programmable Interrupt Controller (APIC) HAL will not run on a machine that does not have an APIC; however a PIC (standard on-board Programmable Interrupt Controller) HAL will run on a machine that has an APIC). Newer HP/Compaq computers often come with an APIC.
- Support NTFS and FAT32 file systems.
- Windows XPe and CE images can be deployed to target machines with flash drives of equal or greater size. For example, an image that is 256 MB can be deployed to target devices of 256 or 512 MB.
- Embedded Linux images can be deployed only to target machines with flash drives of equal size. For example, an image that is 256 MB can be deployed only to target devices that have a flash drive of 256 MB.



Deploying an OS image will in some cases overwrite existing data depending on the number of hard drives and partitions on the target device. The following scenarios describe which partitions are affected and which are left intact during the re-imaging process:

**1 HDD with 2 partitions:**

- The boot partition is re-imaged. Second partition remains intact.

**1 HDD with 1 partition:**

- The hard drive is re-imaged. All existing data is overwritten.

**2 HDDs with 1 partition each:**

- First hard drive is re-imaged. All existing data on first hard drive is overwritten. Second hard drive remains intact.

**2 HDDs with 2 partitions each:**

- First hard drive boot partition is re-imaged. Second partition and second hard drive remain intact.

### Deploying thin client factory images

If you are deploying a factory image of a supported thin client operating system, Windows XP Embedded (XPe), Windows CE, or Embedded Linux, note the following:

- After the image is deployed to the device, you must install the Management Agent to begin managing the device. See [Installing the Management Agent on Thin Clients](#) on page 41 for installation instructions.


### Deploying an OS Image using Local Service Boot (LSB)

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

When using Local Service Boot, 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.

See [Deployment Scenarios](#) on page 103 for prerequisite instructions for OS deployment.

### To deploy an OS image using Local Service Boot

- 1 Select the image for deployment and click the **Deploy Operating System**  toolbar button to launch the [OS Deployment Wizard](#).
- 2 Follow the steps in the wizard, and when prompted for deployment method, select **Local Service Boot (LSB)**.
- 3 This will install the LSB software to the target device which in turn will install the OS you selected. If multiple OS images are entitled to the device, you will be prompted to select which OS to install.

### Deploying an OS Image using PXE

The PXE-based environment allows HPCAS to assume management of the OS on target devices that are booted from the network. See [Deployment Scenarios](#) on page 103 for prerequisite instructions for OS deployment.


Using PXE consists of configuring your DHCP server to provide clients booting from the network a boot image and a TFTP server that will supply these files.

- A DHCP server and TFTP server must be configured prior to using PXE for OS deployment. Refer to the product documentation for configuration instructions. See [Configuring PXE for OS Deployment](#) on page 44 for more information.

When PXE is configured, make sure your target devices boot from the network or have PXE-enabled as the primary boot device. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can hit ESC during the reboot process and change the boot order in the configuration settings).

Now you are ready to deploy an OS image.

### To deploy an OS image using PXE

- 1 Make sure PXE is configured.
- 2 Select the image for deployment and click the **Deploy Operating System**  toolbar button to launch the [OS Deployment Wizard](#).
- 3 Follow the steps in the wizard on page 183, and when prompted for deployment method, select **Local CD or PXE Server**.

When the wizard finishes, the target device is rebooted using the settings you defined on your DHCP server.

The OS image is then deployed and installed on the target device (If multiple OS images are entitled to the device, you will be prompted to select the OS to install).

## Deploying an OS Image using the Service CD

The Service CD is used to locally boot a target device that does not already have an operating system installed (a bare-metal machine).

Use `ImageDeploy.iso` to create the Service CD. This file is located on the HPCAS media in the `\OSManagement\ISO\DeploymentCD\` directory.

Since LSB cannot be used for devices that do not already have an OS installed, you must use either the Service CD or a PXE server to boot a bare-metal machine to allow for OS deployment.


The Service CD must be created and available locally at the target device.

See [Deployment Scenarios](#) on page 103 for prerequisite instructions for OS deployment.

### To deploy an OS image using the Service CD

- 1 Insert the Service CD in the target device and boot off of the CD.
- 2 When prompted, enter your HPCAS server IP address or hostname and port number, then press **Enter** to continue. For example, `HPCAS.acmecorp.com:3469` or `192.168.1.100:3469`. Port 3469 is reserved for OS imaging and deployment.

The device connects to the HPCAS server and is added to the [Devices](#) list using a variation on the MAC address as the device name. After the Service CD connects to the HPCAS server, a message is displayed: “This machine has no local OS or the OS is invalid” and “The machine cannot be used and will be shut down until an administrator specifies Policy and performs a Wake on LAN.”


- 3 At the HPCAS console, use the [OS Management](#) section to add the new device to a group.
- 4 In the OS Management section, select the image for deployment and click the **Deploy Operating System**  toolbar button to launch the [OS Deployment Wizard](#).
- 5 Follow the steps in the wizard, and when prompted for deployment method, select **Local CD or PXE Server**.

- 6 After the wizard completes, reboot the target device again using the Service CD. During this reboot, the OS image is detected and deployed. This can take 10 to 15 minutes depending on the size of the image and network bandwidth (if multiple OS images are entitled to the device, you will be prompted to select the OS to install).
- 7 When the image is finished deploying, the target device reboots and starts Windows. The Sysprep process will start and initialize the new image.

## Adding Group Entitlement

OS images available in the OS library can be entitled to groups of devices.

### To add group entitlement


- 1 Select the check box in the first column to select the OS image for group entitlement.
- 2 Click the **Add Group Entitlement**  toolbar button to launch the [Service Entitlement Wizard](#).
- 3 Follow the steps in the wizard on page 181 to entitle the selected images to groups of devices that you will select using the wizard.

## Importing a Service

HPCAS can import OS services to the OS Library. To import a service, the service import deck must be located within the `ChangeControl` directory on your HPCAS server.

Importing a service is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to your `ChangeControl` directory on your production HPCAS server. Then use the Import Service wizard to import that service to your production Software Library and deploy the software to managed devices.


### To import a service

- 1 Click the **Import Service**  toolbar button to launch the [Service Import Wizard](#).
- 2 Follow the steps in the wizard on page 178 to import the service to the OS Library.

## Exporting a Service

Published OS image services can be exported to the `ChangeControl` directory on your HPCAS server. Exported services are available for import to any other HPCAS server libraries (within a testing environment, for example).


### To export a service

- 1 Select the check box in the first column to select the OS image to export as a service
- 2 Click the **Export Service**  toolbar button to launch the [Service Export Wizard](#).
- 3 Follow the steps in the wizard on page 178 to export the service to the `ChangeControl` directory on your HPCAS server machine

## Removing Operating Systems from the Library

Use the OS toolbar to remove software from the HPCAS database.

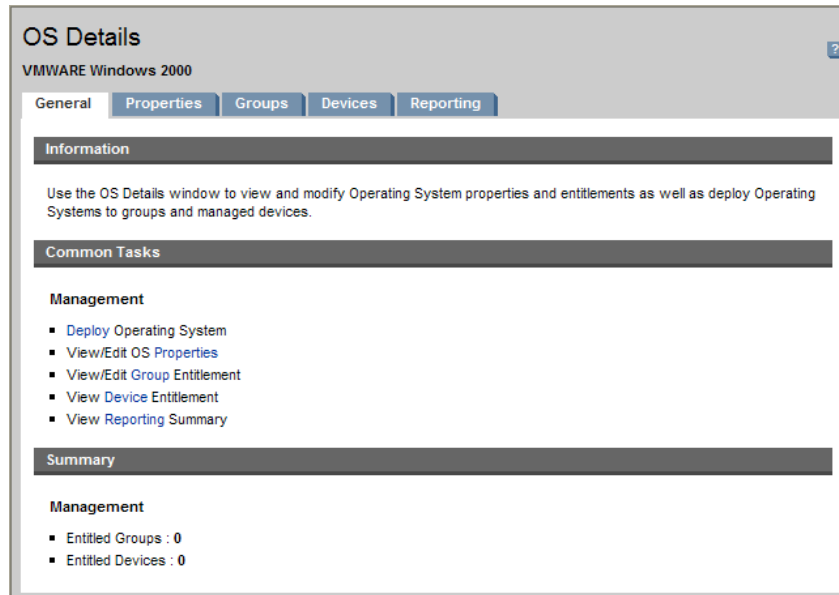
### To remove an operating system service from the Operating System Library

- 1 Select the OS you want to remove.
- 2 Click the **Delete Operating System**  toolbar button.

## OS Details

Click any operating system service details link to open the Operating System Details window. Use the OS Details window to view OS properties, view or modify entitlements, view a reporting summary, or create OS management jobs. The following areas are available:

**Figure 8 OS Details window**



The following areas are available within the details window:

### General

The General tab displays common tasks available for the OS service. To access more configuration tasks click any of the other management area tabs.

### Properties

Use the Properties tab to change the operating system service details.




- **Description**  
The description displayed for the operating system service. This field is required.
- **Contact**  
Optional field to store contact information for this OS service.
- **Web Site**  
Optional field for a URL related to this service.

Click **Save** to commit any changes you make.




## Groups

Groups in the Groups tab have been entitled to the operating system. Use the toolbar to manage entitlement, deploy the OS, discover software and hardware inventory or discover and enforce patch compliance for the groups listed.

- To **entitle** additional groups, click the **Add Group Entitlement**  toolbar button.
- To **remove entitlement** from a group, select the group then click the **Remove Group Entitlement**  toolbar button.
- To **deploy** the operating system to a specific group, select the group and click the **Deploy Operating System**  toolbar button. This launches the [OS Deployment Wizard](#). Follow the steps in the wizard on page 183 to deploy the selected OS.

## Devices

Devices in the Devices tab have been entitled to the operating system. Deploy the OS to a specific device using the toolbar.

- To **deploy** the operating system to a specific device, select the device and click the **Deploy Operating System**  toolbar button. This launches the [OS Deployment Wizard](#). Follow the steps in the wizard on page 183 to deploy the selected OS.

## Reporting

The Reporting tab contains summary reports specific to the operating system service. For detailed reports, use the Reporting tab in the main HPCAS console.

## Current Jobs

Current Jobs shows all currently active or scheduled OS Management jobs. OS Management jobs are used to entitle and deploy operating systems services from managed devices in your HPCAS database.

Click any column heading to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.

For information about the [Job Controls](#) and [Job Status](#), see [Current Jobs](#) on page 115.

## Past Jobs

Past Jobs shows all completed OS Management jobs.

Click any column heading to change the sort order or use the navigation buttons at the top of the table to jump to a specific section.



Completed jobs (from the Current Jobs tab) are moved to the Past Jobs list one minute after they are finished.

# Job Management

Use the Job Management section to view or manage all current and past jobs. The summary information shows the total number of all currently active and scheduled management jobs.

The Job Management tabs are described in the following sections:

- [General](#) on page 115
- [Current Jobs](#) on page 115
- [Past Jobs](#) on page 119

## General

Use the General tab to view all current and past jobs and the total number of all active and scheduled jobs.

## Current Jobs

Current Jobs shows a list of all active or scheduled jobs. Click the description of any job to show more details about the job's status.


Use the toolbar buttons to administer currently scheduled or active jobs. The following sections describe the available job controls and detail window.








- [Job Controls](#) on page 115
- [Job Status](#) on page 116
- [Job Details](#) on page 118

## Job Controls

Use the job controls located at the top of the job list table to manage any existing jobs. See the table below for information about each control.

**Table 8      Job Controls**










Icon	Description
	<b>Refresh Data</b> – Refresh the OS Library.

Icon	Description
	<b>Export to CSV</b> – create a comma-separated list that you can open or save.
	<b>Start Job(s).</b>
	<b>Resume Job(s)</b> that were Disabled or Paused.
	<b>Pause Job(s)</b> that are Currently Active, Waiting to Start, or Waiting to Stop. Job status is set to Paused.
	<b>Stop Job(s)</b> that are currently Active or Paused. Job status is set to Waiting to Stop.
	<b>Reschedule Job(s).</b>
	<b>Delete Job(s).</b>

## Job Status















View the Status column for information about each job. The following table describes the individual job status messages.

**Table 9 Job Status**

Icon	Status	Description
	Ended with Errors	Job completed but with errors. Click the job description for more information.
	Successful	Job completed successfully without errors.
	Currently Active	Job is currently running.
	Paused	Job is currently paused.
	Waiting to Start	Job is scheduled and waiting to run.
	Waiting to Stop	Job is currently stopping.
	Failed	Job did not complete successfully.
	Disabled	Job has been stopped or paused.
	Hibernation	Target device is offline. Job will resume when device is back online.

When using the job controls to manage each job, consult the following table to review expected results.

**Table 10 Job Status and expected Job Control action**

	 Start	 Resume	 Pause	 Stop	 Reschedule	 Delete
 Ended with Errors	Status changed to Currently Active	N/A	Status changed to Disabled	N/A	Updates applied	Job is deleted
 Successful	Status changed to Currently Active	N/A	Status changed to Disabled	N/A	Updates applied	Job is deleted
 Currently Active	N/A	N/A	Status changed to paused	Status changed to Waiting to Stop	Updates applied	N/A
 Paused	N/A	Status changed to pre-paused state	N/A	Status changed to Waiting to Stop	Updates applied	N/A
 Waiting to Start	Status changed to Currently Active	N/A	Status changed to Disabled	N/A	Updates applied	Job is deleted
 Waiting to Stop	N/A	N/A	Status changed to paused	N/A	Updates applied	N/A
 Failed	Status changed to Currently Active	N/A	Status changed to Disabled	N/A	Updates applied	Job is deleted
 Disabled	N/A	Status changed to pre-disabled state	N/A	N/A	Updates applied	Job is deleted

Job controls are available only for jobs in the Current Jobs tabs, this includes currently active jobs and jobs with recurring schedules. Completed jobs in the Past Jobs tab cannot be controlled and should be re-created if you need to run them again.

For more detailed information about a job, click the link in the Description column. This will open a new window displaying the specific [Job Details](#).

▶ When a job is paused, the job action (deployment, collection, etc.) will continue for any currently targeted devices. When the action is complete, the job will not continue executing on additional devices until it is resumed.

## Job Details

Click any job description link to open a new window displaying the specific information for that job. Depending on the Job type, the Job Details window may contain some of the tabs described below.

**Figure 9 Job Details window**

Job Details

10013 - Power On for 4 Device(s)

Details

Targets

Services

Information

Job details for the selected job are displayed below. Detailed information is not available until a job has started.

Job Details

Search:

Any

Contains

Search

Reset

10 items

1 - 4 of 4 items

ID	Device	IP Address	Status	Message	Code	Create Time	Start Time	End Time
10016	cmgr_ac_powertest_dev1		Finished		Notready	2006-02-27 08:46:32	2006-02-27 08:46:33	2006-02-27 08:46:34
10017	cmgr_ac_powertest_dev2		Finished		Notready	2006-02-27 08:46:32	2006-02-27 08:46:33	2006-02-27 08:46:34
10018	cmgr_ac_powertest_dev3		Finished		Notready	2006-02-27 08:46:32	2006-02-27 08:46:33	2006-02-27 08:46:34
10019	cmgr_ac_powertest_dev4		Finished		Notready	2006-02-27 08:46:32	2006-02-27 08:46:33	2006-02-27 08:46:34

### Details

The details tab displays all job information.

### Targets

The Targets tab lists all devices for which the job was created.

### Services

The Services tab displays all software, patches, or operating systems intended for target devices for that job.

See [Troubleshooting](#) on page 297 for some additional information about Job messages.

## Past Jobs

Past Jobs shows all completed Management jobs. Click the description of any job to open the [Job Details](#) window to learn more about the job's status.



Completed jobs are moved to the Past Jobs list one minute after they are finished.



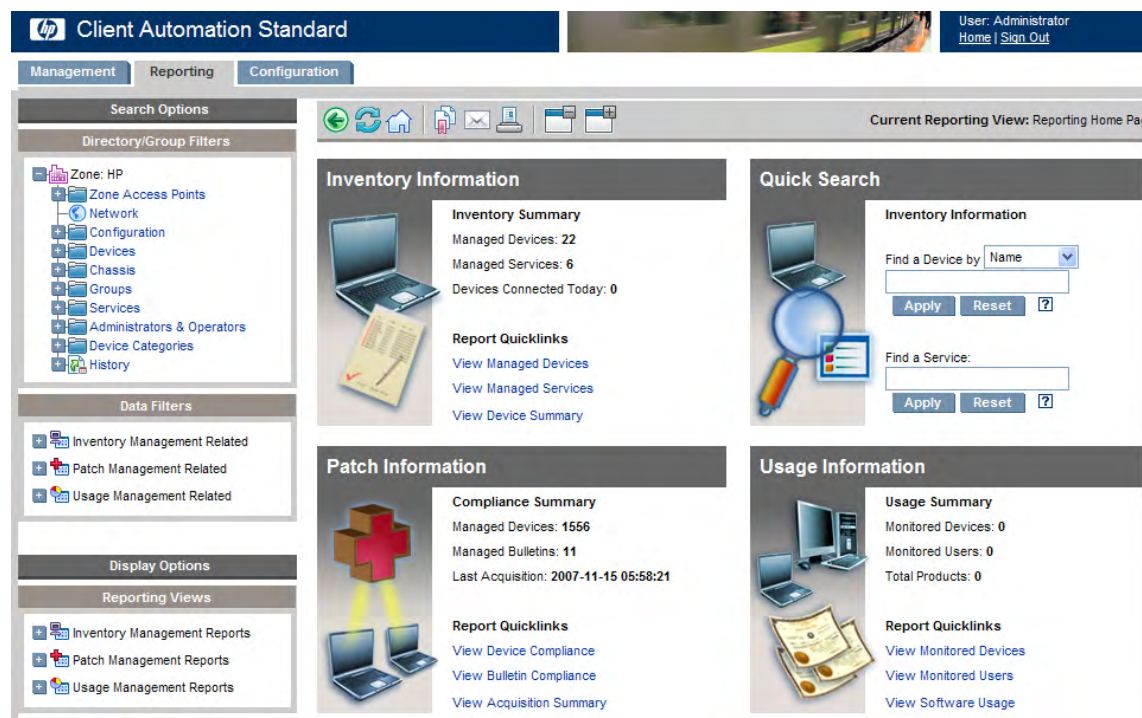


## 5 Reporting

Use the Reporting interface to configure and view detailed reports about the devices and software in your environment. The Reporting interface contains the following areas:

- [Search Options](#) on page 122
- [Display Options](#) on page 122
- [Search Criteria](#) on page 123
- [Report Windows](#) on page 123

**Figure 10** Reporting interface





In order to view the Reporting section's graphical reports, Java Runtime or Virtual Java Machine is required. For more information, go to **<http://java.com/en/index.jsp>**.

## Search Options

Use the Directory/Group Filters or Data Filters area to apply one or more filters to the dataset being accessed for the current view. Any filters you apply are listed as [Search Criteria](#) above the reports.

### Directory/Group Filters

- Click a Directory/Group entry to filter the current dataset to that level. See [Using Search Options to Select Filters](#) on page 124 for details on how to use this area.

### Data Filters

- Use this area to generate or select a filter to be applied to the current dataset. See [Using Search Options to Select Filters](#) on page 124 for details on how to use this area.

## Display Options

Use the Display Options area to control your current session and display.

### Reporting Views

- A Reporting View defines the set of reporting windows to display for the current dataset and initial settings related to each window (such as minimized or maximized, and the number of items per window). When you first access the Reporting Server, the Default View is applied. The current view is listed on the right of the Global Toolbar.

Use the Reporting Views area to change or customize your Reporting View. For details see [Using Display Options to Select Reporting Views](#) on page 127.

## Search Criteria

The Search Criteria list is shown above the report windows and lists the filters that have been applied to the dataset using one of the Search Controls.

- To remove a filter, click the **X** to the left of a filter name in the Search Criteria list.

### Device Filters



Device Filters apply to any report that contains device-related information.

### Report Specific Filters

Report Specific Filters are filters that apply only to data available within a specific Reporting View. For example, if you have applied a Usage by Device, Usage Manager Related Filter, displayed the Usage by Product data, then selected an individual product name, a Report Specific filter is applied to that report based on the criteria you selected.


## Report Windows

Report Windows display the current View.

- Click minimize  on the Window title bar to collapse a report window.
- Click maximize  on the Window title bar to expand a report window.

See [About Reporting Windows](#) on page 132 for details about using the Report Window Action Bar icons, as well as browsing, sorting, and viewing details for the items in a report.

Each window contains an **Action Bar** that includes tools that, depending on the current Report Window, allow you to create groups of devices, create CSV files, create a Web query list, or switch to a graphical view. See [Using the Windows Action Bar](#) on page 133 for more information.

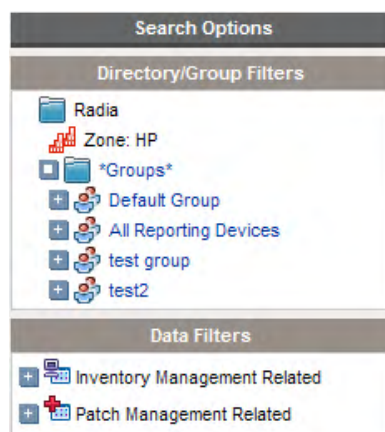
 HPCAS reports are displayed in GMT time zone.

# Using Search Options to Select Filters

The Search Options area gives you two ways to filter datasets within the Reporting Server. You can:

- Select a group entry from the Directory/Group Filter area. This limits the results to the group entry level.
- Use the Data Filter area to create or apply a filter. This limits the results to the specific filter you applied.

**Figure 11 Search Options area**



When you select a Directory/Group Filter or apply a Data Filter, your filter is automatically listed as a Search Criteria entry.

The following sections describe the Search Options areas.

- [The Directory/Group Filters Area](#) on page 124
- [The Data Filters Area](#) on page 125

## The Directory/Group Filters Area

Use the Directory/Group Filter to browse to a group. As you click a group entry, HPCAS automatically filters the reporting data displayed for that entry. For example, if you click the **Sales** group entry, the reporting area displays only the devices that are associated with the Sales group.

Click any image within the Directory/Group Filters area to drill down further into the group. Clicking any text will apply the associated filter to your data.

When you expand the tree view in the Directory/Group Filters area, the expanded branch becomes the root branch.

## The Data Filters Area

The **Data Filters** area is always available as a Search Control (along the left side of the window). Use it to select a filter to apply to the current dataset. When a filter is applied, it is added to the Search Criteria list above the report windows.

To select and apply a filter using the Data Filters area

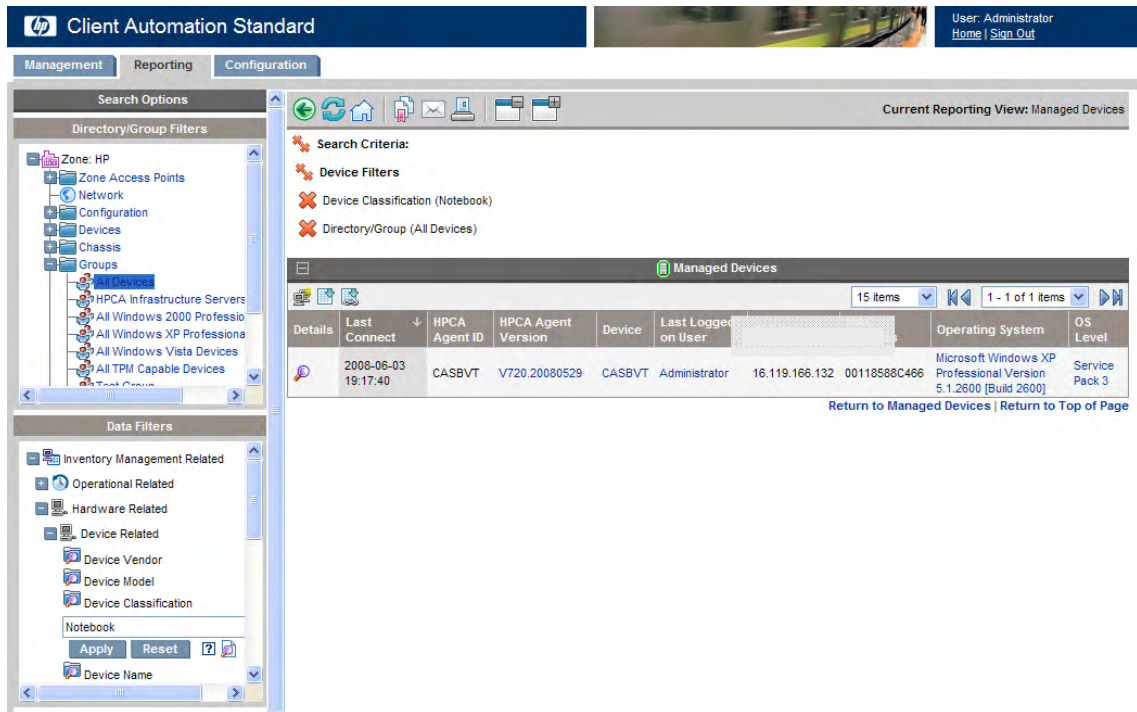
- 1 In the Data Filters area, expand a Filter Group to display the tree-view and select a sub-group. For this example, select **Inventory Management Related** then **Hardware Related**.
- 2 In the tree-view, select a filter. For this example, select, **Device Related** then **Device Classification**.
- 3 In the Filter Value text box, type a specific value. For example, **\*Notebook\***. You can use wildcards, including \* for multiple characters, or ? or \_ (underscore) for single characters.
- 4 Click **Apply** to add the filter to the report. After applying the filter, you will see it added to the Search Criteria list above the report windows.



The Reset button clears the Filter Value field and resets the Filter Group and Filter selections to their default values.

**Figure 12** on page 126 displays an example of the Data Filter entries used to limit the report to only Notebook devices.

**Figure 12 Applying a search criterion to limit report to Notebook Devices**



### Special Filter Value Characters and Wildcards

Finding the right records can be made easier by using special characters and wildcards in your search strings. Use these special characters in conjunction with the text you enter in the Filter Value text box. The following table explains each special character.

**Table 11 Special Characters and Wildcards**

Character	Description
* or %	Return all records of specific text string. Example: Device Vendor Filter HP* returns all HP records. %HP% returns all records including HP.

Character	Description
? or _	Return any single character Example: Device Classification Filter Not?book returns all records beginning with 'Not' and ending with 'book'. Note_ook returns all records beginning with 'Note' and ending with 'ook'.
!	Negates filter. The ! must be placed before the text string. Example: Device Vendor Filter !HP* will return all non-HP records.

## Using Display Options to Select Reporting Views

Within the Display Options area, Reporting Views specify which windows should be displayed on the report page, as well as their initial state (maximized or minimized).

**Figure 13 Display Options area**




To apply a View

- 1 In the Reporting Views area, expand a View Group list and select a group. **Inventory Management Reports, Software Reports** is expanded in the figure on page 128.
- 2 Next, select a view for that group. The following figure on page 128 shows the available report views for **Managed Service Reports**.

When the view is selected, the appropriate report is displayed.

**Figure 14 Sample Selections for Software Reports**



Use the back button  to return to any of the previous reporting windows.

The following sections describe Reporting Views in more detail:

- [Reporting View Types](#) on page 128
- [Viewing HP Hardware Reports](#) on page 131

## Reporting View Types

Depending on the type of data you want to view, select the appropriate Reporting View.

- [Inventory Management Reports](#) on page 129
- [Patch Management Reports](#) on page 130
- [Usage Manager Reports](#) on page 130



HPCAS reports are displayed in GMT time zone.



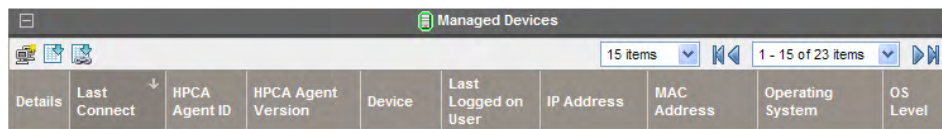
## Inventory Management Reports

Inventory Management Reports display hardware and software information for all devices in HPCAS. This includes reports for HP specific hardware, detailed and summary device components, blade servers, TPM Chipset and SMBIOS information, and Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) Alerts.

Expand the Inventory Management Reports reporting view to see the report options. Note that certain data, like S.M.A.R.T Alerts and HP Specific Reports are only available after HPCAS components are configured. Refer to the [Hardware Management](#) section on page 156 for configuration details.

A typical report on Managed Devices includes the following table headings, illustrated in the screen capture, below.

**Figure 15 Typical Column Headings for Managed Devices Report**



The screenshot shows a web application window titled "Managed Devices". Below the title bar is a toolbar with icons for search, refresh, and other functions. To the right of the toolbar, there are two dropdown menus: "15 items" and "1 - 15 of 23 items". Below these is a table with ten columns. The first column is "Details" with a downward arrow. The other columns are "Last Connect", "HPCA Agent ID", "HPCA Agent Version", "Device", "Last Logged on User", "IP Address", "MAC Address", "Operating System", and "OS Level".

Details	Last Connect	HPCA Agent ID	HPCA Agent Version	Device	Last Logged on User	IP Address	MAC Address	Operating System	OS Level
---------	--------------	---------------	--------------------	--------	---------------------	------------	-------------	------------------	----------

- **Details** – opens a Device Summary page.
- **Last Connect** – displays when the device last connected.
- **HPCA Agent ID** – displays the device name.
- **HPCA Agent Version** – shows the currently installed Management Agent version.
- **Device** – also displays the device name.
- **Last Logged on User** – displays the last user account used to log on to the device. If multiple users are logged on, only the last to log on is recorded—switching between currently logged on users does not affect this.
- **IP Address** – shows the device IP address.
- **MAC Address** – shows the device MAC address.
- **Operating System** – describes the operating system installed on the device.
- **OS Level** – current operating system level (Service Pack 2, for example).

## Patch Management Reports

Patch Management Reports display patch compliance information for managed devices and acquisition information for patches and Softpaqs.

- **Compliance Reports** – The Management Agent sends product and patch information to HPCAS. This information is compared to the available patches to see if managed devices require certain patches to remove vulnerabilities. Compliance reports show only the information applicable to detected devices in your environment.
- **Patch Acquisition Reports** – Acquisition-based reports show the success and failures of the patch acquisition process from the vendor's web site.
- **Research Reports** – Research-based reports display information about the patches acquired from the software vendor's web site. Research-based reports offer a Filter bar.

## Usage Manager Reports

Usage Manager Reports show usage information for devices that have the Usage Collection Agent installed. Use the [Application Usage Collection Wizard](#) to install the collection agent and begin collecting usage data.

- **Device Reports** – Display collected usage information by the individual devices or users.
- **Monthly Usage Reports** – Display usage information by vendor, product, or application.

Usage Management Reports may contain some of the following data columns:

- **Usage Time** – the amount of time an application is running.
- **Focus Time** – the amount of time an application is the active window.
- **Usage Count** – tracks the number of times an application is run on a user's device.
- **Usage Status** – represents the relation of Used versus Unused instances for an individual application or a group of applications.

► After the Collection Agent is deployed, Usage Time collection begins right away. Focus Time collection does not begin until the next time the user logs on.

- Most logical folders, Program Files, for example, are machine-related and not associated with an individual user. Therefore, Usage Management Reports, Device Reports, Usage by User report may contain [undefined] in the User Name column.

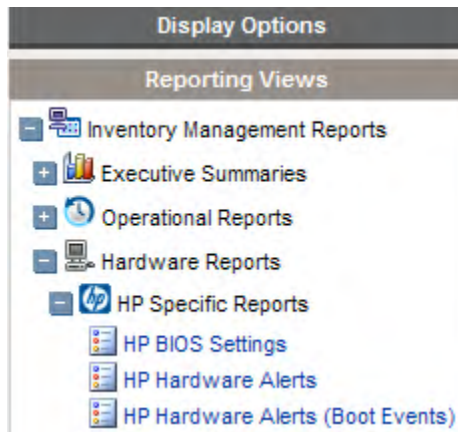
Depending on the Usage Settings defined in the Configuration tab, Reporting section, some or all usage data may be obfuscated.

## Viewing HP Hardware Reports


Use the Display Options to show HP Hardware reports. These reports contain simple alert information captured by HP Client Management Interface (CMI) on compatible, HP devices.

To display HP Hardware reports


- 1 In the Display Options area, select **Inventory Management Reports**.
- 2 Select **Hardware Reports**.
- 3 Select **HP Specific Reports**.



- 4 Select the HP-specific hardware reporting view. The report is displayed in the right pane.
- 5 To search for a specific alert type or bios setting (based on the report view you chose) use the additional data filter search box displayed at the top of the report window.

Data Filters							
Hardware Alert Name				<input type="text"/>			
				Apply		Reset	

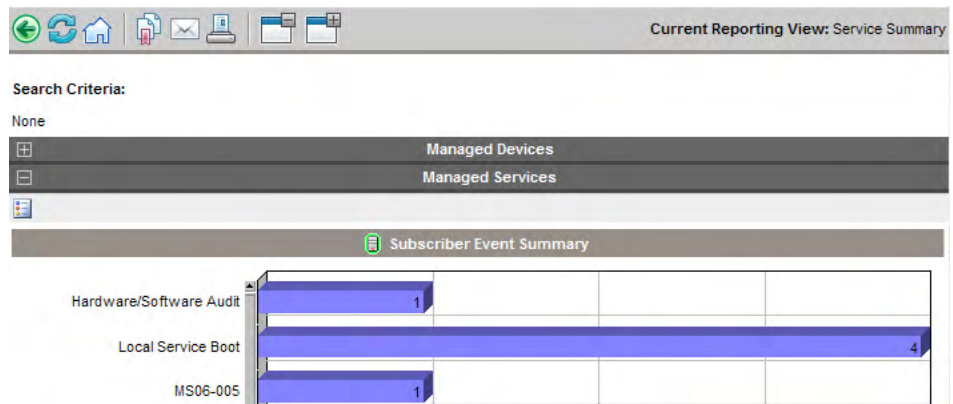
  

HP Hardware Alerts							
				15 items	1 - 1 of 1 items		
Details	Device Name	Last Modified	Name	Description	Category	Status	Severity
	HP16293324192	2006-04-18 14:38:02	Chassis Fan Stall	Chassis Fan Speed	3: Sensor	5: Predictive Failure	25: Critical Failure

## About Reporting Windows

The Report Page displays the windows specified in the applied view. The figure below shows an example of report windows displayed on the Report Page: **Managed Devices** and **Managed Services**. The Managed Devices window is minimized and the Managed Services window is maximized to show report data.

**Figure 16    Sample Reporting Window**





The following sections describe Reporting Windows features and options.


- [Using the Windows Action Bar on page 133](#)
- [Creating Dynamic Reporting Groups on page 136](#)


## Using the Windows Action Bar

Each window contains an **Action Bar** with the following possible icons:


 **Create new Dynamic Reporting Group** – launches the [Group Creation Wizard](#), described on page 174, and uses the devices returned in the report to create a new group.

 The group creation button is only visible on reports that contain lists of devices.


 **Export to CSV** – creates a comma-separated list of the report query that you can open or save.


 **Export to IQY** – creates a Web query list of the report query that you can open or save as an MS Excel file. A live link to the source report is created allowing you to refresh the Reporting data from within the Excel spreadsheet by retrieving the data directly from HPCAS. When you open the IQY file, you are prompted for access credentials. Use the following defaults:

- **Enter your Reporting Server User ID** = admin
- **Password** = secret
- **Directory Source** = Blank space (For example, hit the spacebar once and then hit Enter)

 **Switch to Graphical View** – switches the reporting view to graphical mode.

**Figure 17** Sample Reporting window



Details	Last Connect ↓	Radia ID	Device	IP Address	Operating System	OS Level
	2006-04-18 13:06:54	HP16293324192	<a href="#">HP16293324192</a>	16.119.237.28	Microsoft Windows XP Professional Version 5.1.2600 [Build 2600]	Service Pack 2

### Browsing Items in a Report

There may be large number of items in a report. The Action Bar lets you customize how many items to view in a given window area. To browse to records outside your current window area, use the Browse buttons or drop-down list.

### Maximum items per window

Use this drop-down list box to limit how many items to display in the current window. For example, if you select a maximum of 30 items, you will be able to scroll 30 items in the current window.

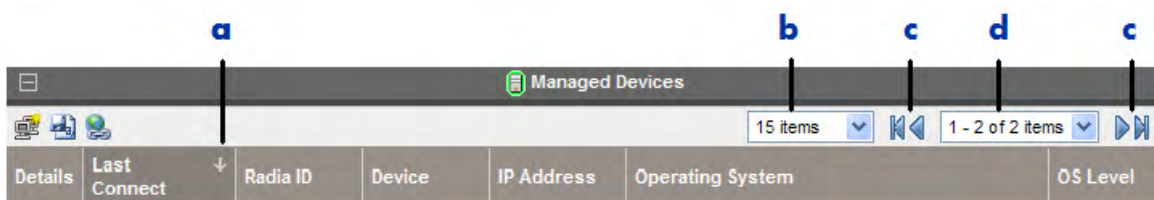
### Browse Back and Forward Buttons

If you set the maximum items per window smaller than the total items in the report, you will have the ability to browse through multiple windows. Use the browse buttons to go to the First, Previous, Next, or Last window for the current report.

**Browse** to a specific window.

Alternatively, select which set of items to view from the list of available windows. For example, select **1 - 15 of 46** items from drop-down list box to view that set of items.

**Figure 18 Report Display Settings**



### Legend

- a** Current sort field and order
- b** Maximum items per window
- c** Browse buttons
- d** Current display and total


### Sorting Columns

Click the column heading name to sort items in a report by that column either in ascending or descending order.

To toggle between ascending and descending sorts, click a currently selected column (indicated by the arrow). An up arrow indicates the active sort column and ascending order. A down arrow indicates the items are displayed in descending order.

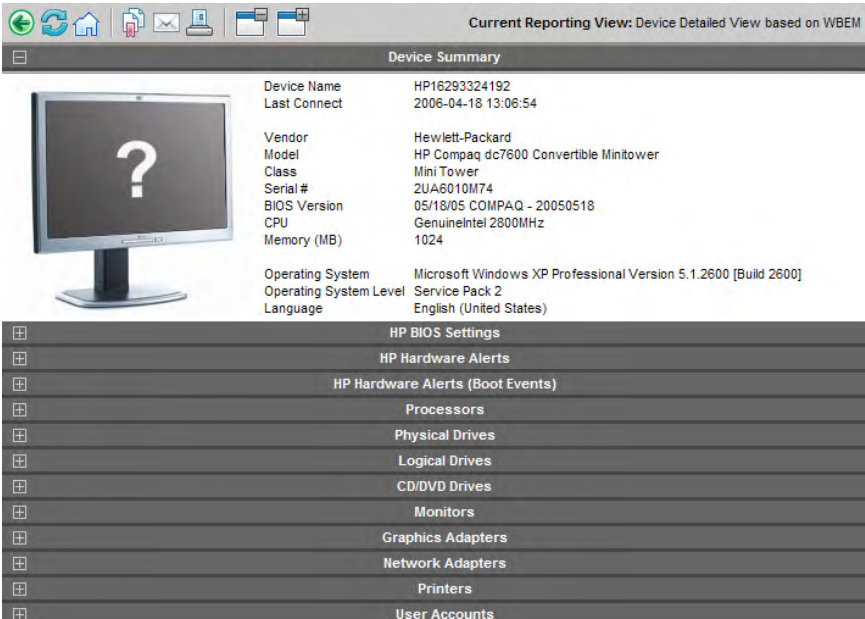
For example, the figure above shows a report sorted on the Last Connect column in descending order. Notice the down arrow to the right of the Last Connect column heading.

### Displaying Device Summary

In the Managed Devices report window, click **Show Details**  next to any item to display the details for that device.

The Device Summary window opens, as shown in the following figure below. Notice that in addition to the standard global icons, the green arrow icon allows you to return to the previous window.

**Figure 19    Device Summary Window**



Click any heading at the bottom of the page to expand its listing. For example, if you expand **HP Hardware Alerts**, you will see the list of hardware alerts reported for that device.

The Device Summary contents will vary according to the starting Report Window.


### Applying Filters from Report Data

Click hyperlinked data within a report to filter by that specific criterion. A filter is applied and displayed in the Search Criteria.

## Creating Dynamic Reporting Groups

Dynamic Reporting groups contain devices returned as the result of a reporting query. Create a Dynamic Reporting Group by first generating a list of devices in a report query, then using the [Group Creation Wizard](#).

To create a Dynamic Reporting group

- 1 Generate a list of devices using a report query, for example, from the default Reporting window, click **View Managed Devices**.
- 2 Filter the device list to include only devices you want to include in your group. For example, click Microsoft Windows XP Professional Version 5.1.2600, in the Operating System column. The report then displays all managed devices using Version 5.1.2600 of Windows XP Professional. You can filter the device list further by adding additional filters.
- 3 When you have the list of devices you want to add to your group, click the  **Create new Dynamic Reporting Group** button to start the [Group Creation Wizard](#).
- 4 Follow the steps in the wizard on page 174 to create your dynamic group of devices.

### About Dynamic Reporting Groups

- Dynamic Reporting group membership depends upon the devices meeting the criteria defined in the query used to create the original list. Membership is updated based on the schedule you define during the Group Creation Wizard or can be altered using the Group Details window.
- Existing Reporting group criteria cannot be modified. If you want to create a group with the same name as an existing Reporting group but with different criteria you will need to first delete the existing group, create a new device query, then use the Group Creation Wizard to create a new group with the new criteria.



## 6 Configuration

The Configuration section allows you to contact support, manage console user access, define and configure Infrastructure Servers, manage patch acquisition schedule and settings, manage hardware, and configure ODBC settings.

Click a link in the section contents area on the left to show the configuration options available in each area. The following sections define the Configuration areas you can control:

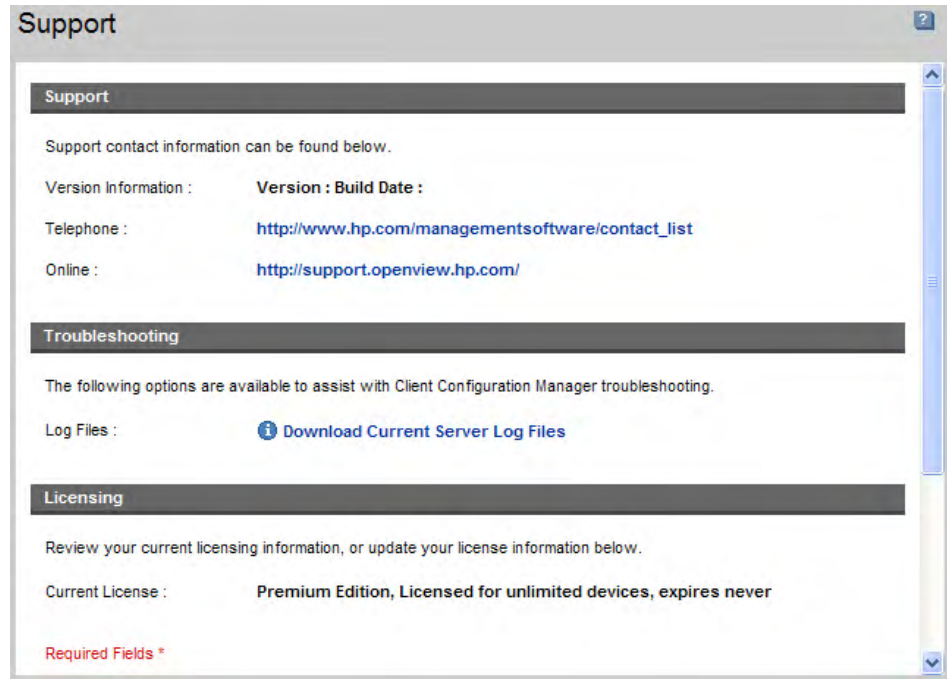
- [Support](#) on page 137
- [Console Access](#) on page 139
- [Infrastructure Management](#) on page 142
- [Patch Management](#) on page 151
- [OS Management](#) on page 155
- [Hardware Management](#) on page 156
- [Reporting](#) on page 159

### Support

Use the Support section to locate support information, download current server log files, and review your licensing information.

The licensing section shows the type of HPCAS license (Starter or Standard) you have installed.

**Figure 20 Support section of the Configuration tab**



The following tasks can be completed in the Support area:

- [Downloading Log Files](#) below
- [Updating Licensing Information](#) on page 139

## Downloading Log Files

When working with support, you may be asked to supply log files. Use the link provided to download and save a compressed file of current server log files.

To download log files

- 1 In the Troubleshooting area, click the link **Download Current Server Log Files**. A new window opens.
- 2 When the log files are prepared, click **Download logfiles.zip**.
- 3 When prompted, click **Save** to store the compressed file on your computer.

- 4 Specify a location to store the file and click **OK**.
- 5 The log files are downloaded to your computer and saved in a single ZIP formatted file called `logfiles.zip`.

## Updating Licensing Information

Current licensing information is required to use HPCAS. Use the Licensing section to view and update this information.


To apply a new license

- 1 Copy and paste the text from your new `license.nvd` file into the **License Data** text box.
- 2 Click **Save**. Updated license information is displayed after **Current License**.

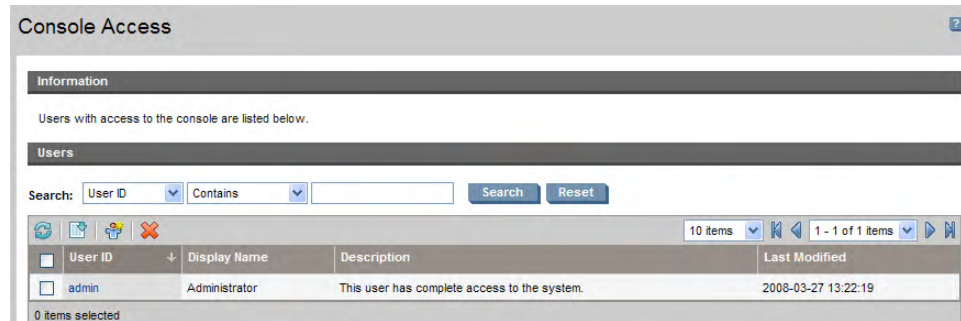
## Console Access

Use the Console Access section to manage console users. Management jobs contain a Creator field which displays the user ID used to create the job. This allows you to keep track of which console users created individual jobs.

By default, one console user exists, **admin**, with the default password of **secret**. This console user account cannot be deleted. Also, the currently active user account cannot be deleted. If you need to delete the currently active account, first log out then log back in as a different user. Then you will have the option to remove the previously active console user account.

Use the **Export to CSV** button  to create a comma-separated value format list of the console users table.


**Figure 21 Console Access section**



The following sections describe how to manage your console users:

- [Creating additional console users](#) on page 140
- [Removing console users](#) on page 140
- [Viewing and Modifying Console User](#) on page 141
- [Changing the Console Password](#) on page 141


## Creating additional console users

- Click the **Create New User** toolbar button  to launch the [User Creation Wizard](#).
- Follow the steps in the wizard on page 182 to add additional console users.



User IDs cannot contain reserved characters ( underscore `_`, space, or slashes `/` or `\` ). Reserved characters are automatically removed when the User ID is generated. For example, if you attempted to create User ID, `jdoe_1`, you would end up with `jdoe1`.

## Removing console users

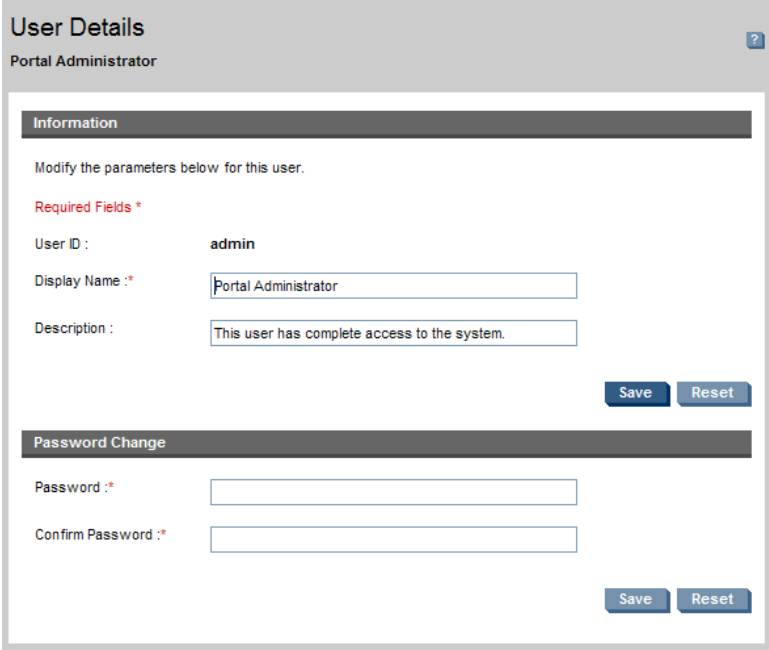
- To remove a console user, first select the user from the list and then click the **Delete Users** toolbar button .

## Viewing and Modifying Console User Details

Click any User ID to view that console user's details.

From the User Details window, you can modify the display name, description, and password. Be sure to click **Save** to confirm any changes.

**Figure 22** User Details window



The screenshot shows the 'User Details' window for the 'Portal Administrator' user. The window has a title bar with the text 'User Details' and a question mark icon. Below the title bar, the user's name 'Portal Administrator' is displayed. The main content area is divided into two sections: 'Information' and 'Password Change'. The 'Information' section contains a heading 'Information' and a sub-heading 'Modify the parameters below for this user.' Below this, there is a red label 'Required Fields \*'. The 'User ID' is 'admin'. The 'Display Name' is 'Portal Administrator' and the 'Description' is 'This user has complete access to the system.' There are 'Save' and 'Reset' buttons at the bottom right of this section. The 'Password Change' section contains a heading 'Password Change' and two text boxes for 'Password' and 'Confirm Password', both marked with a red asterisk. There are 'Save' and 'Reset' buttons at the bottom right of this section.

## Changing the Console Password

When console users are created, a console access password is defined. To change the password, use the User Details window.

To change a console password

- 1 Click the User ID to open the User Details window.
- 2 In the **Password Change** section, enter and confirm a new password by typing it into the text boxes provided.
- 3 Click **Save**.

# Infrastructure Management

Implementing Infrastructure Servers allows you to optimize bandwidth and increase network performance by providing data caching services for managed devices. Use the Infrastructure Management section of the Configuration tab to manage Infrastructure Servers and Locations (subnets).

Managed devices connect to the Infrastructure Server located within their own subnet, as defined by the Infrastructure Location assigned to that server. Devices will then use that server for data transfer tasks.

The Infrastructure Management area contains two tabs described in the following areas:

- [Servers](#) on page 142
- [Locations](#) on page 149



## Servers







Define servers by adding devices to the Infrastructure Server group then by deploying the Infrastructure service. When you are finished adding Infrastructure Servers, you will need to assign Infrastructure Locations for each server. See [Locations](#) on page 149 for additional information.

► Infrastructure Servers automatically cache all requested data with the exception of operating system images. Infrastructure Servers can also be pre-populated with all data on the HPCAS server using the synchronize feature. See [Synchronizing Infrastructure Servers](#) on page 145 for details.

The Infrastructure Servers toolbar contains buttons you can use to define and configure Infrastructure Servers in your environment.

**Table 12     Infrastructure Servers toolbar buttons**

Toolbar Button	Description
	<b>Refresh Data</b> – Refresh the list data.
	<b>Export to CSV</b> – creates a comma-separated list that you can open or save.

Toolbar Button	Description
	<b>Add Infrastructure Server(s)</b> – Add devices to the Infrastructure Servers group.
	<b>Remove Infrastructure Server (s)</b> – Remove devices from the Infrastructure Servers group.
	<b>Deploy the Infrastructure Service</b> – Launches the <a href="#">Infrastructure Deployment Wizard</a> .
	<b>Remove the Infrastructure Service</b> – Launches the <a href="#">Infrastructure Removal Wizard</a> .
	<b>Synchronize the selected Infrastructure Servers service cache</b> – Synchronizes the selected server's service cache with the HPCAS Server.
	<b>Delete Device(s)</b> – Delete devices.

Infrastructure Servers are devices that have been added to the Infrastructure Servers group and have the Infrastructure service installed.

The following sections explain how to define and configure Infrastructure Servers:

- [Managing Infrastructure Servers](#) below
- [Deploying the Infrastructure Service](#) on page 144
- [Synchronizing Infrastructure Servers](#) on page 145
- [Server Details Window](#) on page 147

## Managing Infrastructure Servers

When selecting devices to add as Infrastructure Servers, consider the following:

- The devices should have adequate space to store published services.
- The devices should have a capable, high-speed network card (100 MB or 1 GB data transfer rates).
- The devices should be located on a subnet where you want to localize download traffic to that network.

Use the toolbar to add and remove devices from the Infrastructure Servers group.




The following ports must be excluded if a firewall is enabled on any of the Infrastructure Servers you will be using.

- TCP 3463, 139, 445, and 3467
- UDP 137 and 138


Windows Firewall users can select File and Printer sharing to exclude TCP ports 139 and 445 and UDP ports 137 and 138.

### To add an Infrastructure Server

- 1 On the Infrastructure toolbar, click the **Add Devices**  toolbar button. The HPCAS Infrastructure Servers group membership window opens and shows a list of all devices imported into HPCAS.
- 2 Select devices from the list and click **Add Devices**.

Devices added appear in the Infrastructure Servers list.

### To remove an Infrastructure Server

- 1 On the Infrastructure toolbar, select the device you want to remove from the Infrastructure Servers group.
- 2 Click the **Remove Device**  toolbar button.

The device is removed from the group.



If you remove a device from the Infrastructure group that had the Infrastructure Service installed, it will continue to operate as an Infrastructure Server until the service is removed. Use the **Remove the Infrastructure Service** toolbar button to remove the service.

When devices are added, you can begin [Deploying the Infrastructure Service](#). This service is required to begin remote data caching on each server.

## Deploying the Infrastructure Service

Deploy the Infrastructure service to enable remote services on the Infrastructure Server devices.



### To deploy the Infrastructure Service

- 1 Select devices from the Infrastructure Servers list using the check boxes in the left column.
- 2 Click **Deploy the Infrastructure Service**  toolbar button to launch the [Infrastructure Deployment Wizard](#).
- 3 Follow the steps in the wizard on page 185 to deploy the Infrastructure Service to the selected devices.

Each time devices request resources not available on the Infrastructure Server's local cache, the data is retrieved from the HPCAS server, stored in the dynamic cache of the Infrastructure Server, and provided to the client devices. Services can be pre-loaded to Infrastructure Services using the Synchronize feature. See [Synchronizing Infrastructure Servers](#) on page 145 for details.

### To remove the Infrastructure Service

- 1 Select devices from the Infrastructure Servers list using the check boxes in the left column.
- 2 Click **Remove the Infrastructure Service**  toolbar button to launch the [Infrastructure Removal Wizard](#).
- 3 Follow the steps in the wizard on page 186 to remove the Infrastructure Service from selected devices.

After you have created Infrastructure Servers, you need to define [Locations](#) to then assign those servers to specific subnets.

## Synchronizing Infrastructure Servers

An Infrastructure Server's service cache can be pre-populated with the data required by managed devices. Normally, an Infrastructure Service will automatically cache data when it is requested by a client device (with the exception of operating system images). Using the Synchronize feature, you can pre-load an Infrastructure Server's cache with all available data on the HPCAS Server.

You can select which data to pre-load using the Cache tab in the Server Details window (after the Infrastructure Server service has been deployed).

- ▶ Pre-loading Infrastructure Servers consists of downloading large binary files and therefore may impact overall network performance. When possible, synchronization should be performed during off-hours when optimal network performance is not a priority.

To view the current synchronization status of each Infrastructure Server, see the **Last Synchronized** column on the Infrastructure Servers list or refer to the General tab's Summary section in the Server Details window. **Last Synchronized** records the last time the synchronize feature was *initiated* on a server.


- ▶ After an Infrastructure Server is first synchronized, a new entry is added to the Managed Devices report with an HPCA Agent ID of <DeviceName>\_PRELOAD. This entry exists specifically to display the preload status of the Infrastructure Server services, and does not contain detailed hardware information for the associated device. Information about the services that have been preloaded or removed from the Infrastructure Server can be found by clicking the Details link for the Managed Device entry and expanding Managed Services. This same information can also be found on the Reporting tab of the Server Details window for an Infrastructure Server, under Preloaded Services.

#### To select which data to preload

- 1 After the Infrastructure Server service is deployed, in the Infrastructure Servers list, click a Server link to open the **Server Details** window.
- 2 Click the **Cache** tab.
- 3 Use the drop-down lists to enable or disable the services you want to make available for pre-loading from the HPCAS Server. By default, pre-loading is disabled for all services.
- 4 Click Save to commit your changes.
- 5 Finally, click **Synchronize** to pre-load the Infrastructure Server with available data right away.

#### To synchronize Infrastructure Servers

There are two methods you can use to synchronize Infrastructure Servers in the Configuration tab, Infrastructure Management section's Server tab:

- 1 To synchronize one or more servers, use the Infrastructure Servers list and select all of the servers for synchronization. Click the **Synchronize the selected Infrastructure Servers service cache**  toolbar button to update all selected server's with the latest data from the HPCAS Server. The services pre-loaded to each server depend on the settings configured in each server's Server Details window **Cache** tab.  
  
or
- 2 To synchronize a single server, select the server and use the toolbar button, or click the Server name to open the Server Details window and click **Synchronize** in the **Common Tasks** area. You can also use the Cache tab to determine which services to pre-load, and then click **Synchronize**.

To view a summary of pre-loaded services in an Infrastructure Server's cache

- Open the Server Details window and click the **Reporting** tab.

The Reporting tab displays the pre-loaded services available in the cache and the status of each.

The **Event** column describes the current status:

- **Update (Preload)** – the service was updated during the last cache synchronization.
- **Install (Preload)** – the service was pre-loaded successfully (initial pre-load).
- **Uninstall (Preload)** – the service was removed from the preload cache.
- **Repair (Preload)** – the cache for the service was either missing files or contained invalid files and was repaired during the last synchronization.

Only pre-loaded services are displayed in the report. Services stored on an Infrastructure Server through the default method (cached automatically when requested by a managed device) are not displayed.

## Server Details Window

To access the Server Details window click any Server name link in the Infrastructure Servers list.

From the Server Details window, you can manage your Infrastructure Server and view status and other details related to devices, subnets, and pre-loaded services.

## General

From the General tab you can view information about the Infrastructure Server in the Common Tasks section and complete tasks like [Deploying the Infrastructure Service](#) and [Synchronizing Infrastructure Servers](#) service cache.

The Summary area shows the number of Locations (subnets) assigned to the server and the number of devices connecting to that server for updates. Status shows whether or not the Infrastructure Service is installed and the last time the server's service cache was synchronized with the HPCAS Server.

## Properties

Use the Properties tab to view all information about the Infrastructure Server device. Expand the Advanced Properties section to view additional detailed information.

## Cache

The Cache tab allows you to select the types of services stored in the Infrastructure Server's service cache. See [Synchronizing Infrastructure Servers](#) on page 145 for additional details.

## Locations

The Locations tab defines which subnets are assigned to the Infrastructure Server. For details on adding and assigning subnets see [Locations](#) on page 149.

## Devices

The Devices tab displays all devices currently assigned to the Infrastructure Server. The list is based on each device's last connect and can change if a device's subnet changes.

## Reporting

Use the Reporting tab to view the pre-load summary for services. Only pre-loaded services are displayed. Services cached automatically (after a






device request) are not displayed. For details on each pre-load status, see [Synchronizing Infrastructure Servers](#) on page 145.

## Locations

Use the Locations tab to view existing Locations or to add new Locations (subnets) to which you will then assign Infrastructure Servers. This ensures that managed devices will connect to a local Infrastructure Server (located on their same subnet).

The Locations toolbar contains buttons you can use to define and configure Locations in your environment.

**Table 13 Infrastructure Servers toolbar buttons**

Toolbar Button	Description
	<b>Refresh Data</b> – Refresh the list data.
	<b>Export to CSV</b> – creates a comma-separated list that you can open or save.
	<b>Create a New Location</b> – Launches the Infrastructure Location Creation Wizard.
	<b>Auto-create locations based on Inventory Data</b> – Creates a list of Locations based on inventory data from managed devices.
	<b>Delete Location(s)</b> – Delete selected Infrastructure Locations.

The Locations list includes information about each added Location including the Infrastructure Server that was assigned and the number of devices that exist on the subnet. Click any **Subnet Address** to open a [Location Details](#) window.

You can create new Infrastructure Locations manually or automatically based on inventory data stored in HPCAS. To obtain the required inventory data, the Management Agent must be deployed.

### To create a New Location

- 1 Click **Create a New Location**  toolbar button to launch the [Infrastructure Location Creation Wizard](#).

- 2 Follow the steps in the wizard on page 186 to create a new Infrastructure Location.


#### To create new Locations based on Inventory Data

- 1 Click **Auto-create locations based on Inventory Data** .
- 2 Click **OK**.
- 3 Click **Close**.


The list of Infrastructure Locations is updated. This method will create one Location per each new subnet found.

After a Location is added, assign Infrastructure Servers.

#### To assign a Locations to an Infrastructure Server


- 1 Click the **Servers** tab.
- 2 Click the Infrastructure Server to which you want to assign a Location. The Server Details window opens.
- 3 Click the **Locations** tab.
- 4 Click **Add Locations**  toolbar button. The Server Locations window opens.
- 5 Select the Locations to assign to the Infrastructure Server and click **Add Locations**.
- 6 Click **Close**. If you are finished adding Locations, click **Close** again to close the Server Details window.

After you are finished with these steps, a Location is assigned to the Infrastructure Server and any devices connecting within the defined subnet will be routed to that Infrastructure Server for resource needs.

You can remove any Locations assigned to an Infrastructure Server using the **Remove Locations**  toolbar button.

#### To remove Locations from an Infrastructure Server

- 1 Click the **Servers** tab.
- 2 Click the Infrastructure Server for which you want to remove a Location. The Server Details window opens.
- 3 Click the **Locations** tab.

- 4 Select the Locations to remove from and click the **Remove Locations**  toolbar button.
- 5 Click **Close**. If you are finished removing Locations, click **Close** again to close the Server Details window.

## Location Details

Click the subnet address of a Location to open the Location Detail window.

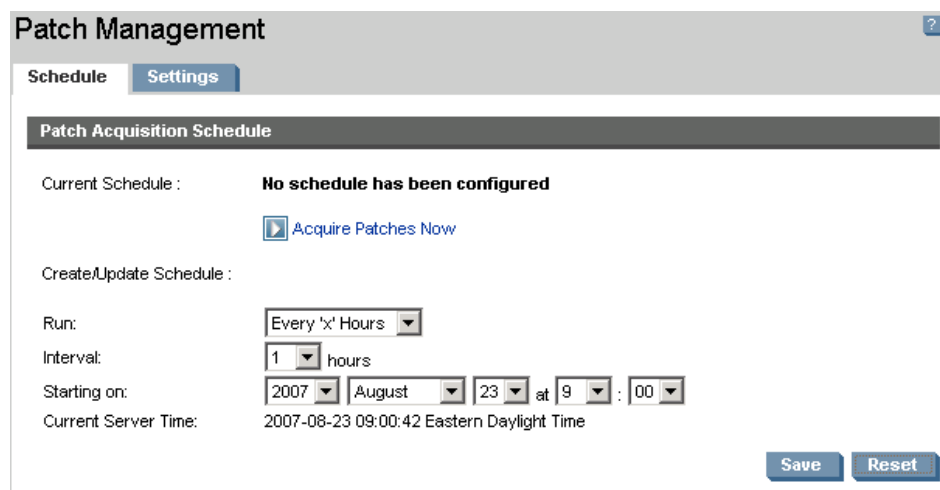
- Use the **Properties** tab to change the description for the Location. Click **Save** after making any changes.
- Use the **Devices** tab to list all devices that are located on the subnet.

# Patch Management — Configuration

Use the Patch Management section to acquire patches and HP Softpaqs, configure schedules for patch acquisition, and to define patch acquisition settings.

Entitled patches are deployed automatically based on the compliance discovery schedule you define using the [Patch Compliance Discovery Wizard](#). Patches can be deployed immediately using the [Patch Deployment Wizard](#).

**Figure 23 Patch Management section of the Configuration tab**




**Patch Management** ?

**Schedule** **Settings**

**Patch Acquisition Schedule**

Current Schedule : **No schedule has been configured**

 [Acquire Patches Now](#)

Create/Update Schedule :

Run:

Interval:  hours

Starting on:    at  :

Current Server Time: 2007-08-23 09:00:42 Eastern Daylight Time

**Save** **Reset**

The following sections explain each Patch Management tab:

- [Configuring Patch Acquisition Schedule](#) on page 152
- [Configuring Patch Acquisition Settings](#) on page 153

## Configuring Patch Acquisition Schedule

Use the **Schedule** tab to acquire patches or to configure a patch acquisition schedule.



To ensure efficient acquisition of the latest available patches, we recommend configuring your Patch Acquisition Schedule to run during off-peak hours and no more than once daily.

**Current Schedule** shows the currently configured patch acquisition schedule.

### To acquire patches

- Click **Acquire Patches Now** to acquire patches based on the current Patch Acquisition settings. Patches are downloaded and stored in the Patch Library.
- View acquired patches in the Patch Management, [Patches](#) tab.

### To configure the patch acquisition schedule

- 1 Use the tools provided to set the acquisition schedule.
  - **Run:** Select whether to discover patches based on an interval hours, days, or weeks.
  - **Interval:** Select the specific interval (hours, days, or weeks).
  - **Starting on:** Use the drop-down lists to select the date patch compliance should be discovered.
  - **Current Server Time** displays the current time of the HPCAS server.
- 2 When finished, click **Save** to commit your changes.

The new schedule is displayed after **Current Schedule**.



## Configuring Patch Acquisition Settings

Use the **Settings** tab to configure the acquisition settings for the Windows patches and HP Softpaqs you want to acquire. Patches are acquired from HP and Microsoft sources and Softpaqs are acquired by leveraging HP Instant Support technologies.

Required fields are marked with an asterisk (\*).

**Figure 24 Patch Acquisition settings tab**

The screenshot shows the 'Patch Management' window with the 'Settings' tab selected. The 'Patch Acquisition Settings' section contains the following fields:

- Microsoft Bulletins**
  - Enabled :** A dropdown menu set to 'Yes'.
  - Bulletins to Acquire :\*** A text box containing 'MS04\*,MS05\*,MS06\*' with a help icon. Below it, an example reads 'e.g. MS05\* or MS05\*,MS06\*'.
  - Languages to Acquire :\*** A text box containing 'en' with a help icon. Below it, an example reads 'e.g. en or en,ja,fr'.
- HP Softpaqs**
  - Enabled :** A dropdown menu set to 'Yes'.
  - HP System IDs :\*** A text box containing '0890' with a help icon and a blue icon. Below it, an example reads 'e.g. 088C'.
- Connection Settings**
  - Proxy Server Address :** A text box containing 'http://web-proxy.atl.hp.com:8088' with a help icon. Below it, an example reads 'e.g. http://proxyserver:8080'.


To configure patch acquisition settings


- 1 Complete the **Microsoft Bulletins** area.
  - In the **Enabled** drop-down list, select **Yes** to acquire Microsoft Bulletins.
  - In the **Bulletins to Acquire** text box, type the Bulletins to download for each discovery period. Use wildcard characters to designate a range of bulletins (for example, MS05\*). Separate multiple bulletin searches with a comma (for example, MS05\*, MS06\*).

- In the **Languages to Acquire** text box, type the language codes for each language version available for the patches you want to download. Use the following table to find the appropriate language codes. Separate multiple language codes with a comma and no space (for example: en,fr,ja). Codes are case-sensitive.

**Table 14 Language Codes**

Language = Code	Language = Code	Language = Code
Arabic = ar	French = fr	Norwegian (Bokml) = no
Chinese (Hong Kong S.A R) = zh-hk	German = de	Polish = pl
Chinese (Simplified) = zh-cn	Greek = el	Portugese (Brazil) = pt-br
Chinese (Traditional) = zh-tw	Hebrew = he	Portugese (Portugal) = pt-pt
Czech = cs	Hungarian = hu	Russian = ru
Danish = da	Italian = it	Spanish = es
Dutch = nl	Japanese = ja	Swedish = sv
English = en	Japanese (NEC) = ja-nec	Turkish = tr
Finnish = fi	Korean = ko	

- Complete the **HP Softpaqs** area.
  - In the **Enabled** drop-down list, select **Yes** to acquire HP Softpaqs.
  - In the **HP System IDs** text box, determine which device-related HP Softpaqs are acquired by either typing a list of HP System IDs in the text box or by clicking the **Retrieve Data** button  to the right of the text box to automatically create the list of System IDs based on devices in HPCAS.
- Complete the **Connection Settings** area if needed.
  - Type a **Proxy Server Address** from which to obtain bulletins (for example, `http://proxyserver:8080/`).
  - Type a **Proxy User ID** and **Proxy Password** to use when acquiring patches.

 Patch acquisition is limited to proxy servers configured with basic authentication only.
- Click **Save** to apply your changes.



Initial patch acquisition may take an extended period of time.

## OS Management

Use the OS Management section to configure settings for operating system deployment.

**Figure 25 OS Management section of the Configuration tab.**

OS Management

**Information**

Configure the settings for OS Deployment below. These settings will be used for all OS Deployment operations.

**Caution:** Deploying an Operating System will in some cases overwrite existing data depending on the number of hard drives and partitions on the target device. If you select Unattended mode, be sure to back up existing data on target devices before deploying a new Operating System.

**Properties**

OS Deployment Mode :

### To configure the OS Deployment mode

- In the Configuration tab, OS Management section, select the OS Deployment Mode:
  - **Prompt User (Attended)** — A user must be present at the managed device during operating system deployment to continue the deployment process.
  - **Do not prompt user (Unattended)** — No dialogue windows are displayed on managed devices during operating system deployment. No user interaction is required.



Deploying an operating system image will in some cases overwrite existing data depending on the number of hard drives and partitions on the target device. If you select **Do not prompt user (Unattended)**, be sure to back up existing data on target devices before deploying a new operating system.



If you are migrating settings during operating system deployment, you will be required to supply a password to back up device settings before the operating system is installed.

- Click **Save** to commit your changes.



Changes to the OS Deployment Mode affects all new and scheduled OS deployment jobs.

## Hardware Management

Use the Hardware Management section to configure alert options for HP Client Management Interface (CMI), Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T.) and Trusted Platform Module (TPM) settings.

The following sections describe the hardware configuration options available:

- [Configuring CMI](#) on page 156
- [Configuring S.M.A.R.T](#) on page 157
- [Configuring TPM](#) on page 158

## Configuring CMI

The CMI Softpaq is installed to each HP targeted device as part of the HPCAS Agent Deployment. The HP Client Management Interface (CMI) provides enterprise managers and information technology professionals with an increased level of management instrumentation for HP business-class desktops, notebooks, and workstations.

CMI hardware-specific information is captured and available for reporting. Use the **HP Specific Reports** Reporting View in the Display Options section of the Reporting tab to create CMI hardware-related reports. (Select **Inventory Management Reports, Hardware Reports**, then **HP Specific Reports** to view CMI-related reporting options).

For additional CMI information see:

<http://h20331.www2.hp.com/Hpsub/cache/284014-0-0-225-121.html>

Use the CMI tab to modify HP CMI settings. Modified settings take effect the next time a managed client connects to the HPCAS infrastructure.



CMI is compatible with only specific HP device models. Refer to your device description for compatibility information.

#### To configure CMI

- 1 In the HPCAS console click the **Configuration** tab, then select **Hardware Management**.
- 2 Click the **CMI** tab.

#### To enable Client Alert reporting

- 1 Select **Enabled** from the Report Client Alerts drop-down list to report on captured client alerts from managed HP devices. Alert reporting is disabled by default.
- 2 Select the minimum alert severity to report from the drop-down list.

#### To display Client Alerts on the client device

- 1 Select **Enabled** from the Show Client Alerts drop-down list to turn on client alerts on managed HP devices. Alerts are disabled by default.
- 2 Select the minimum alert severity to display on the client device.
- 3 Type the number of seconds an alert should appear on the client device. By default, an alert is displayed for five seconds.

## Configuring S.M.A.R.T.

Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.), is a monitoring system for computer hard disks that detects and reports on various indicators of reliability, acting as an early warning system for drive problems. As part of the Client Automation Management Agent, detection of these events can be enabled for both display and reporting purposes. Use the Configuration tab's Hardware Management area to configure the S.M.A.R.T. monitoring settings. S.M.A.R.T. monitoring is disabled by default.

#### To enable and configure S.M.A.R.T. monitoring

- 1 In the HPCAS console click the **Configuration** tab, then select **Hardware Management**.

- 2 Click the **S.M.A.R.T.** tab.
- 3 Use the **Enable S.M.A.R.T Monitoring** drop-down list and select **Enabled**. S.M.A.R.T. monitoring is disabled by default.
- 4 Use the **Display Client Alerts** drop-down list to either enable or disable S.M.A.R.T. client alerts. Alerts are disabled by default. Enabling client alerts will cause an alert window to appear on managed devices when a possible drive problem is detected on that device.
- 5 Use the **Report Client Alerts** drop-down list to enable or disable S.M.A.R.T. client alert reporting. When enabled, client alerts are captured and available for reporting purposes. Reporting is disabled by default.
- 6 Click **Save**.

After **Enable S.M.A.R.T. Monitoring** and **Report Client Alerts** are enabled, use the [Reporting](#) area of the HPCAS console to create S.M.A.R.T. reports. Alert reports are included in the [Inventory Management Reports](#) reporting view. Select **Inventory Management Reports**, then **Hardware Reports**, then **Detail Reports** to view the **S.M.A.R.T. Alerts** report.

## Configuring TPM

Use the TPM tab to configure the Trusted Platform Module chip on compatible HP devices. Deploy the [CCM\\_TPM\\_ENABLEMENT](#) service to initialize TPM ownership and apply these settings. See [Deploying Software](#) on page 83 for software deployment information.

► In order to enable and initialize the TPM security chip, the HP ProtectTools software must first be installed on the device. Some device models have this software pre-installed while for others you will need to either download or purchase the software separately. For more information, review the HP documentation for your particular device model.

TPM is a hardware security chip that is installed on the motherboard of an HP business PC. It is included as part of HP ProtectTools Embedded Security.

For additional information see:

**<http://h20331.www2.hp.com/hpsub/cache/292199-0-0-225-121.html>**

### To configure TPM

- 1 In the HPCAS console click the **Configuration** tab, then select **Hardware Management**.
- 2 Click the **TPM** tab.
- 3 Type the BIOS Admin and TPM Owner passwords.
- 4 Type the Emergency Recovery and Password Reset Tokens.
- 5 Select the Reboot Settings. After the TPM chip is enabled, the device is rebooted. This setting determines the level of interaction the end user will have.
  - **Accept Only** – After reboot, user must accept enablement
  - **Accept or Reject** – After reboot, user can accept or reject enablement
  - **Silent** – User is not prompted to confirm enablement after reboot
- 6 Type the file paths for Backup Archive, Emergency Recovery Archive, and TPM Password Reset Archives.
- 7 Click **Save**.

## Reporting

Use the Reporting section tabs to change the database ODBC settings, configure usage data collection settings, manage usage collection filters and clean up old reporting data.

- [Database](#) on page 160
- [Usage Settings](#) on page 160
- [Usage Collection](#) on page 161
- [Maintenance](#) on page 166

**Figure 26 Reporting section of the Configuration tab**

The screenshot shows a web interface titled "Reporting" with a help icon. Below the title are four tabs: "Database", "Usage Settings", "Usage Collection", and "Maintenance". The "Database" tab is selected. Under this tab, there is a sub-header "ODBC Settings". Below this, a message states: "Configure the ODBC settings below. These settings must match the configured ODBC DSN on the Client Configuration Manager server." A red label "Required Fields \*" is present. The form contains three fields: "ODBC DSN :" with the value "CCMDB", "ODBC User ID :\*" with the value "sa", and "ODBC Password :" which is empty. At the bottom right are "Save" and "Reset" buttons.

## Database

Use the Database tab to configure the ODBC settings. These settings must match the configured ODBC DSN on the HPCAS server.

Required fields are marked with an asterisk (\*).

### To configure ODBC settings

- 1 Enter a DSN User ID and Password in the text boxes provided.
- 2 Click **Save** to commit your changes.

## Usage Settings

Use the Usage Settings tab to configure usage collection parameters. If required, usage data can be obfuscated to ensure privacy. Usage data is collected when the Collection Agent is deployed. Use the [Application Usage Collection Wizard](#) to deploy the agent and begin collecting data.

Usage settings are applied to existing client devices during their collection schedule.





Obfuscation should be enabled prior to deploying the Collection Agent. If enabled after the agent is deployed, some reporting data will appear as both obfuscated and non-obfuscated.

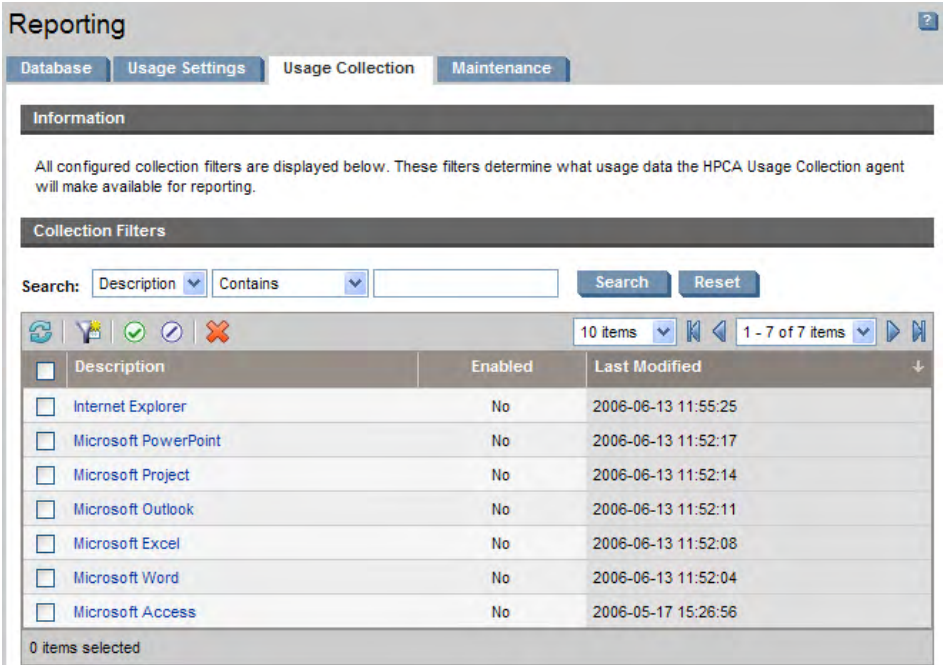
#### To obfuscate usage data

- 1 Use the drop-down lists to select which usage data information should be hidden.
  - **Computer** – hide computer-related information.  
Computer name - reported as a random set of alphanumeric values.
  - **User** – hide user-specific information.  
User name reported as [AnyUser].
  - **Domain** – domain information.  
Domain name reported as a random set of alphanumeric values.
  - **Usage** – hide usage counts and times.  
The executable file usage times and launch counts are all reported as zero values
- 2 Select **Enabled** next to the usage information you want to obfuscate within usage reports.
- 3 **Save** to commit the changes.

## Usage Collection

Use the Usage Collection tab to create and manage usage collection filters.

**Figure 27    Usage Collection tab**



► HP Client Automation Standard is required for collecting application usage data.

Usage collection filters determine what usage data is made available by the Usage Collection Agent for reporting. When the Usage Collection Agent is deployed to a device, all usage data for all applications is collected and stored locally. The usage filters that you create and enable determine which local usage data is sent to HPCAS. Use the [Application Usage Collection Wizard](#) to deploy the Collection Agent and define a collection schedule.

If a filter is enabled after a Usage Collection Agent has already been deployed, all of the usage data defined by the filter that was collected and stored locally is then sent to HPCAS for reporting.

For example, if the Usage Collection Agent is deployed in May and a filter is enabled for Microsoft Word, all usage data for Microsoft Word is sent to HPCAS based on the schedule you defined. Then, in June you decide to create and enable a new filter for Microsoft Excel. The next time usage data is sent to HPCAS, it will include all Excel usage data that was collected and stored

locally from the date the Usage Collection Agent was first installed in May, up until the current date in June. Usage will continue to be sent thereafter for both applications.

Usage data is stored locally on managed devices for 12 months.

For usage collection filter configuration instructions, see:

- [Configuring Usage Collection Filters](#) on page 163
- [Defining Usage Criteria](#) on page 164

## Configuring Usage Collection Filters

Use the Usage Collection Filter Creation Wizard to create new usage collection filters. Use the Filter Details window to modify existing filters.


HPCAS contains pre-configured collection filters by default. You can use these filters as models for creating new filters or you can modify these filters to suit your needs.




Configuring filters to collect usage data based on wildcard characters can cause the collection of a large amount of data that can, over time, create severe reporting performance issues as the database grows in size. We strongly recommend that you create filters to collect data for only those applications for which you want usage information.

Collecting usage data for all applications should be avoided.

### To create a collection filter

- 1 On the Usage tab, click the **Create New Filter**  toolbar button to launch the [Usage Collection Filter Creation Wizard](#).
- 2 Follow the steps in the wizard on page 185, to create and enable the new collection filter.

### To enable a collection filter

- 1 In the Filter list, select the filter you want to enable by clicking the box to the left of the filter description.
- 2 Click the **Enable Selected Items**  toolbar button.
- 3 Click **Save**.

#### To modify an existing filter

- 1 In the Filter list, click the filter description link to open the Filter Details window.
- 2 In the Filter Criteria area, type the specific filter criteria to use when collecting usage data. See [Defining Usage Criteria](#) on page 164 for help in determining what criteria to select.
- 3 Click **Save**.

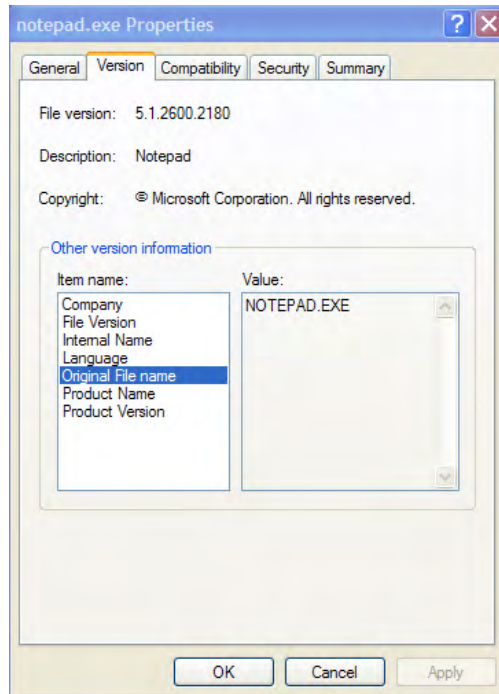
## Defining Usage Criteria

The Usage Collection Agent uses the file header information within each local executable to determine if that application meets defined filter criteria. You can use the file header information to determine what criteria to use to when defining a filter.

#### To determine file header information

- 1 Right-click an executable on your system.
- 2 Select **Properties** from the shortcut menu.
- 3 On the Properties window, click the **Version** tab.

**Figure 28 Application properties window**



The information contained in the **Item Name** and **Value** areas are used by the Usage Collection agent to filter the available usage data (with the exception of the Language and Internal Name items, which are not currently supported).

► Be aware that not all executable files support or correctly populate values stored in the file header.

The following example describes how to create a filter to search for a specific application.

To filter usage data for notepad.exe

- 1 Create a new Usage Filter by launching the [Usage Collection Filter Creation Wizard](#).
- 2 At the Properties step, define the following filter criteria:
  - **Description:** Notepad
  - **Enabled:** Yes

— **File/Application Name:** notepad.exe


- 3 Deploy the Usage Collection agent to managed devices. See [Deploying Software](#) on page 83 for instructions on deploying software to managed devices.

Usage data will be sent to HPCAS weekly and will include all usage data for Notepad for all devices that have the Collection Agent installed.

## Maintenance

The Maintenance tab shows all of the devices that have reporting data stored in HPCAS. Use the Maintenance tab toolbar to clean up reporting data for devices that may no longer be in your HPCAS database.

### To remove device reporting data

- 1 On the Maintenance tab, select the devices for which you would like to remove reporting data from HPCAS.
- 2 Click the Delete Reporting Data  toolbar button.
- 3 The reporting data is removed from HPCAS.

After reporting data are removed for a device, that data are no longer available when generating any reports.



If you are deleting reporting data for an actively managed device, to avoid reporting data discrepancies, you should remove then re-deploy the Management Agent on that device.

## 7 Wizards

While using HPCAS, you will use many different wizards to deploy agents, add devices, create groups, and more. This section contains an explanation of the individual steps you will encounter within each wizard.



Some wizards can be launched from multiple areas of the control panel.

- [Import Device Wizard](#) on page 168
- [Agent Deployment Wizard](#) on page 169
- [Agent Removal Wizard](#) on page 170
- [Software/Hardware Inventory Wizard](#) on page 171
- [Patch Compliance Discovery Wizard](#) on page 171
- [Application Usage Collection Wizard](#) on page 172
- [Power Management Wizard](#) on page 173
- [Group Creation Wizard](#) on page 174
- [Software Deployment Wizard](#) on page 177
- [Service Import Wizard](#) on page 178
- [Service Export Wizard](#) on page 178
- [Software Synchronization Wizard](#) on page 179
- [Patch Deployment Wizard](#) on page 180
- [Service Entitlement Wizard](#) on page 181
- [Software Removal Wizard](#) on page 182
- [User Creation Wizard](#) on page 182
- [OS Deployment Wizard](#) on page 183
- [Usage Collection Filter Creation Wizard](#) on page 185
- [Infrastructure Deployment Wizard](#) on page 185
- [Infrastructure Removal Wizard](#) on page 186
- [Infrastructure Location Creation Wizard](#) on page 186




The HPCAS console may open additional browser instances when running wizards or displaying alerts. To access these wizards and alerts, you must include HPCAS as an Allowed Site in your browser's pop-up blocker settings.

## Import Device Wizard

Use the Import Device Wizard to discover and add devices to your HPCAS database. When devices are imported, they can be targeted for management using the [Agent Deployment Wizard](#).

To import devices using the Import Device wizard

- 1 To launch the wizard, click **Import** on the [General](#) tab in the [Device Management](#) section or click the **Import Devices to Manage**  toolbar button on the [Devices](#) tab.
- 2 Select the Device Source from the drop-down list.
  - **Manual Import** – Type or paste a list of device host names or IP addresses into the text box provided.
  - **LDAP/Active Directory** – To import devices automatically from Active Directory or another LDAP-compliant Directory Service, type the LDAP Host, Port, User ID, password (if required) and the DN to Query.  
Also select the scope, an advanced filter, or a device limit to apply to the query.
  - **Domain** – To scan a network domain for devices to import, type the domain name (for example, type ABC for a full domain scan of the ABC domain) or part of the domain name and a wildcard character (ABC\* returns all devices from domains beginning with ABC). To include specific devices from a domain, use the following syntax, domain\device. For example, Sales\WS\* returns only devices beginning with WS from the Sales domain.  
Use an exclamation mark ! to exclude specific devices from a domain. For example, Sales,!Sales\WS\* will return all devices from the Sales domain with the exception of devices beginning with WS.
- 3 Click **Import**.
- 4 Click **Close** to exit the wizard.



Imported devices are displayed in the [Devices](#) tab.

## Agent Deployment Wizard

Use the Agent Deployment wizard to deploy the Management Agent to devices in your HPCAS database.

► Prior to deploying the Management Agent to a device, review the Firewall Settings rules for [Target Devices](#) on page 32 and ensure the necessary firewall rules are in place

To use the Agent Deployment Wizard to deploy a Management Agent

- 1 To launch the wizard:
  - Click **Deploy** on the [Device Management General](#) tab.
  - Click the **Deploy the Management Agent** toolbar button on the [Device Management, Devices](#) tab.
  - Click the **Deploy the Management Agent** toolbar button from the Group Management, Groups tab.
- 2 Click **Next** to begin the wizard.
- 3 All available devices are displayed. Select each device to which you want to deploy a Management Agent, and then click **Next**. Use the Search function to narrow the list of devices, if necessary.
- 4 Enter the required information for your selected devices, and click **Next**.
- 5 Select **Run: Now** to deploy the agent immediately after the wizard is complete, or select **Run: Later** and enter a date and time for agent deployment.
- 6 In the **Additional Parameters** section, select **Yes** (default) to install the Agent silently or select **No** to allow an installation UI to display on the target devices during the installation process.

► The Management Agent is deployed to Windows Vista and Windows Server 2008 devices in silent mode only, regardless of the Additional Parameter selected.
- 7 Click **Next**.

- 8 Review the summary information and click **Submit**. An Agent Deployment Job is created.
- 9 Click **Close** to exit the wizard.


## Agent Removal Wizard

Use the Agent Removal Wizard to remove the Management Agent from devices in your HPCAS database.



Removing the Management Agent will disable the ability to deploy software and patches and to collect updated inventory information for that device. Unmanaged devices will remain within their respective groups until removed from the groups or deleted from HPCAS and will retain all deployed software.


To remove a Management Agent using the Agent Removal wizard

- 1 Launch the wizard from the Device Management, **Devices** tab or from the Group Management, **Groups** tab.
- 2 Select the devices or groups from which you want to remove the Management Agent and click the **Remove the Management Agent**  toolbar button.
- 3 Click **Next** to begin the wizard.
- 4 Select **Run: Now** to remove the agent immediately after the wizard is complete, or select **Run: Later** and enter a date and time for Agent removal.
- 5 Click **Next**.
- 6 Review the summary information and click **Submit**. An Agent Deployment Job is created.
- 7 Click **Close** to exit the wizard.

# Software/Hardware Inventory Wizard

Use the Software/Hardware Inventory Wizard to create inventory audit jobs that will discover software and hardware inventory for the selected devices.


To discover inventory using the Software/Hardware Inventory wizard

- 1 Launch the wizard from the Device Management, [Devices](#) tab or from the Group Management, [Groups](#) tab.
    - Click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory**.
  - 2 Select **Run: Now** to discover inventory immediately after the wizard is complete, or select **Run: Later** and enter a date and time for inventory discovery. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.
    - Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.
  - 3 Select whether or not to enable Wake-on-LAN for the device. Selecting **Yes** from the drop-down list allows HPCAS to turn on the device to discover inventory, if necessary.
  - 4 Review the summary information and click **Submit**.
  - 5 The job is successfully created. Click **Close** to exit the wizard.
- Use the [Current Jobs](#) tab to view all pending Management Jobs.

# Patch Compliance Discovery Wizard

Use the Patch Compliance Discovery wizard to configure patch compliance schedules for selected devices and groups.

To discover patch compliance

- 1 Launch the wizard from the Device Management, [Devices](#) tab or from the Group Management, [Groups](#) tab.
  - Click the **Inventory Collections**  toolbar button then select **Discover Patch Compliance**.

- 2 Select **Run: Now** to schedule the job to run immediately after the wizard is complete, or select **Run: Later** and enter a date and time for the job to begin. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks**, then select the **Interval** from the drop-down list.



Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.


- 3 Select whether or not to enable Wake-on-LAN for the device. Selecting **Yes** from the drop-down list allows HPCAS to turn on the device if necessary.
- 4 Review the summary information and click **Submit**.
- 5 The job is successfully created. Click **Close** to exit the wizard.

When finished, use the Reporting tab to view compliance reports for the selected devices or groups.

## Application Usage Collection Wizard

Use the Application Usage Collection wizard to collect application usage data for targeted devices or groups. The Application Usage Collection wizard installs the Collection Agent on the targeted devices then returns usage data based on the filters you create and enable. See [Usage Collection](#) on page 161 for additional information.

To discover application usage data

- 1 Launch the wizard from the Device Management, [Devices](#) tab or from the Group Management, [Groups](#) tab.
  - Click the **Inventory Collections**  toolbar button then select **Discover Application Usage**.
- 2 Select **Run: Now** to schedule the job to run immediately after the wizard is complete, or select **Run: Later** and enter a date and time for the job to begin. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.



Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

Collecting application usage data on a weekly basis is recommended.

- 3 Select whether or not to enable Wake-on-LAN for the device. Selecting **Yes** from the drop-down list allows HPCAS to turn on the device if necessary.
- 4 Review the summary information and click **Submit**.
- 5 The job is successfully created. Click **Close** to exit the wizard.

Use the [Current Jobs](#) tab to view all pending Management Jobs.

## Power Management Wizard

Use the Power Management wizard to turn on, turn off, or restart selected devices.





Remotely turning on a device requires the Wake-On-LAN capability built into modern computers. Wake-On-LAN is a management tool that enables the HPCAS server to remotely power on managed devices by sending a packet over the network. Devices may need to have their BIOS configured to enable remote wake up feature. Refer to your hardware documentation for details. BIOS settings for HP devices can be modified and deployed using HPCAS. See [Publishing BIOS Settings](#) on page 225 for details.



Selecting the Power Off feature for Windows XPe devices results in the device rebooting once before powering off. This is necessary to clear the internal cache on the XPe device and is normal operation.

### To remotely turn on, turn off, or restart a device

- 1 Launch the wizard from the Device Management, Devices area or from the Group Management, [Groups](#) area by clicking the **Power Management**  toolbar button.
- 2 Select the Power Management function from the drop-down list. You can choose to turn on, turn off, or restart the selected device.


- **Power On** – turn on the selected device
  - **Power Off** – turn off the selected device
  - **Reboot** – restart the selected device
- 3 Configure the run schedule for the job. Select **Run: Now** to schedule the job to run immediately, or select **Run: Later** to schedule a date and time for the job to begin. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.  
  
 Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.
  - 4 Review the summary information and click **Submit**.
  - 5 The job is successfully created. Click **Close** to exit the wizard.
- Use the [Current Jobs](#) tab to view all pending Management Jobs.

## Group Creation Wizard

Software or patches must be deployed to groups of managed devices in your database. Use the Group Creation Wizard to define device groups based on devices you specify, discovered devices, or on the devices returned as part of a reporting query.

The Group Creation Wizard steps vary depending on the type of group you are creating.


### To create a static group

- 1 Do one of the following to launch the wizard
  - From Group Management, General tab click **Create a new Static Group**.
  - From the [Groups](#) tab click the **Create a New Static Group** toolbar button .
- 2 Click **Next** to begin creating the group.
- 3 Enter a name and description for the group.
- 4 Click **Next**.

- 5 Select the devices you want to include in the group by checking the box in the first column for each device to include. You can use the Search function to narrow the list of devices, if necessary.
- 6 Click **Next**.
- 7 Review the summary information. Make sure the number of devices you selected matches the **# Devices** summary. Click **Previous** if you need to modify the group.
- 8 Click **Create**. The group is successfully created.
- 9 Click **Close** to exit the wizard.

### To create a Dynamic Discovery Group

Discovery group membership is based on the devices found during an LDAP query or domain scan.

- 1 To launch the wizard:
  - From Group Management, General tab, click **Create a new Discovery Group**
  - From the **Groups** tab, click the **Create a New Group** toolbar button  then select **Create a new Dynamic Discovery Group**.
- 2 Click **Next** to begin creating the group.
- 3 Enter a name and description for the group.
- 4 Click **Next**.
- 5 Select the discovery source.
  - **LDAP/Active Directory** – Type the LDAP Host and Port number, User ID, password (if required) and the DN to query.  
Also, select the scope, advanced filter or a device limit to apply to the query.
  - **Domain** – to scan a network domain for devices to import, type the domain name (for example, type ABC for a full domain scan of the ABC domain) or part of the domain name and a wildcard character (ABC\* returns all devices from domains beginning with ABC). To include specific devices from a domain, use the following syntax, domain\device. For example, Sales\WS\* returns only devices beginning with WS from the Sales domain.  
Use an exclamation mark ! to exclude specific devices from a domain.


For example, `Sales,!Sales\WS*` will return all devices from the Sales domain with the exception of devices beginning with `WS`.

- 6 Click **Next**.
- 7 Configure the refresh schedule for the dynamic group.
  - **Run:** Select whether to update dynamic group membership based on an interval of hours, days, or weeks.
  - **Interval:** Select the specific interval (hours, days, or weeks).
  - **Starting on:** Use the drop-down lists to select the date the group should be refreshed.
  - **Current Server Time** displays the current time of the HPCAS server.
- 8 Click **Next**.
- 9 Review the summary information and click **Create**.
- 10 Click **Close** to exit the wizard.

A Discovery Group is created containing the devices found during the LDAP query or domain scan. If discovered devices were not already a part of HPCAS, they are automatically added to the device list. The device membership of this group will update based on the refresh schedule you configured.

### To create a Dynamic Reporting Group

Reporting groups are created using the devices returned in a report query.

- 1 To launch the wizard from the Reporting area, Action Bar click **Create a new Dynamic Reporting Group** .
- 2 Click **Next** to begin the wizard.
- 3 Enter a name and description for the group.
- 4 Click **Next**.
- 5 Configure the refresh schedule for the dynamic group.
  - **Run:** Select whether to update dynamic group membership based on an interval hours, days, or weeks.
  - **Interval:** Select the specific interval (hours, days, or weeks).
  - **Starting on:** Use the drop-down lists to select the date the group should be refreshed.




- **Current Server Time** displays the current time of the HPCAS server.
- 6 Click **Next**.
- 7 Review the summary information and click **Create**.
- 8 A Reporting Group is created containing the current devices in the report query. The device membership of this group will be updated based on the refresh schedule you configured.
- 9 Click **Close** to exit the wizard.

## Software Deployment Wizard

Use the Software Deployment Wizard to entitle and deploy software to managed devices in your environment.

To entitle and deploy software using the Software Deployment wizard

- 1 To launch the wizard:
  - From the Software Management General area, click **Deploy**.
  - From the Software tab, Software Details window, or Group Details window, click the **Deploy Software**  toolbar button.
- 2 Click **Next** to begin the wizard.
- 3 To select the software to entitle and deploy check the box in the first column.
- 4 Click **Next**.
- 5 To select the groups that will be entitled and targeted for deployment check the box in the first column.
- 6 Click **Next**.
- 7 Configure the run schedule for the software deployment job. Select **Run: Now** to deploy the software right away, or select **Run: Later** to schedule a date and time for software deployment. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.




Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

- 8 Click **Next**.
- 9 Review the summary information and click **Submit**. The job is successfully created and added to Current Jobs.
- 10 To view the current software deployment jobs click the Current Jobs tab.
- 11 Click **Close** to exit the wizard.

## Service Import Wizard

Use the Service Import Wizard to import services from the ChangeControl directory on the HPCAS server machine into a Software, Patch, or OS library.


To import a service using the Service Import wizard

- 1 Launch the wizard from the Software Management, Software area, Patch Management, Patch area or the OS Management, Operating Systems area by clicking the **Import Service**  toolbar button.
- 2 Select the service to import. All service decks available within the HPCAS server's ChangeControl directory appear in the list.  
  
The fourth section of each service's file name contains a descriptive name for that software, patch, or OS. For example, PRIMARY.SOFTWARE.ZSERVICE.ORCA is the service deck for the Orca software application.
- 3 Review the summary information and click **Import**. The service is imported and will be available in the HPCAS library.
- 4 Click **Close** to exit the wizard.

## Service Export Wizard

Use the Service Export Wizard to export services from the HPCAS Software, Patch, or OS libraries to the ChangeControl directory on the HPCAS server machine.

To export a service using the Service Export wizard


- 1 Select a service to export (Software, Patch, or OS).
- 2 Launch the wizard from the Software Management, Software area, Patch Management, Patch area, or the OS Management, Operating Systems area by clicking the **Export Service**  toolbar button.
- 3 Review the summary information and click **Export**. The service is exported to the HPCAS server's ChangeControl directory.
- 4 Click **Close** to exit the wizard.

The fourth section of each service's file name contains a descriptive name for that software, patch, or OS. For example, PRIMARY.SOFTWARE.ZSERVICE.ORCA is the service deck for the Orca software application.

## Software Synchronization Wizard

Use the Software Synchronization Wizard to create a Software Synchronization Job that will automatically deploy all entitled software to group members that do not have the software installed. Also, Software Synchronization Jobs ensure all new group members automatically receive all entitled software.

To create a Software Synchronization Job


- 1 On the Group Details window, Software tab, click the Synchronize Software toolbar button to launch the wizard.
- 2 Configure the run schedule for the software synchronization job. Select **Run: Now** to schedule the job to run right away, or select **Run: Later** to schedule a date and time for the job. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.  
  
 Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.
- 3 Use the **Wake On Lan** drop-down list to enable Wake-on-LAN for devices in the group. This allows HPCAS to power on the devices to perform the required job actions.
- 4 Review the summary information and click **Submit**.

- 5 Click **Close** to exit the wizard.

## Patch Deployment Wizard

Use the Patch Deployment wizard to entitle and deploy patches to managed devices in your environment.

To entitle and deploy patches using the Patch Deployment wizard

- 1 To launch the wizard do one of the following:
  - from the Patch Management General tab by clicking **Deploy**
  - from the Patch Library area, Patch Details, or Group Details windows click the **Deploy Patch**  toolbar button.
- 2 Click **Next** to begin the wizard.
- 3 Select a deployment method.

**Compliance Enforcement** – Select this method to determine which patches are applicable to the target devices. Only applicable patches will be installed. As new patches are entitled to the devices, they will be installed the next time this job runs. You must create a recurring schedule in order to enforce patch compliance on an ongoing basis.

**Manual Selection** – Select this method to deploy the patches to the target devices. If the patches are not applicable to the devices, the job may end in error. Use this method to deploy the patches to target devices one time without creating a recurring compliance schedule.
- 4 To select the patches to entitle and deploy check the box in the first column.
- 5 Click **Next**.
- 6 To select the groups that will be entitled and targeted for deployment check the box in the first column.
- 7 Click **Next**.
- 8 Configure the run schedule for the job. Select **Run: Now** to schedule the job to run right away, or select **Run: Later** to schedule a date and time for the job. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.



A recurring schedule is only available when you select the **Compliance Enforcement** deployment method.

- 9 Click **Next**.
- 10 Review the summary information and click **Submit**. The job is successfully created and added to Current Jobs.
- 11 To view the current patch deployment jobs click the Current Jobs tab.
- 12 Click **Close** to exit the wizard.




After a patch is deployed it cannot be removed from a device.

## Service Entitlement Wizard

The Service Entitlement Wizard entitles groups of devices to software, operating system images, and patch services.

To add group entitlement using the [Service Entitlement wizard](#)


Launch the wizard from the Patch Management, Patches tab or from the OS Management, Operating Systems tab.

- 1 Select the patches to entitle to a group then click the **Add Group Entitlement**  toolbar button.
- 2 To select the groups that will receive entitlement to the service click the check box in the left column.
- 3 Click **Next**.
- 4 Review the summary information and click **Submit**. The job is successfully created and added to the current jobs.
- 5 To view the current software removal jobs click the Current Jobs tab.
- 6 Click **Close** to exit the wizard

## Software Removal Wizard

The Software Removal wizard uninstalls software from selected devices or groups.


To remove software using the Software Removal wizard

- 1 From the Software Details window or the Group Details window, select the software to remove.
- 2 Click the **Remove Software**  toolbar button to launch the wizard.
- 3 Click **Next** to begin the wizard.
- 4 Configure the run schedule for the software removal job. Select **Run: Now** to remove the software right away, or select **Run: Later** to schedule a date and time for software removal.
- 5 Click **Next**.
- 6 Review the summary information and click **Submit**. The job is successfully created and added to the current jobs.
- 7 To view the current software removal jobs click the Current Jobs tab.
- 8 Click **Close** to exit the wizard.

## User Creation Wizard

The User Creation wizard adds additional console users.

To create additional console users using the User Creation wizard

- 1 To launch the wizard from the Configuration tab, Console Access section click the **Create New User**  toolbar button.
- 2 Type a **User ID**, for example `jdoe`. This is what you will use to log in to the console.



User IDs cannot contain reserved characters ( underscore `_`, space, or slashes `/` or `\` ). Reserved characters are automatically removed when the User ID is generated. For example, if you attempted to create User ID, `jdoe_1`, you would end up with `jdoe1`.

- 3 Type a **Display Name**. This is the name that will be displayed in the Creator field for management jobs.
- 4 You can optionally type a **Description** for the user.
- 5 Type a **Password** and then confirm your entry in the **Confirm Password** text box.
- 6 Click **Create**. The user is created successfully.



If a user with the same User ID already exists, you will not be able to create the new user.


- 7 Click **Close** to exit the wizard.

The new console user is displayed in the list of Users. Click the User ID to modify or view the console user properties.

## OS Deployment Wizard

The OS Deployment wizard deploys operating systems to managed devices. Operating systems are deployed in either attended or unattended mode. See the Configuration tab, [OS Management](#) section on page 155 to select the deployment mode.

### To deploy an operating system using the OS Deployment wizard

- 1 To launch the wizard from the OS Management section, General or Operating Systems areas click the **Deploy Operating System**  toolbar button.
- 2 Click **Next** to begin the wizard.



Groups created for OS deployment should follow some basic guidelines, for example, all devices within the group should have similar, compatible hardware.

- 3 Select the groups for operating system entitlement and deployment.



You can only assign a single Linux operating system service to a given target device.

- 4 Click **Next**.
- 5 Select the OS deployment method you will use for this job.

- **Local Service Boot (LSB):** Select this option if you want to install LSB in order to deploy the OS. An advantage of LSB is that existing devices 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.
  - **Local CD or PXE Server:** Select this option if you will be using a PXE Server or Service CD to install the operating system on your devices.
- 6 If you have HP Client Automation Standard installed, you are prompted to select whether or not to **Migrate User Data and Settings**. Select **Yes** to deploy the Settings Migration Utility along with the operating system. During the operating system deployment, the Settings Migration Utility launches and prompts users to back up their settings. After the new operating system is installed, deploy the Settings Migration Manager service to the device to restore settings. See [Settings Migration](#) on page 249 for additional information.
    - If you are using unattended mode for OS deployment and select Settings Migration, this process will also run unattended. The required information for Settings Migration—computer name and password—are automatically generated. The end user should use the **Restore from operating system migration** feature in the Settings Migration Utility to restore settings stored during an unattended OS deployment.
  - 7 Configure the run schedule for the job. Select **Run: Now** to deploy the OS right away, or select **Run: Later** to schedule a date and time for OS deployment. To configure a recurring schedule, select **Every 'x' Hours, Days, or Weeks** then select the **Interval** from the drop-down list.
    - Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.
  - 8 Configure any additional job tasks in the **Additional Parameters** section.
  - 9 Click **Next**.
  - 10 Review the summary information and click **Submit**. The job is successfully created and added to Current Jobs.
  - 11 To view the current OS deployment jobs click the Current Jobs tab.
  - 12 Click **Close** to exit the wizard



# Usage Collection Filter Creation Wizard

Use the Usage Collection Filter Creation Wizard to create new usage collection filters.

To create a new collection filter

- 1 To launch the wizard click the Create New Filter toolbar button on the Usage Collection tab in the Configuration tab's, Reporting section.
- 2 To configure the filter parameters type criteria into each text box.  
Only type values for those fields you wish to filter usage data against. Empty text boxes are ignored and not used as part of the filter criteria.  
The values you enter are compared against the file header in the software executable to determine if collected usage data meets the filter criteria.  
See [Defining Usage Criteria](#) on page 164 for methods on determining how to filter for a specific piece of software.




Configuring filters to collect and report on more than 50 applications will result in a large amount of data that can create severe reporting performance issues over time.

- 3 Click **Create**.
- 4 Click **Close**.  
A new filter is added to the Collection Filters list.

# Infrastructure Deployment Wizard

Use the Infrastructure Deployment Wizard to install the Infrastructure service to Infrastructure Servers to enable remote services such as data caching.

To deploy the Infrastructure service


- 1 From the Configuration tab, Infrastructure Management section's Servers tab click the **Deploy the Infrastructure Service**  toolbar button to launch the wizard.

- 2 Enter deployment credentials and click **Next**.
- 3 Select the installation drive for the Infrastructure Service and click **Next**.
- 4 Configure the run schedule for the job. Select **Run: Now** to deploy the service right away, or select **Run: Later** to schedule a date and time for deployment.
- 5 Click **Next**.
- 6 Review the summary information and click **Submit**.
- 7 Click **Close** to exit the wizard

## Infrastructure Removal Wizard

Use the Infrastructure Removal Wizard to remove the Infrastructure service from devices in the Infrastructure Servers group.


To remove the Infrastructure service

- 1 Launch the wizard from the Configuration tab, Infrastructure Management section's Servers tab toolbar.
- 2 Select the devices from which you want to remove the Infrastructure Service and click **Remove the Infrastructure Service**  toolbar button.
- 3 Select **Run: Now** to remove the service immediately after the wizard is complete, or select **Run: Later** and enter a date and time for removal.
- 4 Click **Next**.
- 5 Review the summary information and click **Submit**.
- 6 Click **Close** to exit the wizard.

## Infrastructure Location Creation Wizard

Use the Infrastructure Location Creation Wizard to add new Infrastructure Locations (subnets) to which Infrastructure Servers can be assigned.

### To add a new Location

- 1 Launch the wizard from the Configuration tab, Infrastructure Management section, Location tab toolbar.
- 2 Click the **Create a New Location**  toolbar button
- 3 Type a description for the Location as well as the subnets you want to include as part of this Infrastructure Location. Use the Subnet Address Calculator to help determine which subnet addresses to use.
- 4 Click **Create**.
- 5 Click **Close** to exit the wizard.



## 8 Preparing and Capturing OS Images

Use the Image Preparation Wizard to prepare and capture operating system images for deployment to devices in your environment. After an image is captured, use the Publisher to publish it to HPCAS.

When you run the wizard, it collects inventory information associated with the image and sends the image file to the `\upload` directory on your HPCAS server (C:\Novadigm\OSManagerServer\upload by default).



Images should be sent to a HPCAS Server in a non-production lab environment to prevent performance issues.

The Image Preparation wizard is available as part of the `ImageCapture.iso` file on the HPCAS media within the `OSManagement\ISO\CaptureCD` directory.

- Create an Image Preparation Wizard CD from this file before you begin.

Preparation and capture steps vary depending on the operating system. For OS-specific instructions, see the appropriate section below:

- [Windows OS Image](#) below
- [Thin Client OS Image](#) on page 199

### Windows OS Images

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

- [Task 1 - Prepare the Reference Machine](#) on page 189
- [Task 2 - Create Answer Files](#) on page 192
- [Task 3 - Run the Image Preparation Wizard](#) on page 194

#### Task 1 - Prepare the Reference Machine

The image created on the reference machine (the machine used to create an image of the operating system) is deployed to target devices. Before using the

Image Preparation Wizard (`prepwiz.exe`) to create the image, do the following:

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



The OS must be stored on the C: drive because only the C: drive is captured.

- 2 Customize the OS as necessary. This may require you to install a set of basic or required applications. Be sure to include the latest service pack for the OS and applications. Be sure to include all required drivers for all device configurations 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>**



Windows XP images require Service Pack 1 at a minimum.

- 3 You must deploy the Management Agent to the reference machine or install the agent manually using the HPCAS media. The agent is required so that when the image is deployed, the device can connect to the HPCAS Server.



If you will be capturing and deploying Windows Vista images with HPCAS, you must copy two utilities to the HPCAS Server. These utilities are found on the Windows Vista media and within the default installation directory of the Windows Automated Installation Kit (WAIK). WAIK is available from the Microsoft web site. It is not included as part of a normal Vista installation.

- 1 **Create** `\utilities\Program Files` in  
`C:\Novadigm\OSManagerServer\OSM\SOS\winpe\`
- 2 **Copy** `bootsect.exe` from `\boot` on the Windows Vista media to  
`C:\Novadigm\OSManagerServer\OSM\SOS\winpe\utilities\`  
`Program Files\`
- 3 **Copy** `imagex.exe` from `C:\Program Files\Windows`  
`AIK\Tools\x86` to  
`C:\Novadigm\OSManagerServer\OSM\SOS\winpe\utilities\`  
`Program Files\.`

## Additional Recommendations

- 1 Configure the BIOS power management so that the machine does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the HPCAS server is finished.
- 2 Keep the image file size as small as possible. The ideal configuration would be a partition just large enough to fit the operating system, plus additional space for the Management Agent.



HP supports deploying the image to the primary boot partition of the primary boot drive.

The Image Preparation Wizard offers several options to assist in keeping the image file size down as described below.

- **Resize partition before OS upload.**

Resizes the partition to a smaller size.

- **Optimize compression of unused disk space.**

If you want to zero free space at the end of the system drive partition, select the appropriate option in the Image Preparation Wizard.

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.

- **Span image files.**

If you want to span your images, select the appropriate option in the Image Preparation Wizard. This means that the image file is broken 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 HPCAS Server. If you choose not to use the spanned image option, your images must be less than 4 GB.

In addition, to minimize the footprint of the image:

- **Create free space.**

We recommend 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 1, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on

the disk. The Management Agent can then use the free space on the volume for application installations.

- **Disable hibernation if you are using a laptop.**
- **Disable page file.**
- **Turn off System Restore.**

## Task 2 - Create Answer Files

Create the answer files. See the following sections for details:

- [Prepare unattend.xml \(for Windows Vista deployments\)](#) on page 192
- [Create Sysprep.inf \(for non-Vista OSs only\)](#) on page 192

### Prepare unattend.xml (for Windows Vista deployments)

Copy the sample `unattend.xml` from the `\samples` directory on the Image Preparation CD you created (from `ImageCapture.iso`) to `C:\windows\system32\sysprep`. You may need to modify this file for your environment.

### Create Sysprep.inf (for non-Vista OSs only)

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. For information on Microsoft Sysprep for Windows XP and Windows 2000, go to `\support\tools\deploy.cab` on the installation media. `Deploy.cab` contains three help files (`Deploy.chm` contains detailed Sysprep information).

In the last step of image creation, the Image Preparation Wizard runs Microsoft Sysprep for you. It strips out all of the security identifiers in the image and resets 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. See 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 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`) to create Sysprep files. 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.



When attempting to capture a Windows 2000 image, you must remove the `[SYSPREPMASSTORAGE]` section from the `Sysprep.inf` file. If this section is not removed, the following error may occur "An error occurred while trying to update your registry. Unable to Continue."

Sample `Sysprep.inf` files are available on the Image Preparation CD you created (`ImageCapture.iso`) 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.

When finished with these steps, continue with [Task 3 - Run the Image Preparation Wizard](#) on page 194.

## Task 3 - Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

- 1 Checks if there is enough free disk space on the machine and verifies that the Management Agent is installed. See [Task 1 - Prepare the Reference Machine](#) on page 189. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
- 2 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
- 3 Runs Microsoft Sysprep on supported operating systems (Windows XPe, CE, and Embedded Linux do not support Sysprep).
- 4 Restarts the reference machine into the Service Operating System (booted from the appropriate media). The Service OS runs to collect the image and its associated files.

5 Creates and copies the following files to *SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\upload* on the HPCAS Server:

If you chose to create a pre-Vista image, the files uploaded are:

- *ImageName.IMG*  
This file contains the 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 a Windows Vista image, 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.

▶ 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.log*) is also available in *SystemDrive:\Program Files\Hewlett-Packard\CM\IntegrationServer\upload* after the image is deployed.

To use the Image Preparation Wizard

▶ Before continuing, set the reference machine to boot from the CD-ROM drive. You must do this because the Image Preparation Wizard CD-ROM is bootable. After you run the Image Preparation Wizard, it reboots the device to the appropriate service operating system that boots from the media in order to capture the image.

- 1 Insert the Image Preparation Wizard CD-ROM you created into the CD-ROM drive of the reference machine. This CD is created using the `ImageCapture.iso` found within the `OSManagement\ISO\CaptureCD` directory on your HPCAS media.
  - 2 If autorun is enabled, the HPCAS OS Preparation and Capture CD homepage opens.
  - 3 Click **Browse** to open the `\image_preparation_wizard\win32\` directory.
  - 4 Double-click **prep wiz.exe**.
    - While you are capturing the image, the Image Preparation Wizard verifies that the `C:\Sysprep` folder exists and that Management Agent is installed before continuing. If you see the following message, you will need go back and install the Management Agent on the reference machine then restart the Image Preparation Wizard:  

```
This computer does not have the CM Application Manager installed. You may not be able to manage the target computers with the OS Manager product.
```
- The Image Preparation Wizard opens.
- 5 Click **Next**. The End User Licensing Agreement window opens.
  - 6 Click **Accept**. The Identify the CM OS Manager Server window opens
  - 7 Type the IP address or host name and port for the HPCAS server. This must be specified in the following format: `xxx.xxx.xxx.xxx:port`. The HPCAS server port reserved for OS imaging is 3469.
- If the Image Preparation Wizard cannot connect to the HPCAS server, a message opens and you must:
- Click **Yes** to continue anyway.
  - Click **No** to modify the host name or IP address.
  - Click **Cancel** to exit the Image Preparation Wizard.
- 8 Click **Next**. The Image Name window opens.
  - 9 Type a name for the image file. This is the image name that will be stored in the `/upload` directory on the HPCAS server.
  - 10 Click **Next**.
  - 11 Use the text box to enter or modify Sysprep options.
  - 12 Click **Next**.

- 13 Type a description for the image file and click **Next**. The Options window opens.
- 14 Select the appropriate options.

**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 2000 and above.

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.

**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.

**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 disk. Note that this may take some time depending on the size of the hard drive.

- 15 Accept the defaults and click **Next**. The Summary window opens.
- 16 Click **Start**. If you are working with an APIC machine, a new window opens.
- 17 If necessary, select the check box.



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

- 18 Click **Next**. If you selected the check box in the previous step, the Select Windows CD window opens.
- 19 Browse to the Windows CD-ROM.
- 20 Click **Next**.
- 21 Click **Finish** to run Sysprep.

The Image Preparation Wizard will start Sysprep, this can take 15-20 minutes to complete. Sysprep will automatically reboot the machine when complete.

22 Click **OK**. Sysprep starts.



If you are using Windows 2000, Sysprep may take some time to run even if you do not see any activity on the screen.

After Sysprep restarts the device, the device must boot 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 press 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 instead) you will need to restart the process from [Task 1 - Prepare the Reference Machine](#), above.



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.

23 The Image Preparation Wizard connects to the network, and stores the image on the HPCAS 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
```

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

Now you can use the Publisher to publish the image file to the HPCAS server for distribution to managed devices. See [Publishing Operating System Images](#) on page 218.

# Thin Client OS Images

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

- [Windows XPe OS images](#) below
- [Windows CE OS images](#) on page 203
- [Embedded Linux OS images](#) on page 206

## Windows XPe OS images

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

- [Task 1 – Prepare the XPe Reference Machine](#) on page 199
- [Task 2 – Run the Image Preparation Wizard](#) on page 200

► 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 – Prepare the XPe Reference Machine

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

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

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

- 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 Management Agent.

### To install the Management Agent on Windows XPe

- 1 Access the HPCAS media from the Windows XPe Thin Client device.
- 2 On the HPCAS 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 HPCAS server.

The Management Agent is installed.

## Task 2 – Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

- 1 Checks if there is enough free disk space on the machine and verifies that the Management Agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
- 2 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
- 3 Restarts the reference machine into the service operating system (booted from the Image Prep CD you created). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.
- 4 Creates and copies the following files to *SystemDrive:\Novadigm\OSManagerServer\upload* on the HPCAS 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.log*) is also available in *SystemDrive:\Novadigm\OSManagerServer\upload* after the image is deployed.

### To use the Image Preparation Wizard

- 1 Insert the Image Preparation Wizard CD-ROM you created into the CD-ROM drive of the reference machine (Thin client devices require a USB CD-ROM drive). This CD is created using the ImageCapture.iso found within the *OSManagement\ISO\CaptureCD* directory on your HPCAS media.
- 2 If autorun is enabled, the HPCAS OS Preparation and Capture CD homepage opens.
- 3 Click **Browse** to open the *\image\_preparation\_wizard\win32\* directory.
- 4 Double-click **prep wiz.exe**. The Image Preparation Wizard verifies that *etprep.exe* and *fbreseal.exe* are available before continuing. The Welcome window opens.
- 5 Click **Next**. The End User Licensing Agreement window opens.
- 6 Click **Accept**.
- 7 Type the IP address or host name and port for the HPCAS server. This must be specified in the following format: *xxx.xxx.xxx.xxx:port*. The HPCAS server port reserved for OS imaging is 3469.  
  
If the Image Preparation Wizard cannot connect to the HPCAS server, a message opens and you must:
  - Click **Yes** to continue anyway.
  - Click **No** to modify the host name or IP address.
  - Click **Cancel** to exit the Image Preparation Wizard.
- 8 Click **Next**. The Image Name window opens.
- 9 Type a name for the image file. This is the image name that will be stored in the */upload* directory on the HPCAS server.
- 10 Click **Next**. A window opens so you can enter a description for the image.
- 11 Type a description for the image file.

12 Click **Next**. The Options window opens.

13 Select the appropriate options.

**Perform client connect after OS install.**

Select this check box to connect to the HPCAS 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.

14 Accept the defaults and click **Next**. The Summary window opens.

15 Click **Start**.

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

17 Click **OK**.

The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can press 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 XP instead) you will need to restart the process from [Task 1 – Prepare the XPe Reference Machine](#), above.



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.

18 OS Image Preparation Wizard connects to the network, and stores the image on the HPCAS 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
```

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

Now you can use the Publisher to publish the image file to the HPCAS server for distribution to managed devices. See [Publishing Operating System Images](#) on page 218.

## Windows CE OS images

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

- [Task 1 – Prepare the CE Reference Machine](#) on page 203
- [Task 2 – Run the Image Preparation Wizard](#) on page 203

### Task 1 – Prepare the CE Reference Machine

To prepare a CE thin client for image capture, you will need the following:

- HPCAS media
- Image Preparation CD-ROM

Before you capture the image, you must install the Management Agent to the Windows CE device.

[To install the Management Agent to Windows CE](#)


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

The Management Agent is installed.

### Task 2 – Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

- 1 Checks if there is enough free disk space on the machine and verifies that the Management Agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
- 2 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.

- 3 Restarts the reference machine into the service operating system (booted from the Image Prep CD you created). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.
  - 4 Creates and copies the following files to *SystemDrive:\Novadigm\OSManagerServer\upload* on the HPCAS 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.log*) is also available in *SystemDrive:\Novadigm\OSManagerServer\upload* after the image is deployed.

#### To use the Image Preparation Wizard

- 1 Insert the Image Preparation Wizard CD-ROM you created into the CD-ROM drive of the reference machine (Thin client devices require a USB CD-ROM drive). This CD is created using the *ImageCapture.iso* found within the *OSManagement\ISO\CaptureCD* directory on your HPCAS media.
- 2 If autorun is enabled, the HPCAS OS Preparation and Capture CD homepage opens.
- 3 Click **Browse** to open the *\image\_preparation\_wizard\WinCE\* directory.
- 4 Double-click **prep wiz.exe**. The Image Preparation Wizard opens.



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

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

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

- 6 Click **OK**. The wizard prepares the image.

The device boots to the Image Preparation Wizard CD in the CD-ROM drive. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can press 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 [Task 1 – Prepare the CE Reference Machine](#), above.



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.

- 7 OS Image Preparation Wizard connects to the network, and stores the image on the HPCAS 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
```

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

Now you can use the Publisher to publish the image file to the HPCAS server for distribution to managed devices. See [Publishing Operating System Images](#) on page 218.

## Embedded Linux OS images

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

- [Task 1 – Prepare the Embedded Linux Reference Machine](#) below
- [Task 2 – Run the Image Preparation Wizard](#) on page 207

### Task 1 – Prepare the Embedded Linux Reference Machine

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

- HPCAS media
- Image Preparation CD-ROM

Before you can capture the image, the Management Agent must be installed on the embedded Linux thin client.

► For additional thin client device information and instructions for running the installation using NFS, see the installation chapter in the guide or the README file included with `ThinClient.tar`.

### To install the Management Agent on Embedded Linux

- 1 Login to the target thin client device.
- 2 Create a new directory called `/mnt/opt/OVCM`.
- 3 Copy the contents of `ThinClient.tar` (located on the HPCAS media in the `/ThinClient/Linux` directory) to `/mnt/opt/OVCM`.

Depending on your device model, you may have to un-tar these files 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 (would require approximately 7-8 MB free). After un-tarring, you can delete the `ThinClient.tar`.

- 4 To change the current directory to `/mnt/opt/OVCM` and run the installation type:

```
./install -i HPCAS_Server
```

Where `HPCAS_Server` is the hostname or IP address of the HPCAS server.

The Management Agent is installed.

## Task 2 – Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

- 1 Checks if there is enough free disk space on the machine and verifies that the Management Agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.
- 2 Creates an object that contains information (including hardware and BIOS capabilities) about the reference machine.
- 3 Restarts the reference machine into the service operating system (booted from the Image Prep CD you created). The Linux-based portion of the OS Manager Image Preparation Wizard runs to collect the image and its associated files.

- 4 Creates and copies the following files to *SystemDrive:\Novadigm\OSManagerServer\upload* on the HPCAS Server.

- *ImageName.DD*

This file contains the image. Thin Client image files are the same size as the reference machine's flash drive. Embedded Linux 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.log*) is also available in *SystemDrive:\Novadigm\OSManagerServer\upload* after the image is deployed.

### To use the Image Preparation Wizard

- 1 Insert the Image Preparation Wizard CD-ROM you created into the CD-ROM drive of the reference machine (Thin client devices require a USB CD-ROM drive). This CD is created using the *ImageCapture.iso* found within the *OSManagement\ISO\CaptureCD* directory on your HPCAS 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 HPCAS server. This must be specified in the following format: *xxx.xxx.xxx.xxx:port*. The HPCAS server port reserved for OS imaging is 3469.



If the Image Preparation Wizard cannot connect to the HPCAS 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 HPCAS 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 HPCAS 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 press 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 Embedded Linux instead) you will need to restart the process from [Task 1 – Prepare the Embedded Linux Reference Machine](#), above.



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 HPCAS 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
```

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

Now you can use the Publisher to publish the image file to the HPCAS server for distribution to managed devices. See [Publishing Operating System Images](#) on page 218.

## Publishing and Deploying OS images

After you have captured an image, use the Publisher to publish it to HPCAS. For instructions, see [Publishing Operating Systems](#) on page 218 or refer to the Publisher online help.

When published to HPCAS, refresh the OS Library to view the new image. Use the HPCAS console toolbar to deploy the image to selected devices. See [Deploying Operating Systems](#) on page 103 for instructions.





## 9 Using the Publisher

Use the Publisher to publish software, BIOS configuration settings, HP Softpaqs, and operating system images to HP Client Automation Starter and Standard (HPCAS). All published software is available in the Software Management, Software tab of the main HPCAS console. Published operating systems are available within the OS Management, Operating Systems tab.

After publishing software, it must be entitled and deployed to managed devices in your environment.



The Publisher is installed separately from HPCAS with the HP Client Automation Administrator installation file on the product media or by with the HP Client Automation Publisher service in the Software Library. See the installation instructions on page 39 for more information.

### To start the Publisher

- 1 On the device where you installed the Publisher, use the **Start** menu and go to:  
**Start > All Programs > HP Client Automation Administrator > HP Client Automation Administrator Publisher**
- 2 To log in to the Publisher use the HPCAS user name and password. By default, the user name is **admin** and the password is **secret**.

The following sections explain how to use the Publisher for publishing Windows installer files, operating system images, HP Softpaqs, and other software formats to HPCAS.

- [Publishing Software](#) on page 214
- [Publishing Operating System Images](#) on page 218
- [Publishing HP Softpaqs](#) on page 223
- [Publishing BIOS Settings](#) on page 225



Publishing options vary based on the intended target devices and the HPCAS license you have installed:

- Publishing options, **Component Select**, **OS Images**, and **Windows Installer** require HP Client Automation Standard. **HP BIOS Configuration** and HP Softpaq publishing options are available with HP Client Automation Starter and Standard.
- Thin Client Publishing options, **OS Images** and **Component Select**, are available for both HP Client Automation Starter and Standard.

## Publishing Software

Depending on the type of software you intend to publish, you will use one of two publishing options. At the login screen, you are given the choice of Windows Installer to publish Windows Installer files (.msi) or Component Select to use when publishing non-Windows Installer files. The following sections explain the steps for publishing each file type.

- [Publishing Windows Installer Files](#) below
- [Publishing Using Component Select](#) on page 216

### Publishing Windows Installer Files

Windows Installer uses MSI files to distribute software services to your operating system. The Publisher uses the files to create a service that is then published to HPCAS. When the software service is contained in HPCAS, it is ready for distribution to managed devices in your environment.

[To publish Windows Installer files](#)

- 1 Start the Publisher (see, [To start the Publisher](#) on page 213).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.



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

- 3 In the Publishing Options area, select **Windows Installer** and click **OK**.
- 4 Navigate to the Windows Installer file in the left pane. The right pane displays any information that is available for the MSI file you select.
- 5 Click **Next**.
- 6 Review the available Publishing Options.

— **Management Options**

To create an administrative installation point (AIP) select **Use setup** or **Use msixexec**.



The AIP path is a temporary location and will be removed after the publishing session completes.

— **Transforms**

Select and reorder the application of any transform files associated with the Windows Installer file.

— **Additional Files**

Include additional files as part of the AIP.

- Click **Select all** to select all available files listed.
- Click **Select none** to deselect all files.

— **Properties**

View and modify the msi file properties. Some Windows Installer files may require additional command line parameters to deploy correctly. For example, an application may require a custom property to pass a serial number during installation. Use the Properties dialog to include any additional parameters.

- Click **Add** to add a new property.
- Click **Remove** to delete an existing property.
- To modify a property **Name** or **Value**, click the item you want to change and enter the new value.

When you are finished editing your publishing options, click **Next**.

- 7 Use the Application Information section to enter the software service information.
- 8 Use the **Limit package to systems with** section to limit the service to any specific operating system or hardware. Click any link to display the configurable options.
- 9 Click **Next**.

- 10 Review the Summary section to verify the service information you provided during the previous steps. When you are satisfied, click **Publish**.
- 11 Click **Finish** when the publishing process is finished to close the Publisher.

The Windows Installer service is now ready for distribution to your enterprise.

#### To apply additional parameters using a transform file


- 1 Create the transform using Orca or another MSI editor. Be sure to save the transform in the same directory as the Windows Installer file are publishing.
- 2 Start a Windows Installer publishing session. Follow the instructions above for details.
- 3 At the Edit step, click **Transforms**.
- 4 Select the available transform file and continue with the publishing session.

When the software service is deployed, the transform file will be applied, supplying the additional command line parameters.

## Publishing Using Component Select

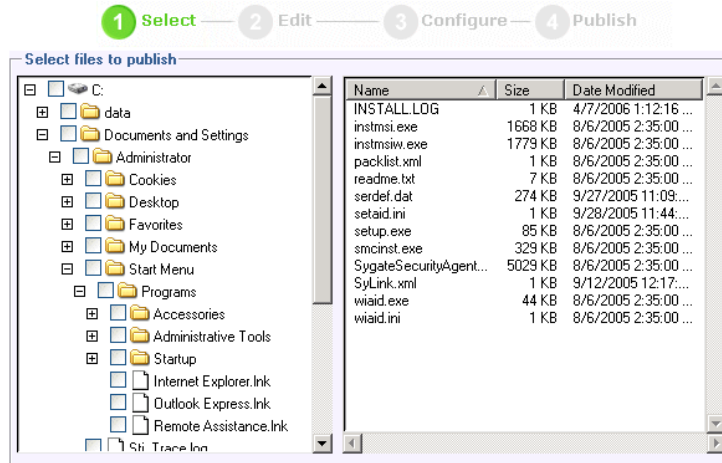
To publish software other than Windows Installer files, use the Component Select option and select the software you want to publish.

#### To publish using Component Select

- 1 Start the Publisher (see [To start the Publisher](#) on page 213).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.  
 Log in to the Publisher using the HPCAS user name and password. By default, the user name is **admin** and the password is **secret**.
- 3 In the Publishing Options area:
  - If you are publishing for thin clients, select **Thin Client Publishing**.
  - From the drop-down list, select **Component Select**.



- 4 Click **OK**. The Select files to publish window opens.



- 5 Select the files to publish and click **Next**.

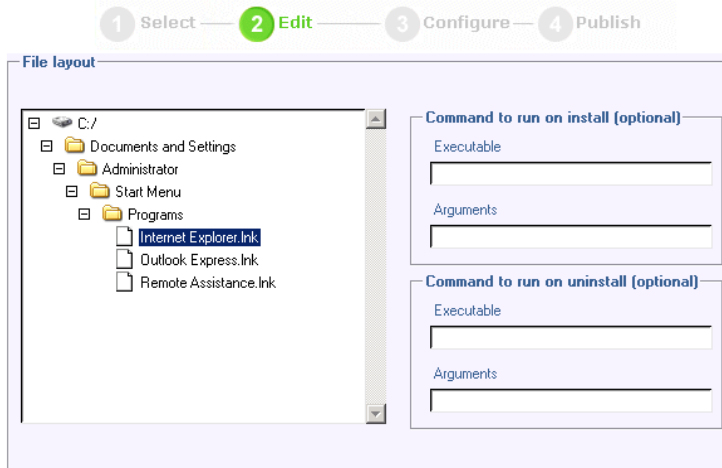


The directory path where the software is located (and published from) will be the directory path to where the software is deployed on target devices.

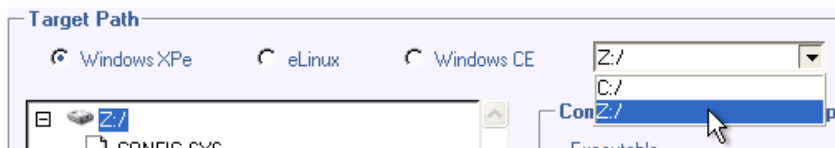


Although network shares are displayed, they should not be used to publish software (since they may not be available during deployment).

The Target Path window opens.



- 6 If you are publishing for thin clients, select the install point, as shown in the following figure.



- 7 Enter the commands to run on application install and uninstall. For example, a command to run on install might be: `C:\temp\installs\install.exe /quietmode /automatic c:\mydestination`

A command to run on uninstall could be: `C:\temp\installs\uninstall.exe /quietmode /automatic`



You can right-click any file to set it as the install or uninstall command.

- 8 Click **Next**. The Application Information window opens.
- 9 Use the Application Information section to enter the software service information.
- 10 Use the **Limit package to systems with** section to limit the service to any specific operating system or hardware. Click any link to display the configurable options.
- 11 Click **Next**.
- 12 Review the Summary section to verify the service information you provided during the previous steps. When you are finished, click **Publish**.
- 13 Click **Finish** when the publishing process is finished to exit the Publisher.

The software service is now ready for distribution to your enterprise.

## Publishing Operating System Images

Operating system images created using the Image Preparation wizard are stored on the HPCAS server in `\Novadigm\OSManagerServer\upload`. Use the Publisher to publish operating system image files (`.IMG`) for distribution to managed devices.

- If you will be publishing `.WIM` images, see [Prerequisites for publishing .WIM images of a Vista OS](#) on page 219.

- See [Publishing OS Images](#) on page 222 for a description of the steps required to use the Publisher to publish OS images.

## Prerequisites for publishing .WIM images of a Vista OS

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

- Have access to the `RadAgent\client` folder on the HPCAS media. This folder is only required the first time you publish a .WIM file or if you want to publish an updated agent package. The Management 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.
- Have WAIK installed (WAIK is available from the Microsoft web site. It is not included as part of a normal Vista installation).
- Copy `filename.wim` and `filename.edm` from the HPCAS Server's `\upload` directory (C:\Novadigm\OSManagerServer\upload, by default) to the device where you are publishing the image.
- Copy `substitutes` and `unattend.xml` to the same directory as `filename.wim`. Samples of these files are available on the Image Capture media in `\samples`. If you choose to use the samples, modify information as needed such as the setting the time zone and entering the product key. See the instructions below for more information. Note that all of these files must have the same prefix. For example, `install.wim`, `install.subs`, and `install.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 an `unattend.xml` file that is used to provide 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 first open the corresponding .wim file before opening *filename.xml*.



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

Do not delete any XML values from this file! If you modify this .xml file incorrectly, you may cause serious problems that can 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-Shell-Setup"
      processorArchitecture="x86"
      publicKeyToken="31bf3856ad364e35" language="neutral"
      versionScope="nonSxS"
      xmlns:wcm="http://schemas.microsoft.com/WMIconfig/2002/State"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
```

```

        <Identification>
            <JoinDomain>anything</JoinDomain>
        </Identification>
    </component>
</settings>

    <cpu:offlineImage
        cpu:source="wim://hpfcovcm/c$/vista_inst/vista.wim#Windows 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-Shell-Setup'][@processorArchitecture='x86']/un:Identification/un:JoinDomain,VistaTeam

```

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

```

<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
        <component name="Microsoft-Windows-Shell-Setup"
            processorArchitecture="x86"
            publicKeyToken="31bf3856ad364e35" language="neutral"
            versionScope="nonSxS"
            xmlns:wcm="http://schemas.microsoft.com/WMIconfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <Identification>
                <JoinDomain>VistaTeam</JoinDomain>
            </Identification>
        </component>
    </settings>

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

```

</unattend>

## Preparing filename.xml

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

## Publishing OS Images

The following section describes how to use the Administrator Publisher to publish operating system images.

### To publish operating system images

- 1 Start the Publisher (see [To start the Publisher](#) on page 213).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.



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

- 3 In the Publishing Options area:
  - If you are publishing for thin clients, select **Thin Client Publishing**
  - From the drop-down list, select **OS Image**
- 4 Click **OK**. The Select OS image file window opens.
- 5 Use the Select window to find and select the file you want to publish. (Images created using the Image Preparation Wizard are stored on the HPCAS server in the \Novadigm\OSManagerServer\upload directory).
- 6 Use the **Description** area to verify the file before you continue. You can also add information to the description if you choose.
- 7 Click **Next**.

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

- a From the **Deployment method** drop-down list box, select ImageX.
- b Leave the **Sources Directory** blank. This is not required.

- c In the **Client media location**, browse to the correct path for the Management Agent media (this is the `RadAgent/client` folder on the HPCAS media).

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

- 8 Click **Next**. The Application Information window opens.
- 9 Use the **Application Information** section to enter the service information.
- 10 Click **Next**. The Summary window opens.
- 11 Review the **Summary** information to verify the package and service information you provided during the previous steps. When you are satisfied, click **Publish**.
- 12 Click **Finish** to exit the Publisher when the publishing process is complete.

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

You can view the published operating system image service in the OS Management section, Operating Systems OS Library list.

## Publishing HP Softpaqs

HP Softpaqs are bundles of support software, which may include device drivers, configuration programs, flashable ROM images, and other utilities available to keep devices up to date and performing at their best.

Softpaqs are available as executable (.EXE) files.

Use the Publisher to publish HP Softpaqs to HPCAS for distribution to managed devices.

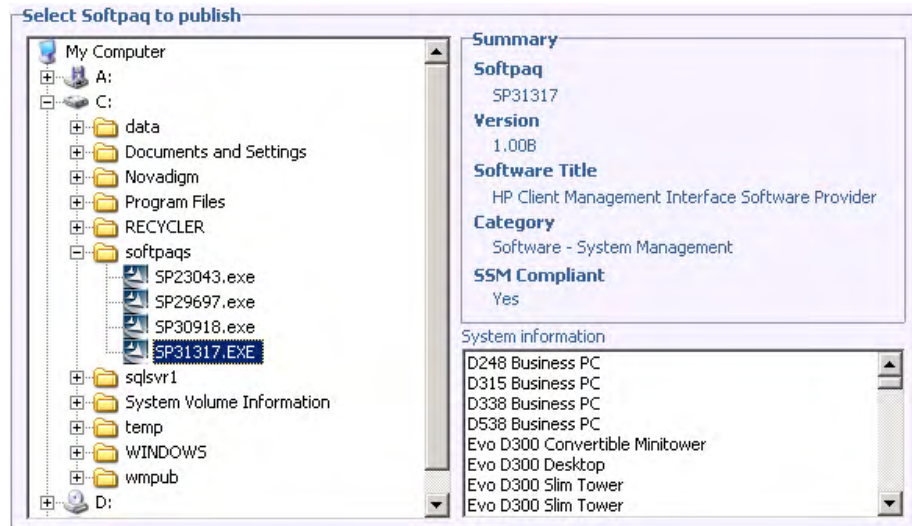
### To publish a Softpaq

- 1 Start the Publisher (see [To start the Publisher](#) on page 213).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.



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

- 3 In the Publishing Options area, select **HP Softpaq** and click **OK**. The Select window opens.



- 4 Select the Softpaq file to publish.
  - The Summary section shows the selected Softpaq information, including whether or not the Softpaq is SSM compliant. If the selected Softpaq is not SSM compliant and no silent install is included as part of the Softpaq, you must extract the Softpaq contents and read the accompanying documentation. Publish the required files and set up the installation method as instructed.
  - The System information dialog box shows all of the hardware the selected Softpaq supports.
- 5 Click **Next**. The Application Information window opens.
- 6 View, and if necessary, modify the Softpaq information. The application information is pre-determined based on what is available from the Softpaq file.
- 7 Click **Next**. The Summary window opens.
- 8 Review the summary information and when satisfied, click **Publish**.



- 9 When the publishing process is complete, click **Finish** to close the Publisher.

The Softpaq is published to HPCAS and is available for distribution to managed devices. View the published Softpaq in the HPCAS console Software Management, Software Library. Deployed Softpaqs are included within the HP Softpaq category group in the Application Self-service Manager on managed devices.


## Publishing BIOS Settings

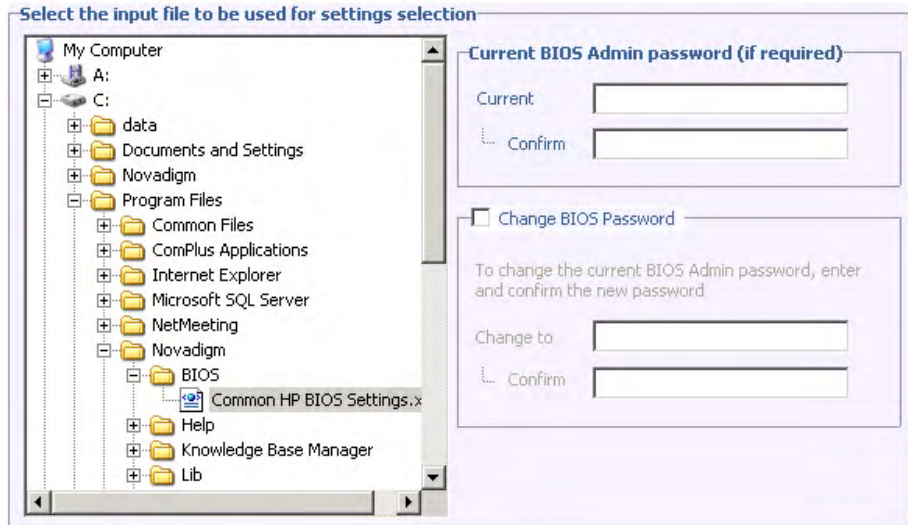
Use the Publisher to publish a BIOS settings file as a service for distribution to client devices. You can use the settings file to update or modify BIOS settings (for example, boot order) or to change the BIOS password on the client device.

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

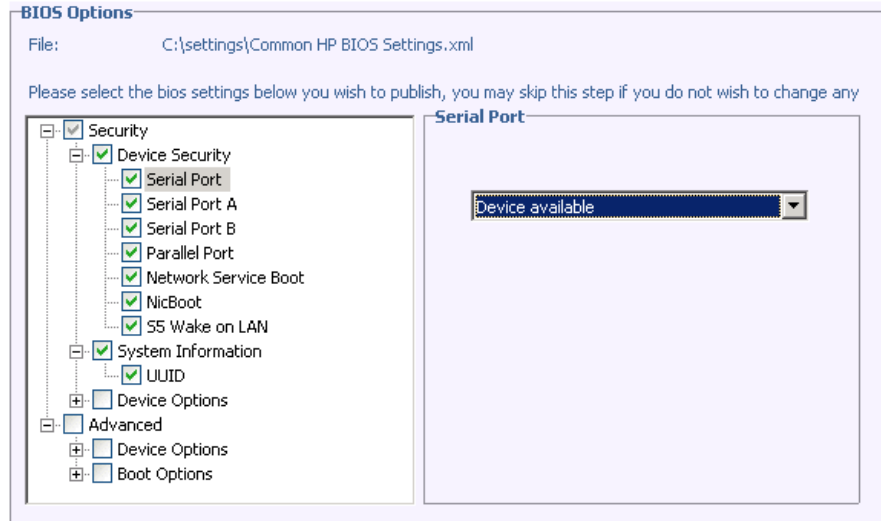
If the sample BIOS settings file does not include the options you require, or you would like to create a settings file for a specific device, see [Creating a BIOS Settings File](#) on page 227.

### To publish BIOS settings

- 1 Start the Publisher (see [To start the Publisher](#) on page 213).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.  
 Log in to the Publisher using the HPCAS user name and password. By default, the user name is **admin** and the password is **secret**.
- 3 In the Publishing Options area, select **HP BIOS Configuration** and click **OK**. The Select window opens



- 4 Select the BIOS settings file to publish. The sample BIOS settings file (Common HP BIOS Settings.xml) is located by default in: C:\Program Files\Novadigm\BIOS.
- 5 In the **Current BIOS Admin Password** area, type and then confirm a BIOS password if required. This is required to change any settings if the target devices have a BIOS password.
- 6 If you want to change the current BIOS password, select, **Change BIOS Password**, then type and confirm the new password. This is required only if you want to change the BIOS password on a client device.
- 7 Click **Next**. The BIOS Options window opens.



- 8 To select the BIOS settings to publish click the check box to the left of the BIOS setting name.
- 9 If you need to change the value of a BIOS setting, click the setting name and adjust the available options as necessary.
- 10 Click **Next**. The Application Information window opens.
- 11 View, and if necessary, modify the application information. Application information is pre-determined based on what is available from the settings file.
- 12 Click **Next**. The Summary window opens.
- 13 Review the summary information and when satisfied, click **Publish**.
- 14 When the publishing process is complete, click **Finish** to close the Publisher.

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

## Creating a BIOS Settings File

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

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

#### To create a BIOS settings file

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

- 2 Type the following:

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

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

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

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

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

- 3 When you are ready to publish BIOS settings, select this file in Step 6 of [To publish BIOS settings](#), above.

## Viewing Published Services

View published software in the Software tab. The following figure shows the Software tab with sample published services and available applications in the HPCAS console.

**Figure 29    Software Library**

HP Client Automation Standard

User: Administrator  
[Home](#) | [Sign Out](#)

Management   Reporting   Configuration

Device Management  
Group Management  
**Software Management**  
Patch Management  
OS Management  
Job Management

Software Management

General   Software   Current Jobs   Past Jobs

Information

Software services published into the repository are displayed below. Click on a software service description to view or modify its properties and entitlements.

Software Library

Search:  Service ID    Contains

10 Items

1 - 4 of 4 Items

<input type="checkbox"/>	Service ID	Description	Software Category	Size (MB)	Entitled Groups	Installed Devices	Last Modified
<input type="checkbox"/>	TEST	test			0	1	2008-04-30 11:04:33
<input type="checkbox"/>	CCM_SMM	HP Client Automation Settings Migration Manager	CAS Applications	11.50	2	1	2008-04-23 02:34:47
<input type="checkbox"/>	CCM_PUBLISHER	HP Client Automation Administrator Publisher	CAS Applications	19.71	8	1	2008-03-25 17:05:32
<input type="checkbox"/>	CCM_TPM_ENABLEMENT	TPM Enablement	ProtectTools	0.08	1	1	2008-02-22 22:35:45

0 items selected

Published operating systems are stored in the Operating System area within the OS Management section of the console.

## HP Client Automation Administrator Agent Explorer

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

Using the Publisher

229



# 10 Using the Application Self-service Manager

The HP Client Automation Application Self-service Manager (ASM) is installed when the Management Agent is deployed to a device. Use the Application Self-service Manager to install software that has been entitled to a device.

The following sections describe how to use the ASM user interface:

- [Accessing the Application Self-service Manager](#) below
- [Application Self-service Manager Overview](#) on page 232
- [Using the Application Self-service Manager User Interface](#) on page 235
- [Customizing the User Interface](#) on page 240
- [HPCA System Tray Icon](#) on page 246

## Accessing the Application Self-service Manager

Access the ASM user interface through the Windows Start menu, or by double-clicking the Application Self-service Manager icon on your desktop.

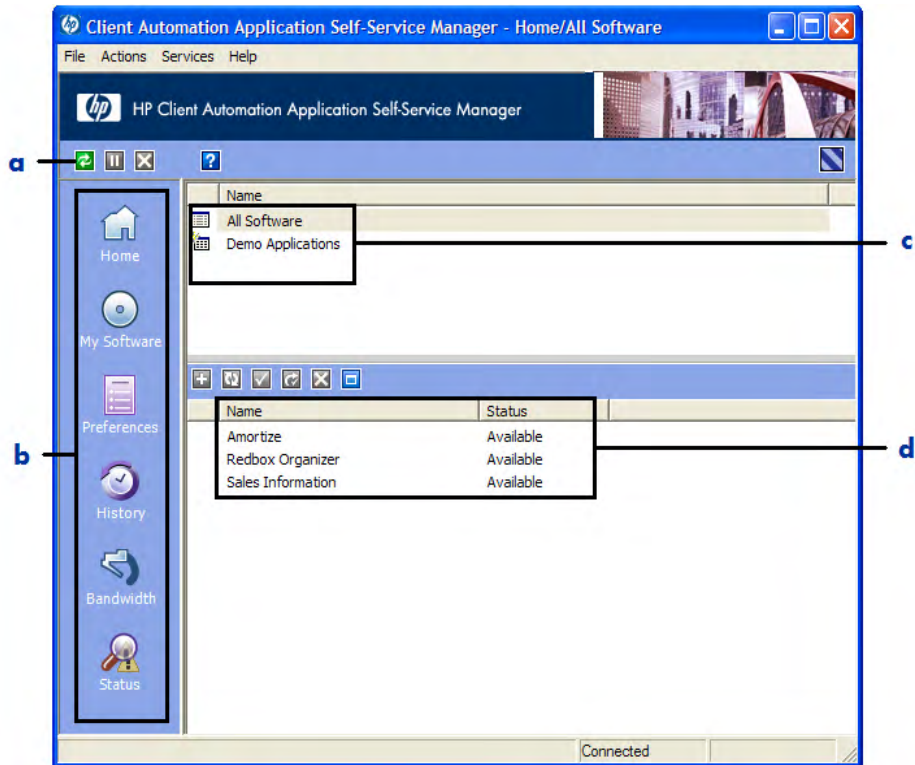
[To access the user interface](#)

- Go to **Start > Programs > HP Client Automation Agent > Client Automation Application Self-Service Manager**  
or
- Double-click the **Client Automation Application Self-Service Manager** desktop shortcut.

# Application Self-service Manager Overview

The ASM user interface has four main sections that allow you to manage available software, view information and status for software in your catalog and customize the user interface display.

**Figure 30 Application Self-service Manager user interface**



## Legend

- a Global Toolbar** — Allows you to refresh the catalog and pause or cancel the current action
- b Menu Bar** — Displays various menu choices available while using the Application Self-service Manager
- c Catalog List** — Lists the different software catalogs available
- d Service List** — Lists the applications to which you are entitled



The following sections describe the user interface sections in more detail:


- [Global Toolbar](#) below
- [The Menu Bar](#) below
- [Catalog List](#) on page 234
- [Service List](#) on page 234

## Global Toolbar



The Global Toolbar allows you to refresh the catalog, pause the current action, or cancel the current action. When an action has been paused, no other action can take place until you either resume the action by clicking the **Pause** button again, or cancel the paused action by clicking the **Cancel** button.

Any time one of the buttons in the Global Toolbar is not available for the current action, it will appear grayed-out.


### To refresh the catalog

- To refresh the selected catalog using the Global Toolbar, click **Refresh** .

### To pause or resume the current action

- To pause the current action using the Global Toolbar, click **Pause** .
- To resume a paused action, click **Resume** . (The **Pause** button is replaced with this button after you pause an action).

### To cancel the current action

- To cancel the current action using the Global Toolbar, click **Cancel** .

## The Menu Bar

Use the Menu Bar to configure and customize the Application Self-service Manager.

The following sections describe each icon on the Menu Bar.

## Home

Click this button to access your home catalog.

## My Software

Click this button to display only those services that you have installed.

## Preferences

Click this button to access various display options, service list options, and connection options for the ASM.

At any point you can click **OK**, **Apply**, or **Cancel** in the top right corner of the Preferences section to keep or disregard any changes you make.

# Catalog List

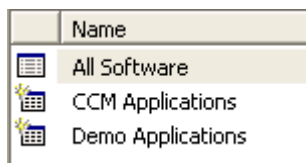
The Catalog List section lists the available software catalogs and any virtual catalogs.




## To select a catalog

- In the Catalog List, click the catalog you want to view in the Service List section. To refresh the catalog, right-click the name of the catalog and select **Refresh** from the shortcut menu.

## Virtual Catalogs

Virtual catalogs are subsets of the default catalog defined by the administrator in HPCAS in the Software Details. Any services with the same catalog group value will be grouped together in a virtual catalog. The following image displays a few sample catalogs:






	Name
	All Software
	CCM Applications
	Demo Applications

# Service List

The Service list section lists the applications available to you. A check mark appears next to software that is already installed. The column headings

displayed can be changed to suit your needs, see [Preferences](#) on page 234 for more information.

**Table 15    Buttons in the Service List Section**

Button	Action	Description
	Install	Installs the selected service on your machine.
	Remove	Removes the selected service from your machine.
	Expand/Collapse	Expands or collapses the selected service.



The buttons in the Service List section are gray when they are not available for the selected application.

# Using the Application Self-service Manager User Interface

You will use the user interface to install and remove software, refresh the catalog of available software, and view information about the available software. The Menu Bar contains buttons for viewing session history, adjusting bandwidth, and viewing the current status of an application.


See the following sections for additional information:

- [Installing Software](#) on page 236
- [Refreshing the Catalog](#) on page 236
- [Viewing Information](#) on page 236
- [Removing Software](#) on page 237
- [Viewing History](#) on page 238
- [Adjusting Bandwidth](#) on page 238
- [Viewing Status](#) on page 239

## Installing Software

The applications that are available to you are listed in the Service List. You can install one or more of these applications at any time.

### To install software



- 1 In the Service List, click the name of the software that you want to install.
- 2 Click the Install button .

Some installations may display a set of dialog boxes. If so, follow the instructions. Otherwise, the installation begins immediately.




You can also right-click the name of the software that you want to install, then select **Install** from the shortcut menu that opens.

A progress bar indicates the installation progress.

- Click **Cancel**  in the Global Toolbar to cancel the installation.
- Click **Pause**  in the Global Toolbar to pause the installation. If you pause an action, you will not be able to perform any other actions until you either cancel or resume the currently paused action.

## Refreshing the Catalog


The catalog is refreshed whenever you log on to the ASM user interface. While you are logged on, if you believe that the list of applications that you are authorized to use has changed, or that updates to your installed applications have become available, click **Refresh Catalog**  in the Global Toolbar to retrieve an updated list of applications.




You can also right-click any item in the Service List, then select **Refresh Catalog** from the shortcut menu that opens.

## Viewing Information

You may want more information about an application than the Service List provides. If you want to know the vendor, version, size, and date the

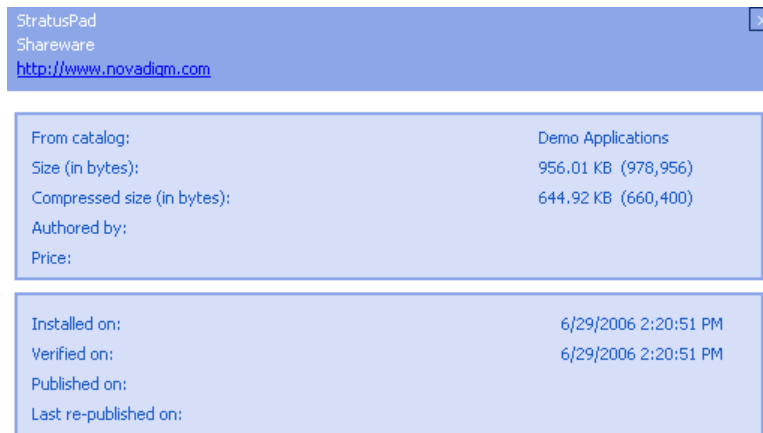
application was installed, you can either add these columns to the Service List or click **Show Extended Information**  in the expanded service box. If you want more information from the manufacturer, click that vendor's link.

To view more information

- In the Service list, select the appropriate software, and click **Show Extended Information** .




You can also right-click the appropriate software, select **Properties**, then select **Information from the shortcut menu** that opens.




Click the corresponding **Cancel** button to return to the Service List.

## Removing Software

Use the **Remove** button  to remove software from your computer.

To remove software

- 1 Select the software that you want to remove.
- 2 Click **Remove** .
- 3 Click **Yes** if you are asked to confirm that you want to remove the application.

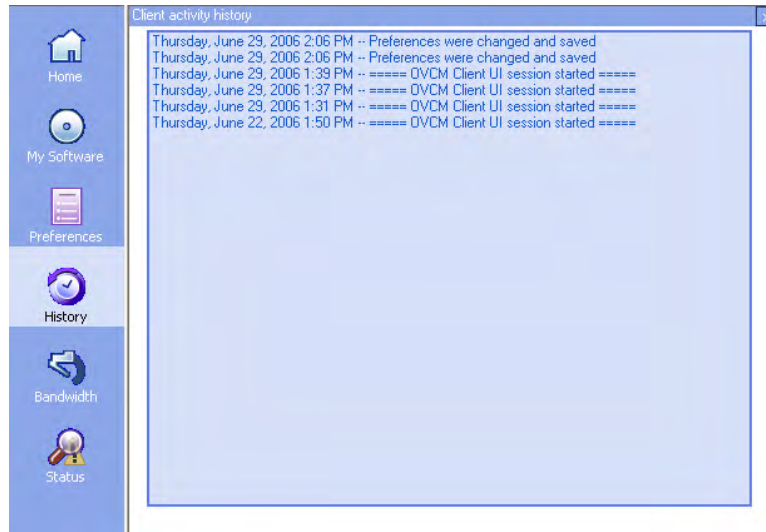


You can also right-click the name of the installed software that you want to remove, then select **Remove** from the shortcut menu that opens.

## Viewing History

- 1 In the Menu Bar, click **History** to display a history of the current session.

**Figure 31 History window**



- 2 Close the history window to show the service list.

## Adjusting Bandwidth

In the Menu Bar, click **Bandwidth** to display the bandwidth slider. Changing this value dynamically changes the throttling value.

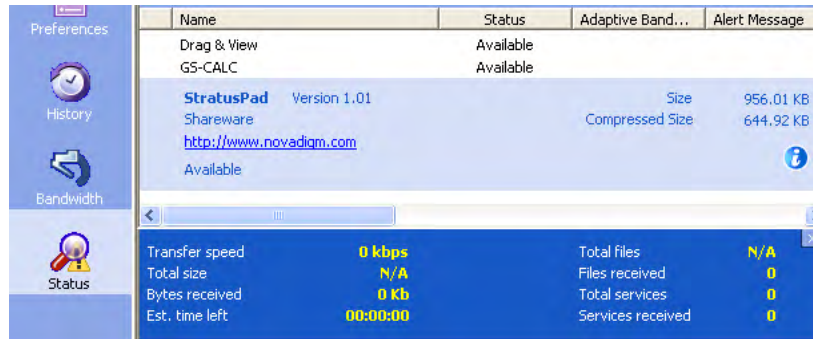
To adjust the bandwidth settings using the bandwidth slider

- Click and drag the slider to increase or decrease the amount of bandwidth throttling desired.
- You can also adjust bandwidth throttling from within the Preferences, Connection options section.

## Viewing Status

In the Menu bar, click **Status** to display the status of the current action including the size, estimated time, progress, and available bandwidth.

**Figure 32** Status display for selected application.



Name	Status	Adaptive Band...	Alert Message
Drag & View	Available		
GS-CALC	Available		
<b>StratusPad</b> Version 1.01			
Shareware		Size	956.01 KB
<a href="http://www.novadiqm.com">http://www.novadiqm.com</a>		Compressed Size	644.92 KB
Available			

Transfer speed	0 kbps	Total files	N/A
Total size	N/A	Files received	0
Bytes received	0 Kb	Total services	0
Est. time left	00:00:00	Services received	0

The Status window can be docked or un-docked from the Application Self-service Manager. This enables you to position the Status window anywhere on your screen. The Status window is docked by default.

### To un-dock the Status window

- 1 Click **Status** in the Menu Bar.
- 2 Right-click in the Status window that opens.
- 3 Select **Docked** from the shortcut menu. When the Status window is docked, a check mark will appear next to the word **Docked** in the shortcut menu.



The Status window will be released from the ASM user interface, allowing you to position it anywhere on your screen.

### To dock the Status window

- 1 Click **Status** in the Menu Bar.
- 2 Right-click in the Status window that opens.

- 3 Select **Docked** from the shortcut menu (only if there is no check mark present).



The Status window will be docked into the Application Self-service Manager.

## Customizing the User Interface

Click the **Preferences** button in the Menu Bar to view the customization options available.

The following sections describe each customization area:

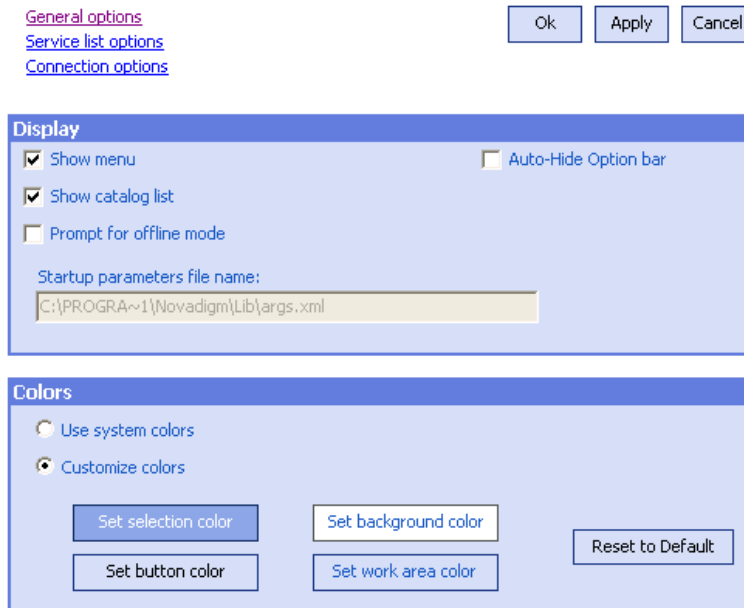
- [General Options](#) below
- [Service List Options](#) on page 242
- [Connection Options](#) on page 244

### General Options

Use the General options window to modify the appearance of the Application Self-service Manager.



**Figure 33    General options window**



### To modify the display

- If you want to display the menu, select the appropriate check box.
- If you want to display the catalog list, select the appropriate check box.
- If you want to be prompted to use the ASM in offline mode at the beginning of each session, select the appropriate check box.

### To modify the colors

- If you want to use the system colors, select the **Use system colors** option button.
- If you decide to use your own custom colors, select the **Customize colors** option button.
  - After selecting Customize colors, click the box labeled:
    - **Set selection color** to modify the color of selections.
    - **Set button color** to modify the button colors.

- **Set background color** to modify the background color.
- **Set work area color** to modify the background color.

## Service List Options

Use the **Service list options** to modify the appearance of the Service list.

**Figure 34** Service List options

[General options](#)
[Service list options](#)
[Connection options](#)

Ok Apply Cancel

Columns Available

- AdaptiveBandwidth
- AlertMessage
- Author
- Avis
- CompressedSize
- Description
- ErrorCode
- InstalledDate
- LocalRepair
- Mandatory
- OwnerCatalog
- Price

Add ->

Remove

Columns to show

- Name
- Status

Display

☒ Expand active service item
 ☐ Show grid lines

☐ Expand active catalog item
 ☐ Show advanced operations

To customize the column Names in the Service List

Use the Columns area to customize the columns that appear in your service List. The right column lists the column names displayed in your Service List. For a description of each available column heading, see [Customizing the Display](#) on page 243.

To add columns to the Service List

- In the Columns Available list box, select one or more names and click **Add**. The selected columns are listed in the Columns to show list box.

### To remove columns from the Service List

- 1 In the Columns to show list box, select one or more names. Hold the **Shift** or **Ctrl** key on your keyboard to select multiple consecutive or non-consecutive column names, respectively.
- 2 Click **Remove**. The selected columns are removed from the Columns to show list box and returned to Columns available.

### Customizing the Display

- Select **Expand active service item** to expand the current service item in the Service list.
- Select **Show grid lines** to display the Service list with grid lines separating each service.
- Select **Expand active catalog item** to expand the current catalog selected.
- **Show advanced operations** is not available at this time.

**Table 16** Column headings available for the Service List

Column Heading	Description
AdaptiveBandwidth	Adaptive minimum percentage of bandwidth used when using bandwidth throttling.
AlertMessage	Allows longer service description or instruction message to the end user. (Optional service text field as part of Alert/Defer configuration).
Author	The author of the service.
Avis	Service status flags for internal use only.
CompressedSize	The size of the compressed service (bytes).
ErrorCode	Current Service status. Example: Initial = 999. Method Failure = 709.
Description	A short description of the service.
InstalledDate	The date the service was installed on your computer.
LocalRepair	If data is repairable locally (cached on your computer).
Name	The name of the service.
Mandatory	Mandatory/Optional files defined on service (for internal use).
OwnerCatalog	The originating application domain name.

Column Heading	Description
Price	Price of the service.
PublishedDate	The date the service was published to the catalog.
Reboot	Service Reboot settings (for internal use).
RepublishedDate	The date the service was republished to the catalog.
ReservedBandwidth	Reserved maximum percentage of bandwidth used when using bandwidth throttling.
ScheduleAllowed	Specifies whether end users are allowed to change the update schedule for the service, locally.
Size	The size of the service (bytes). Note: You will need this amount of free space on your computer to successfully install the service.
Status	Current status of the software <ul style="list-style-type: none"> <li>• Available</li> <li>• Installed</li> <li>• Update Available</li> <li>• Broken</li> </ul>
SystemInstall	Displays if service will be installed using System account.
ThrottlingType	Type of Bandwidth throttling to use. Possible values: ADAPTIVE, RESERVED or NONE.
UIOption	Determines whether the status window is displayed.
UpgradedDate	The date the service was upgraded.
Url	The software vendor's url.
Vendor	The software vendor who supplied the service.
VerifiedDate	The date the service was last verified.
Version	The version of the service.

## Connection Options

Use **Connection options**, as shown in the following figure on page 245, to select the type of bandwidth throttling to use or to specify the settings required for using a proxy server.

**Figure 35 Connection Options**

[General options](#) [Service list options](#) [Connection options](#)

---

**Throttling**

☒ None

☐ Reserve Bandwidth

☐ Adapt to Traffic

---

**Proxy**

☐ Use a proxy server

☐ Discover proxy address

Address of proxy server  Port

- **Throttling**
  - Select **None** for no throttling.
  - Select **Reserve Bandwidth** to select along the scale to indicate the maximum percentage of the network bandwidth to use. The reserve bandwidth can be changed in the user interface by the subscriber as the download is happening.
  - Select **Adapt to traffic** to slide along the scale to indicate the minimum percentage of the network bandwidth to use. The adaptive bandwidth cannot be changed during a data download process. It can only be set before a job is dispatched.
- **Proxy**
  - The ASM can detect an Internet proxy when an Internet proxy is used. The Internet proxy's address is then stored in `PROXYINF.EDM` located in the client computer's `IDMLIB` directory. The default location of `IDMLIB` is `SystemDrive:\Program Files\Novadigm\Lib`. The next time the client computer connects to the HPCAS server the specified Internet proxy will be used. To use this feature, you must enable your client to use and discover an Internet Proxy. If you are using the ASM, set the Proxy settings in the Connection section of Preferences.

# HPCA System Tray Icon

The HP Client Automation System Tray icon provides status and statistics information, as well as pause and cancel mechanisms to the subscriber.

**Figure 36    HPCA System Tray icon**



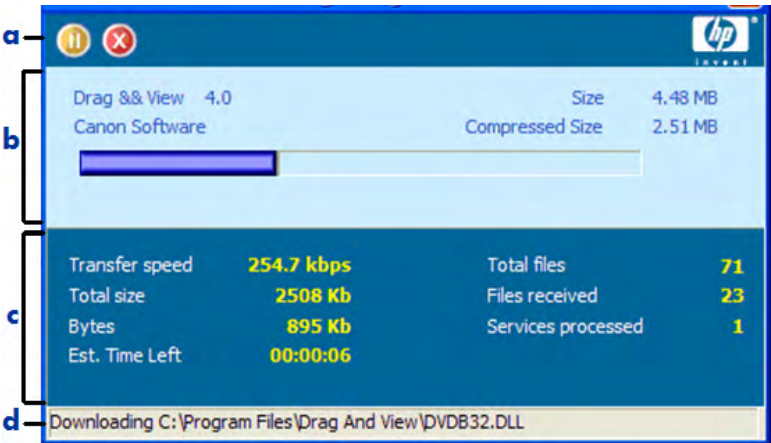
Move your cursor over the icon to see HPCA states:

- **Idle**  
When no actions are in process and no user intervention is required, the icon is static. When the system tray icon is idle, it may be hidden.
- **Active**  
The icon becomes activated when the ASM is working or when user intervention is required. Pause your cursor on the icon to view a bubble that provides activity information. If a critical notify occurs, the bubble will popup automatically:

## HPCA Status window

Left-click the HPCA System Tray icon to view the Status window. The Status window opens as shown in the following figure.


**Figure 37    HPCA Status**



## Legend

- a** Button bar
- b** Information panel
- c** Status area
- d** Status message

The Status window contains the following areas:

- **Button Bar**  
Contains buttons for Pause and Cancel, and a logo that becomes animated when the Agent is actively working.
- **Information Panel**  
This area contains information about the active service, and also contains a progress bar that shows the percentage of the task finished.
- **Status Area**  
Contains statistics about the active processes, including transfer speed, total size of transmission, bytes received, estimated time left of transmission, total files to be transmitted, number of files received, and number of services processed.
- **Status Message Area**  
The Status Message Area shows a message about the current process.
- **Bandwidth Control**
  - If you set bandwidth throttling for the service on the HPCAS server, and you click the bandwidth toggle button  in the System Tray Console, a slider for bandwidth control appears. Adjust the slider to change the bandwidth throttle value.





# 11 Settings Migration

Settings Migration allows you to backup and restore user settings for applications and operating systems on individual managed devices. Settings and files are stored on the HPCAS server and are available for restoration to the original device, a new device, or to be included during operating system deployment.

The **Settings Migration Manager** is used to create and store a configuration template for capturing user settings and files on managed devices.

The **Settings Migration Utility** is deployed to individual devices and used to back up and restore those settings files.

- ▶ Settings Migration requires HP Client Automation Standard.
- ▶ After upgrading to the latest version of HPCAS, you must perform new backups of your user settings. Backups created with previous versions of HPCAS cannot be restored.

The following sections explain how to implement settings migration in your environment.

- [Supported Applications and Settings](#) on page 250
- [Creating the Configuration Template](#) on page 273
- [Using the Settings Migration Utility](#) on page 275
- [Migrating Settings during OS Deployment](#) on page 279
- [File Rules](#) on page 279

# Supported Applications and Settings

The following sections, MS Office Support Notes and Other Support Notes, provide important usage notes as well as restrictions or limitations to keep in mind for each personality object supported in this release of Settings Migration Manager

## Microsoft Office Supported Applications

- Microsoft Access 95, 97, 2000, XP, 2003, 2007
- Microsoft Excel 95, 97, 2000, XP, 2003, 2007
- Microsoft FrontPage 2000, XP, 2003, 2007
- Microsoft Groove 2007
- Microsoft InfoPath 2003, 2007
- Microsoft OneNote 2003, 2007
- Microsoft Outlook (Windows Messaging), 97, 98, 2000, XP, 2003, 2007
- Microsoft PowerPoint 95, 97, 2000, XP, 2003, 2007
- Microsoft Project 98, 2000, 2002, 2003, 2007
- Microsoft Publisher 2003, 2007
- Microsoft Word 95, 97, 2000, XP, 2003, 2007

## Other Supported Applications

- Adobe Acrobat 4.x, 5.x, 6
- Acrobat Reader 4.x, 5.x, 6.x, 7.x, 8.x
- CuteFTP Pro 8
- FileZilla 2.x, 3.x
- AOL Instant Messenger 5.9
- MSN Messenger 7.0, 7.5
- Yahoo Messenger 7.0, 7.5, 8
- Lotus Notes 5.x, 6.x, 7.x, 8.x

- Microsoft Internet Explorer 4.01, 5.x, 6.x, 7.x
- Microsoft NetMeeting 2.x, 3.x
- Microsoft Outlook Express 5.x, 6.x
- Mozilla Firefox 1.x, 2.x
- Norton AntiVirus Corporate Edition
- Visio 2000, 2002, 2003, 2007
- WinZip 7.x, 8.x, 9.0

## Windows Options

- Desktop Shortcuts
- Dial-Up Networking
- Folder Options
- Local Printer Logging
- Mapped Network Drives
- Network and Shared Printer Connections
- Taskbar and Quick Launch Bar
  - Quick Launch Bar Shortcuts
  - Taskbar Settings
- User Documents and Media Files
  - My Documents
  - My Pictures
  - My Music
  - My Videos
- Windows Address Book

## Control Panel (Settings)

- Accessibility Options
- Display

- Appearance and Themes
  - Background
  - Visual Effects
- Internet Options
- Keyboard
  - Keyboard Languages
  - Keyboard Settings
- Mouse Settings
  - Buttons and Motions
  - Pointers and Schemes
- Power Management
- Regional Settings
- Sounds
- Time Zones

## Microsoft Office Support Notes

Following are important usage notes to keep in mind for Microsoft Office.

### Microsoft Office

Migrates data files, templates, and persistent settings for the following Office applications:

- MS Access
- MS Excel
- MS FrontPage
- MS Groove
- MS InfoPath
- Office Assistant Settings
- Office Shortcut Bar
- MS OneNote

- MS Outlook
- MS PowerPoint
- MS Project
- MS Publisher
- MS Word

The following versions of Office are supported

Office 95, Office 97, Office 2000, Office XP, Office 2003 and Office 2007

Cross version migration is supported for the following paths:

- Office 95 to Office 97
- Office 95 to Office 2000
- Office 95 to Office XP
- Office 95 to Office 2003
- Office 97 to Office 97
- Office 97 to Office 2000
- Office 97 to Office XP
- Office 97 to Office 2003
- Office 97 to Office 2007
- Office 2000 to Office 2000
- Office 2000 to Office XP
- Office 2000 to Office 2003
- Office 2000 to Office 2007
- Office XP to Office XP
- Office XP to Office 2003
- Office XP to Office 2007
- Office 2003 to Office 2003
- Office 2003 to Office 2007
- Office 2007 to Office 2007

## Microsoft Access

Migrates Access data files, persistent settings, and templates.

The following file types are migrated:

### Access Data Files

.accda, .accdb, .accdc, .ade, .adp, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .mat, .mav, .maw, .mda, .mdb, .mdbhtml, .mde, .mdt, .mdw

### Access Template Files

.accdt, .mdn, mdz, .wizhtml

The following versions of Access are supported:

Access 95, Access 97, Access 2000, Access XP, Access 2003 and Access 2007

Cross version migration is supported for the following paths:

- Access 95 to Access 97
- Access 95 to Access 2000
- Access 95 to Access XP
- Access 95 to Access 2003
- Access 95 to Access 2007
- Access 97 to Access 97
- Access 97 to Access 2000
- Access 97 to Access XP
- Access 97 to Access 2003
- Access 97 to Access 2007
- Access 2000 to Access 2000
- Access 2000 to Access XP
- Access 2000 to Access 2003
- Access 2000 to Access 2007
- Access XP to Access XP
- Access XP to Access 2003
- Access XP to Access 2007
- Access 2003 to Access 2003
- Access 2003 to Access 2007

- Access 2007 to Access 2007

## Microsoft Excel

Migrates Excel data files, persistent settings, and templates.

The following file types are migrated:

### Excel Data Files

.csv, .dif, .dqy, .iqy, .oqy, .rqy, .slk, .thmx, .xla, .xlam, .xlb, .xlc, .xld, .xlk, .xll, .xlm, .xls, .xlsb, .xlshtml, .xlsml, .xlsx, .xlv, .xlw, .xps

### Excel Template Files

.xlt, .xltx, .xltm

The following versions of Excel are supported:

Excel 95, Excel 97, Excel 2000, Excel XP, Excel 2003 and Excel 2007

Cross version migration is supported for the following paths:

- Excel 95 to Excel 97
- Excel 95 to Excel 2000
- Excel 95 to Excel XP
- Excel 95 to Excel 2003
- Excel 95 to Excel 2007
- Excel 97 to Excel 97
- Excel 97 to Excel 2000
- Excel 97 to Excel XP
- Excel 97 to Excel 2003
- Excel 97 to Excel 2007
- Excel 2000 to Excel 2000
- Excel 2000 to Excel XP
- Excel 2000 to Excel 2003
- Excel 2000 to Excel 2007
- Excel XP to Excel XP
- Excel XP to Excel 2003
- Excel XP to Excel 2007

- Excel 2003 to Excel 2003
- Excel 2003 to Excel 2007
- Excel 2007 to Excel 2007

## Microsoft FrontPage

Migrates FrontPage data files, persistent settings, and templates.



Selecting to migrate FrontPage data files will result in the migration of all .html and .htm files on your local disk drives unless the policies **Exclude User's Temporary Directory** and **Exclude User's Temporary Internet Directory** are set (default). This may not be welcomed behavior. If migrating all .html and .htm files is not desired you can use File Rules to exclude these file types entirely, or selectively in specified file folders on the local disk.

The following file types are migrated:

### FrontPage Data Files

.asa, .asp, .cdx, .fphtml, .htm, .html, .htx, .shtm, .shtml, .stm

### FrontPage Template Files

.tem

The following versions of FrontPage are supported:

FrontPage 2000, FrontPage XP, FrontPage 2003

Cross version migration is supported for the following paths:

- FrontPage 2000 to FrontPage 2000
- FrontPage 2000 to FrontPage XP
- FrontPage 2000 to FrontPage 2003
- FrontPage XP to FrontPage XP
- FrontPage XP to FrontPage 2003
- FrontPage 2003 to FrontPage 2003

## Microsoft Groove

Migrates Groove data files and persistent settings.

The following file types are migrated:



### **Groove Data Files**

.grv, .gsa, .vcg

The following versions of Groove are supported  
Groove 2007

Cross version migration is supported for the following paths:

- Groove 2007 to Groove 2007

## Microsoft InfoPath

Migrates InfoPath data files, persistent settings, and templates.

The following file types are migrated:

### **InfoPath Data Files**

.xml, .xsf

### **InfoPath Template Files**

.xsn

The following versions of InfoPath are supported  
InfoPath 2003 and InfoPath 2007

Cross version migration is supported for the following paths:

- InfoPath 2003 to InfoPath 2003
- InfoPath 2003 to InfoPath 2007
- InfoPath 2007 to InfoPath 2007

## Office Assistant Settings

Migrates Persistent settings for Microsoft Office Assistant.



Settings Migration Manager does not migrate the specific assistant, only the settings associated with the office assistant.

## Office Shortcut Bar

Migrates Persistent settings for Office Shortcut Bar.

## Microsoft OneNote

Migrates OneNote data files and persistent settings.

The following file types are migrated:

**OneNote Data Files**

.mht, .one, .onetoc

The following versions of OneNote are supported:

OneNote 2003 and OneNote 2007

Cross version migration is supported for the following paths:

- OneNote 2003 to OneNote 2003
- OneNote 2003 to OneNote 2007
- OneNote 2007 to OneNote 2007

## Microsoft Outlook

Migrates Outlook data files, Outlook Mail Clients and associated files, and Outlook persistent settings.

► Services on the target/injection machine must be the same as the services on the source/extraction machine. For example, if the source machine has Outlook set to Corporate Workgroup, then Outlook on the target machine must also be set to Corporate Workgroup.

The following file types are migrated:

**Outlook Files**

.ics, .msg, .oft, .pst (Inactive), .vcs

► If you migrate .pst files without selecting Outlook Mail Clients and Associated Files, your active .pst files will be migrated, but they will not be made active on the target computer.

### Outlook Mail Clients and Associated Files

Outlook Exchange and Internet mail clients are migrated, including Windows messaging as an exchange client. Active personal folders (.pst files), address books (.pab files), and offline address books (.oab files) are also migrated.

The following versions of Outlook are supported

Windows Messaging, Outlook 97, Outlook 98, Outlook 2000, Outlook XP, Outlook 2003 and Outlook 2007

Cross version migration is supported for the following paths:

- Windows Messaging to Outlook 97
- Windows Messaging to Outlook 98

- Windows Messaging to Outlook 2000
- Outlook 97 to Outlook 97
- Outlook 97 to Outlook 98
- Outlook 97 to Outlook 2000
- Outlook 97 to Outlook XP
- Outlook 97 to Outlook 2003
- Outlook 97 to Outlook 2007
- Outlook 98 to Outlook 98
- Outlook 98 to Outlook 2000
- Outlook 98 to Outlook XP
- Outlook 98 to Outlook 2003
- Outlook 98 to Outlook 2007
- Outlook 2000 to Outlook 2000
- Outlook 2000 to Outlook XP
- Outlook 2000 to Outlook 2003
- Outlook 2000 to Outlook 2007
- Outlook XP to Outlook XP
- Outlook XP to Outlook 2003
- Outlook XP to Outlook 2007
- Outlook 2003 to Outlook 2003
- Outlook 2003 to Outlook 2007
- Outlook 2007 to Outlook 2007

## Microsoft PowerPoint

Migrates PowerPoint data files, persistent settings, and templates.

The following file types are migrated:

### **PowerPoint Data Files**

.pps, .ppt, .ppthtml, .pptmp, .pptx, .ppz, .pwz

### **PowerPoint Template Files**

.pot, .pothtml, .potm, .potx

The following versions of PowerPoint are supported  
PowerPoint 95, PowerPoint 97, PowerPoint 2000, PowerPoint XP,  
PowerPoint 2003 and PowerPoint 2007

Cross version migration is supported for the following paths:

- PowerPoint 95 to PowerPoint 97
- PowerPoint 95 to PowerPoint 2000
- PowerPoint 95 to PowerPoint XP
- PowerPoint 95 to PowerPoint 2003
- PowerPoint 95 to PowerPoint 2007
- PowerPoint 97 to PowerPoint 97
- PowerPoint 97 to PowerPoint 2000
- PowerPoint 97 to PowerPoint XP
- PowerPoint 97 to PowerPoint 2003
- PowerPoint 97 to PowerPoint 2007
- PowerPoint 2000 to PowerPoint 2000
- PowerPoint 2000 to PowerPoint XP
- PowerPoint 2000 to PowerPoint 2003
- PowerPoint 2000 to PowerPoint 2007
- PowerPoint XP to PowerPoint XP
- PowerPoint XP to PowerPoint 2003
- PowerPoint XP to PowerPoint 2007
- PowerPoint 2003 to PowerPoint 2003
- PowerPoint 2003 to PowerPoint 2007
- PowerPoint 2007 to PowerPoint 2007

## Microsoft Project

Migrates Project data files, persistent settings, and templates.

The following file types are migrated:

### **Project Data Files**

.mpd, .mpp, .mpw, .mpx

## Project Template Files

.mpt

The following versions of Project are supported

Project 98, Project 2000, Project 2002, Project 2003 and Project 2007

Cross version migration is supported for the following paths:

- Project 98 to Project 98
- Project 98 to Project 2000
- Project 98 to Project 2002
- Project 98 to Project 2003
- Project 98 to Project 2007
- Project 2000 to Project 2000
- Project 2000 to Project 2002
- Project 2000 to Project 2003
- Project 2000 to Project 2007
- Project 2002 to Project 2002
- Project 2002 to Project 2003
- Project 2002 to Project 2007
- Project 2003 to Project 2003
- Project 2003 to Project 2007
- Project 2007 to Project 2007

## Microsoft Publisher

Migrates Publisher data files and persistent settings.

The following file types are migrated:

### Publisher Data Files

.pub, .pubhtml, .pubmhtml

The following versions of Publisher are supported

Publisher 2003 and Publisher 2007

**Cross version migration is supported for the following paths:**

- Publisher 2003 to Publisher 2003
- Publisher 2003 to Publisher 2007

- Publisher 2007 to Publisher 2007

## Microsoft Word

Migrates Word data files, persistent settings, and templates.

The following file types are migrated:

### **Word Data Files**

.doc, .dohtml, .docm, .docx, .gly, .rtf, .wbk, .wiz

### **Word Template Files**

.dot, .dohtml, .dotm, .dotx

The following versions of Word are supported:

Word 95, Word 97, Word 2000, Word XP, Word 2003 and Word 2007

Cross version migration is supported for the following paths:

- Word 95 to Word 97
- Word 95 to Word 2000
- Word 95 to Word XP
- Word 95 to Word 2003
- Word 95 to Word 2007
- Word 97 to Word 97
- Word 97 to Word 2000
- Word 97 to Word XP
- Word 97 to Word 2003
- Word 97 to Word 2007
- Word 2000 to Word 2000
- Word 2000 to Word XP
- Word 2000 to Word 2003
- Word 2000 to Word 2007
- Word XP to Word XP
- Word XP to Word 2003
- Word XP to Word 2007
- Word 2003 to Word 2003

- Word 2003 to Word 2007
- Word 2007 to Word 2007

## Other Supported Application and Operating System Notes

Following are important usage notes to keep in mind for each content item included in this release of Settings Migration Manager.

### Adobe Acrobat

Migrates Adobe Acrobat files and persistent settings for Adobe Acrobat and Adobe Acrobat Reader.

The following file types are migrated:

#### **Adobe Acrobat Data Files**

.akf, .apf, .eps, .fdb, .fdf, .joboptions, .ndx, .p7c, .pdf, .pdx, .pfx, .ps, .sequ

The following versions of Adobe Acrobat are supported  
Acrobat Reader 4.x, Acrobat Reader 5.x, Acrobat Reader 6.x, Acrobat Reader 7.x, Acrobat Reader 8.x

Adobe Acrobat 4.x, Adobe Acrobat 5.x, Adobe Acrobat 6.0.

Cross version migration is supported for the following paths:

- Adobe Acrobat 4.x to 4.x
- Adobe Acrobat 4.x to 5.x
- Adobe Acrobat 4.x to 6.0
- Adobe Acrobat 5.x to 5.x
- Adobe Acrobat 5.x to 6.0
- Adobe Acrobat 6.0 to 6.0
- Acrobat Reader 4.x to 4.x
- Acrobat Reader 4.x to 5.x
- Acrobat Reader 4.x to 6.x
- Acrobat Reader 4.x to 7.x
- Acrobat Reader 5.x to 5.x
- Acrobat Reader 5.x to 6.x

- Acrobat Reader 5.x to 7.x
- Acrobat Reader 6.x to 6.x
- Acrobat Reader 6.x to 7.x
- Acrobat Reader 7.x to 7.x
- Acrobat Reader 7.x to 8.x
- Acrobat Reader 8.x to 8.x

## CuteFTP Pro

Migrates CuteFTP Pro persistent settings and CuteFTP Pro PodCast Manager persistent settings

The following versions of CuteFTP Pro are supported  
CuteFTP Pro 8

Cross version migration is supported for the following paths:

- CuteFTP Pro 8 to CuteFTP Pro 8

## FileZilla

Migrates FileZilla persistent settings

The following versions of FileZilla are supported:

FileZilla 2.x, FileZilla 3.x

Cross version migration is supported for the following paths:

- FileZilla 2.x to FileZilla 2.x
- FileZilla 2.x to FileZilla 3.x
- FileZilla 3.x to FileZilla 3.x

## AOL Instant Messenger

Migrates Account Username, Password, and locally stored settings

The following versions of AOL Instant Messenger are supported:

AIM 5.9

Cross version migration is supported for the following paths:

- AIM 5.9 to AIM 5.9



## MSN Messenger

Migrates locally stored, unencrypted settings.

The following versions of MSN Messenger are supported  
MSN Messenger 7.0 and MSN Messenger 7.5

Cross version migration is supported for the following paths:

- MSN Messenger 7.x to 7.x

## Yahoo Messenger

Migrates account Username, Password, and locally stored settings.

The following versions of Yahoo Messenger are supported  
Yahoo Messenger 7, Yahoo Messenger 7.5, Yahoo Messenger 8

Cross version migration is supported for the following paths:

- Yahoo Messenger 7.x to Yahoo Messenger 7.x
- Yahoo Messenger 7.x to Yahoo Messenger 8
- Yahoo Messenger 8 to Yahoo Messenger 8

## Lotus Notes

Migrates Lotus Notes data files and persistent settings. Only user ID files in the default location and the last used user ID file are migrated.



If the migration of user ID files stored in non-default locations is desired this can be accomplished using Settings Migration Manager File Rules.

The following versions of Lotus Notes are supported:

Lotus Notes 5.x, Lotus Notes 6.x, Lotus Notes 7.x, Lotus Notes 8.x

Cross version migration is supported for the following paths:

- Lotus Notes 5.x to Lotus Notes 5.x
- Lotus Notes 5.x to Lotus Notes 6.x
- Lotus Notes 6.x to Lotus Notes 6.x
- Lotus Notes 6.x to Lotus Notes 7.x
- Lotus Notes 7.x to Lotus Notes 7.x

- Lotus Notes 7.x to Lotus Notes 8.x
- Lotus Notes 8.x to Lotus Notes 8.x

## Microsoft Internet Explorer

Migrates Internet Explorer persistent settings, cookies, proxy settings, and favorites.

The following versions of Internet Explorer are supported:  
IE 4.01, IE 5.x, IE 6.x, IE 7.x

Cross version migration is supported for the following paths:

- IE 4.01 to IE 4.01
- IE 4.01 to IE 5.x
- IE 4.01 to IE 6.x
- IE 4.01 to IE 7.x
- IE 5.x to IE 5.x
- IE 5.x to IE 6.x
- IE 5.x to IE 7.x
- IE 6.x to IE 6.x
- IE 6.x to IE 7.x
- IE 7.x to IE 7.x

## Microsoft NetMeeting

Migrates Microsoft NetMeeting settings.

The following file types are migrated:

### **NetMeeting Whiteboard Files**

.nmw, .wht

The following versions of Microsoft NetMeeting are supported  
Microsoft NetMeeting 2.x, Microsoft NetMeeting 3.x

Cross version migration is supported for the following paths:

- Microsoft NetMeeting 2.x to Microsoft NetMeeting 2.x
- Microsoft NetMeeting 2.x to Microsoft NetMeeting 3.x
- Microsoft NetMeeting 3.x to Microsoft NetMeeting 3.x

## Microsoft Outlook Express

Migrates Microsoft Outlook Express persistent settings, Windows Address Book, mail, and news files.

The following file types are migrated:

Outlook Express Files

.eml, .nws, Outlook Express Stationery

The following versions of Microsoft Outlook Express are supported:

Outlook Express 5.x, Outlook Express 6.x

Cross version migration is supported for the following paths:

- Microsoft Outlook Express 5.x to Microsoft Outlook Express 5.x
- Microsoft Outlook Express 5.x to Microsoft Outlook Express 6.x
- Microsoft Outlook Express 6.x to Microsoft Outlook Express 6.x

## Mozilla Firefox

Migrates Mozilla Firefox persistent settings, files, bookmarks, cookies, extensions.

The following versions of Mozilla Firefox are supported

Firefox 1.x, 2.x

Cross version migration is supported for the following paths:

- Firefox 1.x to 1.x
- Firefox 1.x to 2.x
- Firefox 2.x to 2.x

## Norton AntiVirus Corporate Edition

Migrates custom scans and user settings for Norton AntiVirus Corporate Edition.

The following versions of Netscape Communicator are supported

Norton AntiVirus Corporate Edition 7.6 and Symantec AntiVirus Corporate Edition 8.0.

Cross version migration is supported for the following paths:

- Norton AntiVirus Corporate Edition 7.6 to Norton AntiVirus Corporate Edition 7.6

- Norton AntiVirus Corporate Edition 7.6 to Symantec AntiVirus Corporate Edition 8.0
- Symantec AntiVirus Corporate Edition 8.0 to Symantec AntiVirus Corporate Edition 8.0

## Visio

Migrates Visio data files, persistent settings and templates.

The following file types are migrated:

### Visio Data Files

.vdx, .vrd, .vsd, .vss, .vsw, .vsx

### Visio Template Files

.vst, .vtx

The following versions of Visio are supported  
Visio 2000, Visio 2002, Visio 2003 and Visio 2007

Cross version migration is supported for the following paths:

- Visio 2000 to Visio 2000
- Visio 2000 to Visio 2002
- Visio 2000 to Visio 2003
- Visio 2000 to Visio 2007
- Visio 2002 to Visio 2002
- Visio 2002 to Visio 2003
- Visio 2002 to Visio 2007
- Visio 2003 to Visio 2003
- Visio 2003 to Visio 2007
- Visio 2007 to Visio 2007

## WinZip

Migrates WinZip data files and persistent settings



WinZip content does not migrate .cab files by design. If the migration of .cab files is desired this can be accomplished using Settings Migration Manager File Rules.

The following file types are migrated:

#### WinZip Files

.arc, .arj, .b64, .bhx, .gz, .hqx, .lzh, .mim, .tar, .taz, .tgz, .tz, .uu, .uue, .xxe, .z, .zip

The following versions of WinZip are supported:

WinZip 7.x, WinZip 8.x, WinZip 9.0

Cross version migration is supported for the following paths:

- WinZip 7.x to WinZip 7.x
- WinZip 7.x to WinZip 8.x
- WinZip 7.x to WinZip 9.0
- WinZip 8.x to WinZip 8.x
- WinZip 8.x to WinZip 9.0
- WinZip 9.0 to WinZip 9.0

## WS\_FTP Pro

Migrates WS\_FTP Pro persistent settings

The following versions of WS\_FTP Pro are supported:

WS\_FTP Professional 11, WS\_FTP Professional 2007

Cross version migration is supported for the following paths:

- WS\_FTP Professional 11 to WS\_FTP Professional 11
- WS\_FTP Professional 11 to WS\_FTP Professional 2007
- WS\_FTP Professional 2007 to WS\_FTP Professional 2007

## Data Transport

Migrates files and registry values as set in File Rules and Registry Rules.

## Windows Options

**Migrates persistent settings and files for:** Control Panel, Desktop Shortcuts, Dial-up Networking, Folder Options, Local Printer Logging, Mapped Network Drives, Network and Shared Printer Connections, Taskbar

and Quick Launch Bar, User Documents and Media Files, Windows Address Book.

## Desktop Shortcuts

- Migrates shortcuts on the desktop.
- Desktop shortcuts that have broken links are not migrated by default. For example, if there is a shortcut to an installed application on the source machine's desktop but that application is not installed on the target machine, the shortcut will not be migrated because it would have become a broken link on the target machine. To migrate broken link files select Preferences from the Edit menu and check the Broken Shortcut Policy check box. The broken link files will be migrated to the source directory and placed in a folder named “Broken Shortcuts”.

## Dial-Up Networking

Migrates persistent settings and files for dial-up networking.

- Persistent settings that are hardware related are not migrated by design.

## Folder Options

Migrates persistent settings for folder options.

## Local Printer Logging

A file named `printinfo.txt` is created during injection on the users desktop that contains Printer information for both network and local printers.

## Mapped Network Drives

Migrates mapped network drives. If on the target machine a drive letter is in use that is the same as a mapped drive being migrated, the next available drive letter will be used for the migrated network drive.

- Hardware related settings and files are not migrated by design.

## Network and Shared Printer Connections

Migrates networked and shared printers. Printers are migrated if they have a valid UNC path and are accessible via the network or via a share. When printers are migrated a printer icon is placed on the target system's desktop. Double clicking on this icon will install the printer.

- The Settings Migration Manager Operator must have full access to the printers being migrated for each user. Hardware related settings and files are not migrated by design.

## Taskbar and Quick Launch Bar

Migrates Taskbar settings and Quick Launch Bar shortcuts.

## User Documents and Media Files

Migrates the contents of My Documents, My Pictures, My Music, and My Videos.

### My Documents

Migrates the contents of My Documents

- If the My Documents folder is renamed or the location changed, Settings Migration Manager will still recognize this folder as "My Documents" and the contents of the folder will migrate to the "My Documents" folder on the target system.

### My Music

Migrates the contents of My Music

### My Pictures

Migrates the contents of My Pictures

### My Videos

Migrates the contents of My Videos

## Windows Address Book

Migrates the windows address book.

## Control Panel



Hardware related settings and files are not migrated by design

Migrates Persistent settings and files for:

Accessibility Options, Display, Internet Options, Keyboard, Mouse Settings, Power Management, Regional Settings, Sounds, and Time Zones.

## Accessibility Options

Migrates keyboard, sound, display, and mouse accessibility settings

## Display

Migrates appearance and themes, background, and visual effects

## Internet Options

Migrates Internet properties (home page, colors, fonts, languages)

## Keyboard

Migrates Keyboard Languages and Keyboard Settings. Keyboard Languages are stored in different places and named differently, depending upon the operating system installed.

On Windows 2000, the settings are stored under the following path:

Control Panel \ Keyboard \ Input Locales (tab).

The settings can also be found under the following path for Windows 2000:

Control Panel \ Regional Settings \ Input Locales.

On Windows XP Pro, the settings can be found under the following path:

Control Panel \ Regional and Language Options \ Languages (tab)  
 \ Details [Button]

On Windows Vista, the settings can be found under the following path:

Control Panel \ Clock, Language, and Region \ Change keyboards  
or other input methods \ Change keyboards [Button]



## Mouse Settings

Migrates Persistent settings and files for Mouse (buttons, motion, pointers, and schemes).

## Power Management

Migrates Persistent settings for Power Management.

## Regional Settings

Migrates Persistent Regional Settings.

- ▶ If Country Codes between different Operating System Versions have changed or the Country Code is not present on the target machine the settings will not migrate.

## Sounds

Migrates persistent settings and files for Windows system sounds.

## Time Zones

Migrates persistent settings for Time Zones

# Creating the Configuration Template

Use the Settings Migration Manager to create a template that determines which application settings, files, and operating systems settings will be backed up and available for restoring or installing on individual devices.

To use the Settings Migration Manager it must be first deployed using HPCAS.

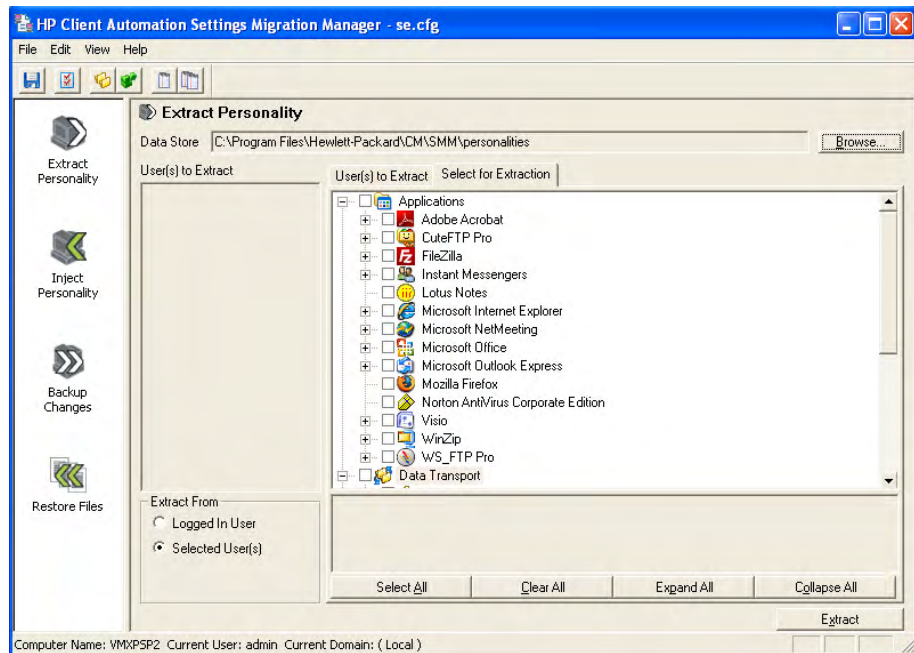
### To deploy Settings Migration Manager

- Deploy the Settings Migration Manager using the Settings Migration Manager service in the HPCAS Software library. See the section [Deploying Software](#) on page 83 for detailed instructions on deploying software services.

Use the Settings Migration Manager to create the configuration template. This template defines what application settings, files, and operating system settings are backed up when the Settings Migration Utility is run.

### To start the Settings Migration Manager

- 1 On a device where Settings Migration Manager is installed, go to `C:\Program Files\Hewlett-Packard\CM\SMM`.
- 2 Double-click **SE.exe**.
- 3 The Setting Migration Manager opens.



### To create the configuration template

- 1 Start the Settings Migration Manager.
- 2 Click **Select for Extraction** to view the list of applications available for settings and file backup.
- 3 Use the tree view to select or exclude application settings and files.
- 4 When you are satisfied with the configuration settings, save the file using the toolbar or the File menu. The filename must be **SE.CFG** (this is the default name).

- 5 Close the Settings Migration Manager.
- 6 Copy the files `se.rul`, `se.ptt`, and `SE.CFG` from `C:\Program Files\Hewlett-Packard\CM\SMM` to the HPCAS server directory `C:\Novadigm\ProxyServer\upload`.

Copying the files to the server directory makes the configuration settings available to the Settings Migration Utility that you will deploy to client devices. Each time the utility is run, it will access these files to determine which settings and files to backup.

When you have copied the configuration files to the HPCAS server, deploy the Settings Migration Manager service to enable settings migration on managed devices.

## Using the Settings Migration Utility

The Settings Migration Utility is installed with the Settings Migration Manager service. See the section [Deploying Software](#) on page 83 for detailed instructions on deploying software services to managed devices.

When deployed to managed devices, use the utility to back up or restore settings. Each time the utility is run, it downloads the latest configuration template (`SE.CFG`) from the HPCAS server. See [Creating the Configuration Template](#) on page 273 for more information.

To start the Setting Migration Utility

- On a device where the Settings Migration Manger service was deployed, use the Start menu and go to:

**Start > All Programs > HP Client Automation Settings Migration > HP Client Automation Settings Migration Utility**

The following sections explain how to use the Settings Migration Utility:

- [Backing Up Settings](#) on page 275
- [Restoring Settings](#) on page 277

## Backing Up Settings

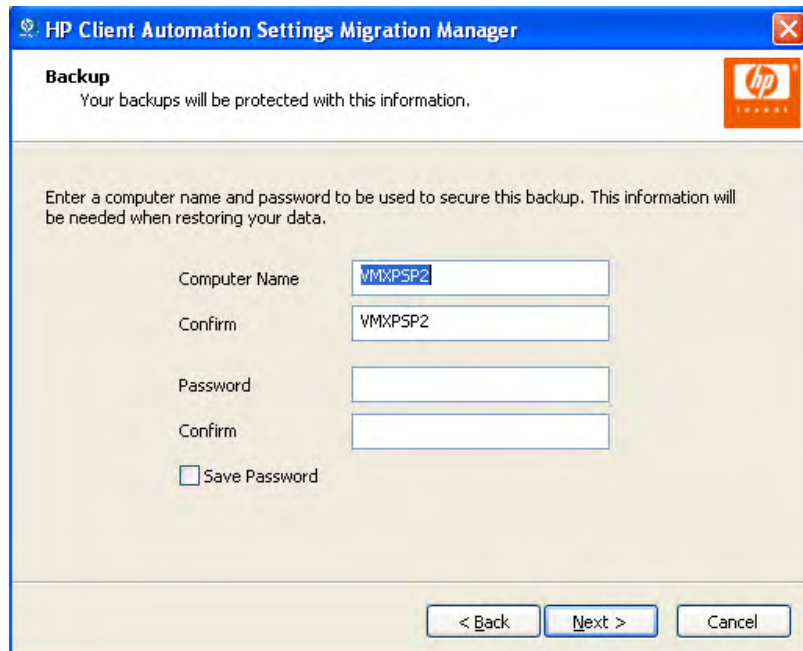
Use the Settings Migration Utility to backup settings and files and store them on the HPCAS server.

- After upgrading to the latest version of HPCAS, you must perform new backups of your user settings. Backups created with previous versions of HPCAS cannot be restored.

Settings are stored in the C:\Novadigm\ProxyServer\upload directory on the HPCAS server.

To backup settings and files

- 1 On the client device, start the Settings Migration Utility
- 2 Select **Backup settings and files**.
- 3 Click **Next**.



The screenshot shows the 'HP Client Automation Settings Migration Manager' window with the 'Backup' tab selected. The window title bar is blue with the HP logo on the left and a close button on the right. The main content area has a light beige background. At the top, it says 'Backup' and 'Your backups will be protected with this information.' Below this, it instructs the user to 'Enter a computer name and password to be used to secure this backup. This information will be needed when restoring your data.' There are four text input fields: 'Computer Name' (containing 'VMXPSP2'), 'Confirm' (containing 'VMXPSP2'), 'Password' (empty), and 'Confirm' (empty). Below these fields is a checkbox labeled 'Save Password' which is unchecked. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 4 Type and confirm a computer name and password. Make note of this information as it is required when restoring settings.
- 5 Click **Next**.
- 6 Review the summary information and click **Finish**.
- 7 When the process is finished, click **OK**.

Settings are now stored on the HPCAS server and available for restoration to a device.

## Stored Settings and Files

Each time you back up settings and files, they are stored on the HPCAS server in the `C:\Novadigm\proxyserver\upload` directory.

All files associated with a device contain the device name as part of the file name.

Periodically, you may want to clean up the `\upload` directory by deleting stored data for individual devices. Look for the device name in each file name to determine which data you want to remove.

## Restoring Settings

Use the Settings Migration Utility to restore settings to a device. If settings were backed up during an unattended operating system deployment (migration), you will have the option to restore those settings. See [To restore settings from an unattended OS deployment](#) on page 278.



Restored settings may include domain profiles. Therefore, settings backed up from a device in a specific domain can only be restored to devices within that same domain.

### To restore settings

- 1 On the client device, start the Settings Migration Utility.
- 2 Select **Restore files and settings**.
- 3 Click **Next**.

**HP Client Automation Settings Migration Manager**

**Restore**  
Your backed up settings and data will be restored.

Enter the information used when the original backup was created. This information is needed to decrypt and restore your settings and data.

☐ Restore from operating system migration

☒ Restore using the following information

Computer Name

Password

< Back   Next >   Cancel

- 4 Type the computer name and password for the settings you want to restore.
  - 5 Click **Next**.
  - 6 Review the summary information and click **Finish**.
  - 7 When the restoration process is complete, click **OK**.
- Settings and files are restored.

#### To restore settings from an unattended OS deployment

- 1 On the client device, start the Settings Migration Utility.
- 2 Select **Restore files and settings**.
- 3 Click **Next**.
- 4 Select **Restore from operating system migration**. Settings stored during the last unattended operating system deployment with migration enabled are accessed. This option is available only when these type of settings are detected.
- 5 Click **Next**.
- 6 Review the summary information and click **Finish**.

7 When the restoration process is complete, click **OK**.

Settings and files are restored.

## Migrating Settings during OS Deployment

Settings and files can be preserved during operating system deployment. Use HPCAS to deploy an operating system, see [Deploying Operating Systems](#) on page 103 for additional information.

During the [OS Deployment Wizard](#), you are prompted to migrate user data and settings. If you select **Yes**, the Settings Migration Manager service is deployed with the new operating system. Then during deployment, the Settings Migration Utility runs and the end users are prompted to backup their existing settings by supplying the device name and password. See [Using the Settings Migration Utility](#) on page 275 for additional information.

After the operating system installation is complete, redeploy the Settings Migration Manager service and use the Settings Migration Utility to restore the device settings that were backed up. Be sure to use the device name and password you supplied during the initial back up process.

► If you are using unattended mode for OS deployment and select settings migration, this process will also run unattended. The required information for Settings Migration, computer name and password, are automatically generated. The end user should use the **Restore from OS Migration** feature in the Settings Migration Utility to restore settings stored during an unattended OS deployment.

## File Rules

Most desired data files can be migrated using OV Settings Migration Manager's built-in support. Enterprise migration projects often require additional file migration support. For example, you may want to migrate proprietary file types created by internally developed applications.

Designed for major migration projects, File Rules provides a method to include or exclude files by path, type, date, and size. Subdirectories can be

included or not. Multiple rules can be created to tailor a migration to meet project goals and requirements.

► File Rules take precedence over files selected using the File Tree.

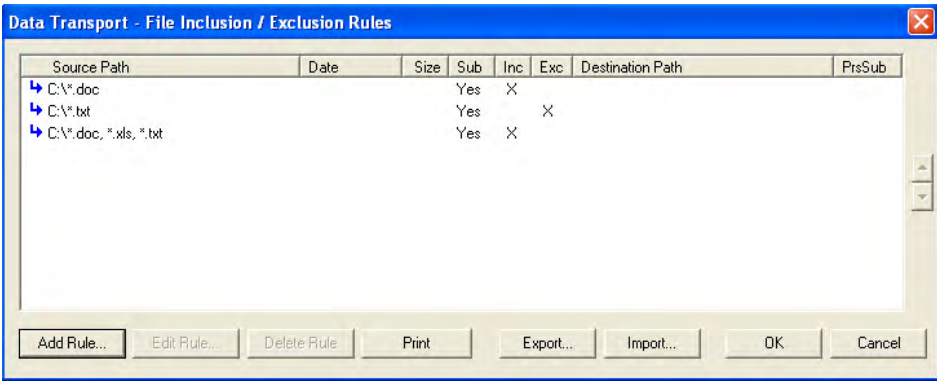
The following sections explained how to use File Rules:

- [Accessing File Rules](#) on page 280
- [File Rules Dialog Box](#) on page 281

## Accessing File Rules

To access file rules, start the Settings Migration Manager and use the **Edit > File Rules** menu item.

**Figure 38    File Rules**



File Rules have hierarchical precedence. If two rules are mutually exclusive, the rule that appears higher in the list takes precedence over the rule that appears below. For example, precedence can be used to migrate all the .jpg files from the directory c:\files, yet prevent any other files in that directory from moving.

Files can also be redirected to a different directory on the target computer with the Destination Re-mapping feature. Any path can be specified as a destination including network paths. Subdirectory structure can be preserved or not.



Use the **Add Rule**, **Edit Rule**, and **Delete Rule** buttons to enter and manipulate rules.

To delete or edit a rule, click on the rule in the Source Path column to highlight it, then click the **Delete Rule** or **Edit Rule** button. Rules can be moved in the list to adjust precedence by using the up and down arrow buttons on the right side of the dialog box.

When finished, click on the **OK** button or click **Cancel** to abandon the session. Rules in the list are saved when you save the current Configuration file.

## File Rules Dialog Box

When adding or editing a rule, the File Rule dialog box opens.

**Figure 39 File Rules Dialog Box**

The screenshot shows the 'File Rule' dialog box. It has a blue title bar with the text 'File Rule' and a close button. The dialog is divided into several sections. The first section has two radio buttons: 'Include' (selected) and 'Exclude'. To the right of these is a text box labeled 'Source Path' with a 'Browse...' button. Below the radio buttons is a checked checkbox labeled 'Include Subdirectories'. The second section is labeled 'Date' and contains a checkbox 'Limit by Date'. To its right is a dropdown menu showing 'On or after' and a date selector showing '7/28/2006'. The third section is labeled 'File Size' and contains a checkbox 'Limit by File Size'. To its right is a dropdown menu showing 'Less than or equal to', a text box containing '0', and the label 'K bytes'. The fourth section is labeled 'Destination Remapping' and contains two checkboxes: 'Remap Destination' and 'Preserve Subdirectories'. Below these is a text box labeled 'Destination Path' with a 'Browse...' button. At the bottom right are 'OK' and 'Cancel' buttons.

- Use the **Include** or **Exclude** radio buttons set to select the rule type.
- Enter the path of the files to be affected in the **Source Path** text box. This control supports wildcard characters asterisk (\*) and question mark (?) in the file name and file type portions of the path. The Source Path also supports Token Substitution.

- Separating files or file types with a semi colon (;) in the File Rule source path allows you to Include or Exclude multiple files or file types. For example, selecting **Include** and typing the following in the Source Path:

**C:\\*.doc;\*.xls;\*.mdb**

will find and extract files on the C: drive that match the specified file types.

Selecting **Exclude** and typing:

**C:\\*.mp3;\*.dll;\*.exe**

will exclude files on the C: drive from being extracted that match the specified file types.

Although you can create two or more rules that may specify the same file or files for migration, only the rule with the higher precedence (closer to the top of the list) will migrate those files.





# 12 FAQs

This chapter includes frequently asked questions regarding common management tasks available when using HPCAS and its components.

- [How do I access the HPCAS console?](#) on page 286
- [How do I determine what version I am using?](#) on page 286
- [How do I change my console password?](#) on page 286
- [How do I begin to manage a device in my environment?](#) on page 287
- [How do I schedule inventory collection?](#) on page 287
- [How do I view inventory information for managed devices?](#) on page 288
- [How do I automate patch acquisition?](#) on page 288
- [How do I configure the patch compliance discovery schedule?](#) on page 289
- [How do I deploy software to all of my managed devices?](#) on page 289
- [How do I acquire a particular Microsoft patch?](#) on page 290
- [How do I update my license key?](#) on page 290
- [How do I create a group of devices to target for an OS Service Pack?](#) on page 290
- [How do I deploy software to a single device?](#) on page 291
- [How do I install the Management Agent without using the console?](#) on page 291
- [How do I publish a Windows Installer package?](#) on page 292
- [How do I publish setup.exe?](#) on page 292
- [How do I know that all my devices received the software?](#) on page 292
- [How do I make software available for a user to install?](#) on page 293
- [How do I generate a device compliance report?](#) on page 293
- [How do I capture an OS image?](#) on page 293
- [How do I add additional drivers to an OS image?](#) on page 294
- [How do I publish an OS image?](#) on page 294

- [How do I deploy an OS image?](#) on page 294
- [How do I start collecting usage data?](#) on page 295
- [How do I contact support?](#) on page 295

## How do I access the HPCAS console?

Use a browser from any device in your environment to access the HPCAS console.

- Go to **`http://HPCAShost:3480/ccm`**, where *HPCAShost* is the name of the server where HPCAS is installed.

## How do I determine what version I am using?

- Use the Configuration area, Support section to view the HPCAS version Information.

## How do I change my console password?

Each console user has its own password defined by the administrator when the console user is created. Change a console user's login password in the [Console Access](#) section of the [Configuration](#) area.

- Click the User ID of the console user to open the User Details window.
- Within the Password Change area, enter and confirm a new password by typing it into the text boxes provided.
- Click **Save**.

The new password has now been saved.

## How do I begin to manage a device in my environment?

Devices are managed when the Management Agent is deployed. To deploy the Agent, the device must be added to HPCAS.

First, import the device:

- From Device Management, General tab, click **Import Devices to Manage**. The [Import Device Wizard](#) opens.
- Follow the steps in the wizard on page 168 to import your devices.


When the device is imported, deploy the Management Agent:

- From Device Management, General tab, click **Deploy the Management Agent**. The [Agent Deployment Wizard](#) opens.
- Follow the steps in the wizard on page 169 to deploy the Management Agent.

When the Agent is deployed, the device is successfully managed and ready for software, patch, and inventory management.

## How do I schedule inventory collection?

Hardware and Software inventory collection is based on the schedule you define using the [Software/Hardware Inventory Wizard](#).


- First select whether to schedule inventory collection for individual devices or a group by selecting them within either the [Device Management, Devices](#) section or the [Group Management, Groups](#) section.
- On the toolbar, click the **Inventory Collections**  toolbar button, then select **Discover Software/Hardware Inventory** to launch the wizard.
- Follow the steps in the wizard on page 171 to define software and hardware inventory collection for your devices and groups.



Additional inventory collection is taken after a software deployment job is completed.

## How do I view inventory information for managed devices?

Use the Reporting tab to view inventory information for managed devices.

- From the home page of the Reporting tab, click **View Managed Devices** under Inventory Information. A list of all managed devices is displayed.
- Use the tools on the left side of the page, or click any criteria within each list item, to filter the list further.
- Click **Show Details**  to display information for a single device.

## How do I automate patch acquisition?


Use the Configuration tab, Patch Management section to define your patch acquisition schedule and settings.

- 1 In the **Patch Acquisition Schedule** area, use the tools provided to set the acquisition schedule.
  - **Run:** Select whether to discover patches based on an interval hours, days, or weeks.
  - **Interval:** Select the specific interval (hours, days, or weeks).
  - **Starting on:** Use the drop-down list to select the date patch compliance should be discovered.
  - **Current Server Time** displays the current time of the HPCAS server.
- 2 When finished, click **Save** to commit your changes. The new schedule is displayed after Current Schedule.
- 3 In the **Patch Acquisition Settings** area, enter the Bulletins to Acquire each discovery period. You can use wildcard characters to designate a range of bulletins (for example, MS05\*). Separate multiple bulletin searches with a comma (for example, MS05\*, MS06\*).
- 4 Type a Proxy Server Address from which to obtain bulletins (for example, **http://proxyserver:8080/**).
- 5 If required, type a Proxy User ID and Proxy Password to acquire patches.




- 6 Click **Save** to commit your changes.

## How do I configure the patch compliance discovery schedule?

- To define a schedule for patch compliance discovery, select the managed devices from the [Devices](#) tab (or select a Group from the [Groups](#) tab).
- Click the **Inventory Collections**  toolbar button, then select **Discover Patch Compliance** to launch the [Patch Compliance Discovery Wizard](#).
- Follow the steps in the wizard on page 171 to define a schedule for patch compliance for your devices and groups.
- Use the [Reporting](#) tab to view patch compliance reports for the selected devices.

## How do I deploy software to all of my managed devices?


First, create a dynamic Reporting group containing all managed devices.

- Within the Reporting tab, under Inventory, click **View Managed Devices**.
- A list of all managed devices is displayed.
- Click **Create new Dynamic Reporting Group** . Follow the steps in the Group Creation wizard to create the group.

Now you can deploy software to devices in the newly created group.

- In the Management tab, click **Software Management**.
- Click **Deploy Software**.
- The Software Deployment Wizard opens. Follow the steps in the wizard to select the newly created group and software for deployment.

## How do I acquire a particular Microsoft patch?

- Use the Configuration tab, Patch Management section and define the specific patch bulletin number in the Patch Acquisition Settings, Bulletins to Acquire text box.
-  You can launch patch acquisition immediately after you define the settings. If your patch acquisition schedule is set to acquire patches on a regular basis, you must reset the acquisition settings values to prevent patch acquisition from acquiring only a specific patch during future acquisitions.


## How do I update my license key?

- 1 Use a text editor and open the new license file (for example `license.nvd`).
- 2 Copy the contents of the file into the License Data text box found in the Configuration tab, Support section.
- 3 Click **Save** to update your license information.

## How do I create a group of devices to target for an OS Service Pack?


Use the Reporting tab to create a query that contains all devices that do not have the particular service pack. In this example, a group of all Windows XP devices without Service Pack 2 installed will be created.

- 1 In the Data Filters area, click **Inventory Management Related**.
- 2 Click **OS Related**.
- 3 Click **Operating System** and enter **\*Windows XP\***
- 4 Click **Apply**. All devices with Windows XP are displayed.
- 5 Click **Operating System Level** and type **!Service Pack 2**

- 6 Click **Apply**. All Windows XP devices that do not have Service Pack 2 installed, are displayed.
- 7 Then click **Create new Dynamic Reporting Group**  and follow the steps in the Group Creation wizard to create the group of devices.

## How do I deploy software to a single device?

Use the Software Details window to deploy software to a single device.

- 1 In the Management tab, click **Software Management**.
- 2 Click **Software Library** to display all published software.
- 3 Click the description link for the software you want to deploy to a single device. The Software Details window opens.
- 4 Click the **Devices** tab and select the device to which you want to deploy the software.
- 5 Click **Deploy Software**  to open the Software Deployment Wizard.
- 6 Follow the steps in the wizard to deploy software to that device.

## How do I install the Management Agent without using the console?

Use the Management Agent installation program included on the HPCAS CD-ROM to install the Agent to devices that may not be consistently connected to the network.

- 1 Use the Management Agent `setup.cmd` file located on the HPCAS installation media in the `RadAgent` directory.
- 2 From a command line, type: **setup.cmd** `HPCAS_IP_Addr`  
where `HPCAS_IP_Addr` is the IP address of your HPCAS server.
- 3 Press **Enter**.

## How do I publish a Windows Installer package?

- Use the Publisher and select **Windows Installer** as the Type of Data to Publish. Follow the steps in the Publisher to make the Windows Installer file available for distribution to your managed devices.

Refer to the Publisher online help or Chapter 9, [Using the Publisher](#) for more information.

## How do I publish setup.exe?

- Use the Publisher and select **Component Select** as the Type of Data to Publish. Select the files to publish and follow the steps in the Publisher to make the file available for distribution to your managed devices.

Refer to the Publisher online help or Chapter 9, [Using the Publisher](#) for more information.

## How do I know that all my devices received the software?


- 1 In the Management area, click Software Management.
- 2 On the Reporting tab, click **Software Summary**. The Reporting area is displayed with a summary of all devices, managed services, and failed services.

You can also use the Software Details window, Devices tab to view the status of software organized by device.

- 1 Click the description link for any software to open the Software Details window.
- 2 Click **Devices** tab.
- 3 View the Software Status column to see which managed devices have the software installed. Only entitled devices are displayed.

## How do I make software available for a user to install?

By adding software entitlement to a group of devices, that software is then available for the user to install from the Application Self-service Manager.

- From the Group Management section of the Management tab, click the **Groups** tab.
- Click any Group description link to open the Group Details window.
- Click the **Software** tab to display all entitled software for that group.
- To entitle additional software, click **Add Software Entitlement** .
- Select the software to entitle and click **Add Entitlement**.

When entitled, software is available for deployment from the console or from the Application Self-service Manager on the individual devices.

## How do I generate a device compliance report?

- Use the Reporting tab to define which patch bulletin you want to see compliance for.
- In Data Filters, click **Patch Management Related**.
- Click **Patch Compliance Status**.
- Enter a bulletin name or partial name, and click **Apply**.
- Use the tools at the top of the report list to export or print the report.

## How do I capture an OS image?

Use the Image Preparation Wizard to prepare and capture operating system images.

- 1 Create the Image Preparation CD from the `ImageCapture.iso` file. The file is located on the HPCAS media in the `\OSManagement\ISO\CaptureCD` directory.

- 2 Follow the preparation steps in the Image Preparation Wizard online help or in the section [Preparing and Capturing OS Images](#) on page 189 for detailed instructions

## How do I add additional drivers to an OS image?

Before you capture an operating system image for deployment, it is a good idea to make sure any OEM drivers for all possible device hardware configurations are installed.

- 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>

## How do I publish an OS image?

- Use the Publisher and select **OS Image** as the Type of Data to Publish. Select the operating system image to publish and follow the steps within the Publisher to make the file available for distribution to your devices.

► Images captured by the Image Preparation Wizard are stored, by default, in the `\Novadigm\OSManagerServer\upload\` directory on the HPCAS server.

Refer to the Publisher online help or Chapter 9, [Using the Publisher](#) for more information.

## How do I deploy an OS image?

First, create a Static Group containing all devices to receive the OS image.

- 1 Within the Group Management, General tab, click **Create a new Static Group**.
- 2 The Group Management Wizard opens. Follow the steps in the Group Creation wizard to create the group.

Now you can deploy software to devices in the newly created group.

- 1 In the Management tab, click **OS Management**.
- 2 Click **Deploy Operating System**.

The OS Deployment Wizard opens. Follow the steps in the wizard to first select the newly created group then the software for deployment. An OS Management Job is created.

## How do I start collecting usage data?

Usage data is collected and stored locally by the Usage Collection Agent on managed devices. You can begin collecting usage data by doing the following:

- 1 Create and enable collection filters using the [Usage Collection Filter Creation Wizard](#). See [Usage Collection](#) on page 161 for additional information.
- 2 Use the [Application Usage Collection Wizard](#) to deploy the Usage Collection agent and begin collecting usage data. Follow the steps in the wizard on page 172 to define a schedule for usage data collection from groups or to force a one-time collection of data from individual devices. Usage data is stored on the local devices for 12 months.



Configuring filters to collect usage data based on wildcard characters can cause the collection of a large amount of data that can, over time, create severe reporting performance issues as the database grows in size. We strongly recommend that you create filters to collect data for only those applications for which you want usage information.

You should *not* collect usage data for all applications.

## How do I contact support?

- Use the Configuration tab of the HPCAS console to view Support Contact information.





# 13 Troubleshooting

Use the following sections to troubleshoot common problems you may encounter while using HPCAS.

- [Log Files on page 297](#)
- [Agent Deployment Issues on page 298](#)
- [OS Deployment Issues on page 299](#)
- [Application Self-service Manager Issues on page 300](#)
- [Power Management Issues on page 300](#)
- [Patch Management Issues on page 301](#)

## Log Files

HPCAS log files are located in the following directories on the server:

- \Novadigm\Apache Group\Apache2\logs
- \Novadigm\ClientConfigurationManager\logs
- \Novadigm\ConfigurationServer\log
- \Novadigm\ManagementPortal\logs
- \Novadigm\MessagingServer\logs
- \Novadigm\MobileManagementServer\logs
- \Novadigm\OSManagerServer\logs
- \Novadigm\PatchManager\logs
- \Novadigm\ProxyServer\logs
- \Novadigm\ReportingServer\log

Log file sizes will grow over time. Some logs will be in use while the HPCAS services are running. These active log files should not be deleted. Historical log files can be archived or removed as necessary.

# Agent Deployment Issues

The following table shows common Agent Deployment Job error messages and the steps to take to resolve possible issues.

**Table 17     Agent Deployment Job messages and troubleshooting**

Message	Troubleshooting Steps
Failed to Install HPCA Management Agent - Reason: Failed to connect to <i>device</i> as user <i>user</i> . Code: No network provider accepted the given network path	<p>The HPCAS server creates an administrative share in order to copy the agent install media. Personal firewalls such as Windows Firewall can block the share. Verify that port 3463 and File and Printer Sharing services are added to the firewall exclusion list on the managed device.</p> <p>Access to the Administrative share (C\$) on Windows Vista devices is disabled for locally defined administrators. Therefore, Windows Vista devices should be part of a domain, and the domain administrator's credentials should be specified during Management Agent deployment through the HPCAS console. If the devices are not part of a domain, additional steps are required to allow access for local administrators. See the following link on Microsoft's support web site for detailed steps:</p> <p><b><a href="http://support.microsoft.com/kb/947232/en-us">http://support.microsoft.com/kb/947232/en-us</a></b></p> <p>After making these changes, reboot the device.</p>
Failed to Install HPCA Management Agent - Reason: Failed to connect to <i>device</i> as user <i>user</i> . Code: Logon failure: unknown user name or bad password.	<p>Verify that the login credentials used during the agent deployment wizard are correct and the userID has administrative privileges on the device. Blank passwords are not permitted. For Windows XP devices, verify that Simple File Sharing is not enabled.</p>

Message	Troubleshooting Steps
Connection timed out	After the HPCAS server deploys the agent to the device it establishes a TCP connection to the device using port 3463. If this port is blocked by a personal firewall, the device can not be managed by HPCAS. Verify that port 3463 and File and Printer Sharing services are added to the firewall exclusion list on the managed device.
Timeout waiting for rma to register	After the agent is installed to the device it registers back to the HPCAS server using port 3466. If this port is blocked by a firewall on the HPCAS server, the device can not be managed by HPCAS. Verify that port 3466 is added to the firewall exclusion list on the HPCAS server.
Installation fails when installing manually (using setup.cmd) to a Vista device.	The Administrator account must be used to install the Agent to a Vista device or if another account is used, User Account Control (UAC) must be disabled.

## OS Deployment Issues

This section includes common issues encountered during operating system image deployment.

### TFTP server shuts down after starting

- Check to make sure you do not have another TFTP server running on the same computer.

### PXE cannot traverse subnet

- In order to allow PXE to navigate subnets, the DHCP helper must be enabled. The DHCP helper allows traversal of broadcast traffic on the DHCP ports, broadcast is typically turned off on routers.

# Application Self-service Manager Issues

This section describes common HP Client Automation Application Self-service Manager (ASM) issues and the steps to follow to resolve possible problems.

*Application installation failed, Catalog displays as installed*

## **Issue**

The application may display as installed in the Catalog if the installation program returned a zero upon failure.

## **Possible Resolutions**

The ASD relies on a return code to detect whether or not the installation was a success. The installation must return a code of non-zero in order for the ASM to detect the failure.

This can be accomplished by wrapping the installation in a command file and using logic to validate whether the process was a success or not by returning the proper code.

# Power Management Issues

This section describes issues and possible resolutions for tasks related to the HPCAS power management feature.

*Device does not respond to power commands from the HPCAS server*

If a managed device is not responding to a power on command from the HPCAS server the problem may exist in the configuration of network devices such as routers and switches.

- Test the network path from the HPCAS server to the managed device for Wake-on-LAN support. A number of third party tools exist for sending a remote power on command to a network device. Searching the internet for "Wake-on-LAN tools" will return many free tools for testing this capability.

# Patch Management Issues

This section describes issues and resolutions related to patch management.

## Error deploying patches

If you encounter an error deploying patches to target devices (for example, you see the following error message: WUA Install Result Code 3 HRESULT \$hresult), check to make sure the correct Windows Installer version is installed on target devices receiving patch updates. See the [Patch Management](#) section on page 91 for details regarding minimum versions supported.



# A About Double-Byte Character Support

This section covers the configuration changes that will set the locale for the service operating system (SOS).



When creating an image with the Image Preparation Wizard the locale for your reference and target machines must match. For example, if you want to create a Simplified Chinese OS image, you must run the Image Preparation Wizard 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, and Korean

## Changing the locale

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

- 1 Use a text editor to open `\X86PC\UNDI\linux-boot\linux.cfg` \default. The file looks similar to the following:  

```
DEFAULT bzImage  
  
APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1  
ISVRPORT=3466
```
- 2 Add the `LANG` parameter to the end of the `APPEND` line and set the language code. Valid codes are:
  - `zh_CN` = Simplified Chinese
  - `ja_JP` = Japanese
  - `ko_KR` = Korean

— en\_US = English

- 3 As a result, the file will look similar to the following (the following example sets the language to Japanese):

```
DEFAULT bzImage  
  
APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1  
ISVRPORT=3466 LANG=ja_JA
```

- 4 Save and close the default file.

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

- Specify LANG=xx\_XX in the ServiceCD section of the `romsinfo.ini` file. Where xx\_XX is the language code for the language you want to set. Valid language codes are:
  - zh\_CN = Simplified Chinese
  - ja\_JP = Japanese
  - ko\_KR = Korean
  - en\_US = English
- The file `romsinfo.ini` is part of the Service CD iso.

## Double-byte support for Sysprep files

If using double byte char in Sysprep, the file must be encoded in UTF-8 coding.



# Index

## A

- accessing HPCAS console, 284
- acquiring patches, 49, 91, 150
- Action Bar, 121
  - icons, 131
  - using, 131
- Active state of system tray, 244
- adapt to traffic, 243
- AdaptiveBandwidth, 241
- Add Group Entitlement, 81, 100
- Add Infrastructure Server(s), 141
- adding columns to Service List, 240
- adding group entitlement, 93, 108
- Additional Files advanced publishing mode option, 213
- advanced programmable interrupt controller. *See* APIC
- Advanced Properties, 63
- Agent Deployment
  - silent install, 167
  - wizard, 167
- Agent Explorer, 27, 227
- Agent Removal wizard, 168
- AlertMessage, 241
- All Devices, 66
  - group, 103
- APIC, 104
  - machine, 195
- Application Self-service Manager, 26
  - accessing, 229
  - user interface, 229

- Catalog List, 232
- Global Toolbar, 231
- installing software, 234
- Menu Bar, 231
- refreshing the catalog, 234
- removing software, 235
- Service List, 232
- viewing information, 234

- Application Usage Collection wizard, 170

- Application Usage, discovering, 59

- Audience, 19

- Author, 85

- Author column, 241

- Auto-create locations based on Inventory Data, 147

- Automatic Updates, 89

- Avis, 241

## B

- back button, 126

- bandwidth

- reserving, 243
  - settings, adjusting, 236
  - slider, 236
  - throttling, 236, 243, 245

- Bandwidth Control, 245

- Bare-metal, 103

- BIOS power management, 189

- blade server reports, 127

- bootsect.exe, 36, 188

- browse back button, 132

- browse forward button, 132

- browsing, 132

- items in a report, 131

Build Mass Storage Section in Sysprep.inf check box, 195

Button Bar, 245

## C

catalog

- refreshing, 231
- selecting, 232
- virtual, 232

Catalog List, 232

Catalog Visibility, 84

CCM\_PUBLISHER, 80

CCM\_SMM, 80

CCM\_TPM\_ENABLEMENT, 80

CCMDB\_Data.MDF, 33

CMI, configuring, 154

collection filter

- creating, 161
- enabling, 161
- modifying, 162

Columns Available list box, 240

Columns to show list box, 241

Component Select publishing, 214

CompressedSize column, 241

configuring

- ODBC settings, 158
- OS deployment mode, 153
- patch acquisition
  - schedule, 150
  - settings, 151
- reporting, 157
- S.M.A.R.T., 155
- schedules, 48
- TPM, 156

conmfiguring

- CMI, 154

Connection options, 242

Console, 24

console access, 137

console user

- creating, 138
- removing, 138
- viewing and modifying details, 139

Create a New Location, 147

Create Groups, 50

creating

- Dynamic Discovery Groups, 173
- Dynamic Reporting Groups, 134, 174
- groups, 68
- New Location, 147
- static group, 172

Current Jobs

- Device Management, 63
- Group Management, 77
- Job Management, 113
- OS Management, 111
- Patch Management, 97
- Software Management, 87

Customize colors option, 239

## D

Data Filters, 120, 123

database setup, 33

Delete Device(s), 141

Delete Devices, 57

Delete Job(s), 114, 115

Delete Location(s), 147

Delete Operating System, 101

Delete Patch, 92

Delete Software, 81

Deploy Operating System, 100

Deploy Software, 81

Deploy the Infrastructure Service, 141

Deploy the Management Agent, 56

Deploy.cab, 190

Deploy.chm, 190

deploying

- Management Agent, 47, 54
- operating systems, 101
- OS image using PXE, 106
- patches, 50, 77, 91, 92
- software, 50, 76, 81, 287
- deployment
  - mode, 101, 181
  - scenarios, os images, 102
- Description column, 241
- device compliance report, 291
- Device Details, 62
  - Advanced Properties, 63
  - general, 62
  - groups, 63
  - os, 63
  - patches, 63
  - properties, 62
  - reporting, 63
  - software, 63
- device discovery, 166
- Device Management, 54
  - Current Jobs, 63
  - Devices, 55
  - General, 54
  - Past Jobs, 64
- Device Summary, reporting, 133
- devices
  - discovery, 57
  - importing, 47, 54, 57
  - removing, 61
- Directory/Group Filters, 120, 122
- discovering
  - devices, 57
- discovery group, 69
- Display Options, 120, 125
- docked Status window, 237
- document changes, 4
- Dynamic Reporting Groups, creating, 134, 174

## E

- Embedded Linux, 105, 204
- Ended with Errors, 114, 115
- Enterprise, 21
- entitling
  - patches, 50, 76
  - software, 50
- ErrorCode, 241
- Expand active catalog item, 241
- Expand active service item, 241
- Expand/Collapse button, 233
- Export Service, 81, 92, 100
- export services, 83
- Export to CSV, 56, 67, 81, 92, 100, 114, 131, 140, 147
- Export to IQY, 131
- exporting
  - services, 109
- exporting services, 94
- ExtendOemPartition parameter, 189, 192

## F

- file header information, 162
- filters
  - applying, 123
  - value characters, 124
  - wildcards, 124
- firewall settings, 30
- Focus Time, 128

## G

- generating reports, 51
- Global Toolbar, 231
- Group Creation wizard, 172
- group details, 72
  - current jobs, 74
  - devices, 73
  - general, 73

- os, 73
- patches, 74
- properties, 73
- reporting, 74
- software, 74
- group details window, tasks, 74
- Group Management, 65
  - Current Jobs, 77
  - General, 65
  - Groups, 66
  - Past Jobs, 78
- group type, 73
- groups
  - adding
    - patch entitlement, 76
    - software entitlement, 75
  - creating, 68
  - deploying software, 76
  - discovery, 66
  - internal, 66
  - removing, 71
    - patch entitlement, 76
    - software, 76
    - software entitlement, 75
  - reporting, 66
  - static, 66
  - types, 66

## H

- HAL, 104
- Hardware Abstraction Layer. *See* HAL
- hardware inventory. discovering, 59
- Hardware Management, 154
- Help, 28
- hibernation, 190
- History button, 236
- Home button, 232
- HP Client Automation Administrator Publisher, 80
- HP Hardware reports, 129
- HP Instant Support, 151

- HP Softpaqs, publishing, 221
- HPCA Administrator Publisher, 27
- HPCA Agent ID, 127
- HPCA Agent Version, 127
- HPCA Status window, 244
  - Status area, 245
  - Status Message area, 245
- HPCA System Tray icon, 244
- HPCAS, 19
  - installing, 33
- HPCAS server, firewall settings, 31
- hpccm.exe, 35, 42

## I

- Idle state of system tray, 244
- image file, spanning, 189
- Image Preparation Wizard, 189
- Image Preparation Wizard, 27
- Image Preparation Wizard, 192
- Image Preparation Wizard
  - using, 193
- Image Preparation Wizard
  - using, 199
- Image Preparation Wizard
  - using, 202
- Image Preparation Wizard
  - using, 206
- ImageName.EDM, 193, 198, 202, 206
- ImageName.IMG, 193
- ImageName.MBR, 193
- ImageName.PAR, 193
- imagex.exe, 36, 188
- Import Device wizard, 166
- Import Devices to Manage, 56
- Import Service, 81, 92, 100
- import services, 82

- importing
  - devices, 57
  - services, 93, 108
- importing devices, 47
- Information Panel of HPCA Status window, 245
- Infrastructure Management, 140
- Infrastructure Server
  - service cache, 143
  - synchronizing the service cache, 143
- Infrastructure service, 140
- Install button, 233
- Install Command Line, 85
- InstalledDate column, 241
- installing
  - HPCAS, 29, 33
  - Management Agent
    - manually, 39
    - thin clients, 39
    - Windows CE, 42
    - Windows XPe, 41
  - Publisher to separate device, 37
  - software using Application Self-service Manager
    - user interface, 234
- Instant Support, 151
- Internet proxy detection, 243
- inventory
  - discovering, 59
  - discovering for group of devices, 70
- Inventory Collections, 56
- Inventory Management Reports, 127

## J

- job controls, 113
- Job Details, 116
  - details, 117
  - services, 117
  - targets, 117
- Job Management, 113
  - Current Jobs, 113
  - General, 113

- Past Jobs, 117

- Job Status, 114

- JoinDomain parameter, 192

## L

- Last Connect, 127
- last logged on user, 62
- Last Logged on User, 127
- Last Synchronized, 144
- license key
  - update, 288
- licensing information, updating, 137
- Local Service Boot, 105
- LocalRepair column, 241
- Location
  - assigning to infrastructure server, 148
  - creating new, 147
  - removing, 148
- Locations, 140, 147
- log files, downloading, 136
- logfiles.zip, 137
- logging in, 45

## M

- management
  - devices, 54
  - groups, 65
  - jobs, 113
  - operating systems, 99
  - patches, 89
- Management Agent, 26
  - deploying, 47, 54, 58
  - deploying to group, 69
  - installing
    - Windows CE, 42
    - Windows XPe, 41
  - installing manually, 39
  - removing, 58
    - Windows XPe, 41
  - removing from a group of devices, 69

Management Options publishing option, 213

managing

jobs, 113

software, 79

manual input, 166

Mass Storage Drivers, 195

Maximum items per window, 132

Menu Bar, 231

Microsoft Automatic Updates

important information, 89

Microsoft patch, 288

Microsoft Sysprep, 190

My Software button, 232

## N

Name column, 241

## O

obfuscation of usage data, 59, 71, 158

obfuscation of usage date, 159

ODBC DSN, 35

ODBC settings, configuring, 158

online help, 28

operating system images, publishing, 216

Optimize compression of unused disk space check  
box, 195

OS Deployment wizard, 181

OS Details, 109

Devices, 111

General, 110

Groups, 111

Properties, 110

Reporting, 111

OS image Target Devices

requirements, 103

OS Management, 99, 153

Current Jobs, 111

General, 99

Operating Systems, 100

Past Jobs, 112

OS partition, 192

OS Service Pack, 288

Overview, 21

OwnerCatalog column, 241

## P

partitions

extending, 189

password

change, 139

Past Jjobs

Patch Management, 97

Past Jobs

Device Management, 64

Group Management, 78

Job Management, 117

OS Management, 112

Software Management, 87

patch acquisition, 286

schedule, 150

settings, 151

Patch Compliance

discovering, 59

patch compliance discovery schedule, 287

Patch Compliance Discovery wizard, 169

Patch Deployment Wizard, 178

patch details, 94

devices, 96

general, 95

groups, 95

properties, 95

reporting, 97

patch management

configuration, 149

Patch Management, 89

Current Jobs, 97

General, 91

- Past Jobs, 97
- Patches, 92
- Patch Management Reports, 128
- patches
  - acquiring, 49, 91, 150
  - adding group entitlement, 93, 108
  - deploying, 50, 77, 91, 92
  - entitling, 50, 76
  - removing entitlement, 77
- Pause Job(s), 114
- Perform client connect after OS install check box, 200, 207
- Power Management, 56, 61
- Power Management for a group of devices, 71
- Power Management wizard, 171
- Preferences button, 232
- prepwiz.exe, 194, 199, 202
- Pre-uninstall Command Line, 85
- Price column, 242
- Properties publishing option, 213
- Proxy, 35
- proxy detection, 243
- published services, viewing, 226
- PublishedDate column, 242
- Publisher, 27
  - accessing, 38
  - installing to a separate device, 37
  - using, 211
- publishing
  - component select, 214
  - modes
    - additional files, 213
    - management options, 213
    - properties, 213
    - transforms, 213
  - os images, 99
  - software, 49, 212
- publishing HP Softpaqs, 221
- PXE, 106

PXE boot, 104

## Q

Quick Start Tasks, 45

## R

RDP, 60

Reboot, 242

Reboot Settings, 85

reference machine  
preparing, 187

Refresh Data, 56, 81, 100, 113, 140, 147

refreshing catalog, 231

Remote Control, 57, 60

Remove button, 233

Remove Infrastructure Server (s), 141

remove software, 83

Remove the Infrastructure Service, 141

Remove the Management Agent, 56

removing
 

- columns from Service List, 241
- Management Agent
  - thin client, 41
  - Windows XPe, 41
- operating systems from library, 109
- patch entitlement, 77
- software, 76, 235

Report Windows, 121

reporting
 

- configuring, 157
- interface, 119
- windows, 130

Reporting, 119

reporting groups
 

- creating, 131
- creating from report query, 131

Reporting tab, 119

Reporting Views, 120, 125

- reports
  - generating, 51
  - viewing, 51
- RepublishedDate column, 242
- Reschedule a job, 115
- Reschedule Job(s), 114
- reserve bandwidth, 243
- ReservedBandwidth, 242
- Resize partition before OS upload check box, 195
- Resume Job(s), 114

## S

- S.M.A.R.T.
  - configuring, 155
  - enabling, 155
- S.M.A.R.T. Alerts
  - reports, 127
- schedule inventory, 285
- ScheduleAllowed, 242
- schedules, configuring, 48
- SCSI, 104
- Search Criteria, 121
- Search Options, 120
  - filters, 122
  - using, 122
- Self-Monitoring, Analysis, and Reporting Technology. *See* S.M.A.R.T.
- Server Details window, 144, 145
- Service CD, 107
- Service Entitlement wizard, 179
- Service Export wizard, 176
- Service Import wizard, 176
- Service list, 232
  - Expand/Collapse button, 233
  - Install button, 233
  - options, 240
  - Remove button, 233
- Service List
  - adding columns, 240
  - removing columns, 241
- services
  - exporting, 94, 109
  - importing, 93, 108
- Settings Migration Manager, 28
- Settings Migration Manager service, 80
- Settings Migration Utility, 28
- setup.exe, 290
- Setupmgr.exe, 191
- Show advanced operations, 241
- Show Extended Information, 235
- Show grid lines, 241
- Size column, 242
- small computer systems interface. *See* SCSI
- software
  - adding group entitlement, 82
  - deploying, 50
  - entitling, 50
  - publishing, 49, 212
  - removing, 235
- Software Category, 84
- Software Deployment wizard, 175
- software details, 83
  - devices, 86
  - general, 84
  - groups, 85
  - properties, 84
  - reporting, 87
- software inventory, discovering, 59
- Software Management, 79
  - Current Jobs, 87
  - General, 79
  - Past Jobs, 87
  - Software, 80
- Software Removal wizard, 180
- Software/Hardware Inventory wizard, 169
- Sort Column, 132



- Span image files, 189
- SQL Server, 30
- SQL Server Enterprise Manager, 34
- SQL Server Management Studio, 34
- SSM, 222
- SSM compliant, 222
- Standard, 21
- Start Job(s), 114
- Starter, 21
- static group, 73
- static groups
  - adding devices, 75
  - creating, 172
  - removing devices, 75
- Status button, 237
- Status column, 242
- Status window
  - docking, 237
  - undocking, 237
- Stop Job(s), 114
- support, 135
  - contacting, 293
- Synchronize Infrastructure Server, 143
- Synchronize Software, 76
- Synchronize the selected Infrastructure Servers
  - service cache, 141
- Sysprep.inf file, 190
- SysprepMassStorage section, 195
- system requirements, 29
  - target devices, 103
- system tray
  - active state, 244
  - idle state, 244
- SystemInstall, 242

## T

- target device

- definition, 103
  - requirements, 103
- target devices
  - firewall settings, 30, 31, 142
- TCP ports, 30
- thin client, 105
  - deploying factory OS images to, 105
  - deploying Management Agent to, 39
- Thin client
  - management, 23
  - prepare and capture images, 197
  - requirements, 30
- thin clients
  - installing Management Agent, 39
- throttling, 243
- ThrottlingType, 242
- TimeZone parameter, 192
- TPM
  - configuring, 156
- TPM Enablement service, 80
- transform file, 214
- Transforms publishing option, 213

## U

- UAC. *See* User Account Control
- UIOption, 242
- UnattendMode parameter, 192
- undocked Status window, 237
- Un-install Command Line, 85
- UpgradedDate column, 242
- Url column, 242
- Usage Collection, 159
- Usage Collection Agent, 162
- Usage Collection Filter
  - configuring, 161
  - creating, 161
  - enabling, 161
  - modifying, 162

- Wizard, 161
- Usage Count, 128
- Usage Criteria, defining, 162
- usage data, filtering, 163
- usage data, obfuscating, 159
- Usage Managed Products (Used), 130
- Usage Manager Reports, 128
- Usage Settings tab, 158
- Usage Status, 128
- Usage Time, 128
- Use system colors option, 239
- User Account Control, 297
- User Creation wizard, 180
- User Details window, 139
- user interface for Application Self-service Manager, 229

## V

- Vendor, 85
- Vendor column, 242
- VerifiedDate column, 242
- version, 284
- Version column, 242
- view inventory, 286
- View, applying, 125
- viewing
  - information in Application Self-service Manager
    - user interface, 234
  - published services, 226
  - reports, 51
- virtual catalogs, 232
- VMware
  - installation requirements, 32
  - installing HPCAS to, 32
- VNC, 60

## W

- web browser support, 29
- Web Site, 85
- Windows 2003 Server, 36
- Windows CE, 105, 201
- Windows Installer files, 212
- Windows Installer package, 290
- Windows Remote Desktop, 60
- Windows XP Embedded, 105
- Windows XPe, 197
- wizards, 165
  - agent deployment, 167
  - agent removal, 168
  - application usage collection, 170
  - group creation, 172
  - import device, 166
  - os deployment, 181
  - patch compliance discovery, 169
  - patch deployment, 178
  - power management, 171
  - service export, 176
  - service import, 176
  - software deployment, 175
  - software entitlement, 179
  - software removal, 180
  - software synchronization, 177
  - software/hardware inventory, 169
  - user creation, 180

## X

- XPe, 105