HP Client Automation

Core and Satellite

Standard Edition

for the Windows® operating system

Software Version: 8.10

User Guide

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

Copyright Notice

Trademark Notices

Acknowledgements

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Introduction

HP Client Automation Standard 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, and software distribution and usage metering all from an integrated web-based console.

About This Guide

This guide provides detailed information and instructions for using the HP Client Automation Console, Publisher, Application Self-service Manager, and the Image Preparation Wizard.

For requirements and directions on installing and initially configuring HPCA Core and Satellites Servers, refer to the Installing HPCA chapter.

HPCA Documentation

The HP Client Automation documentation that is available on the media is also installed during the Core installation. These documents are available as PDFs and can be accessed on the Core server using the Windows Start menu, the shortcut link on the desktop, or by using a browser from any device with access to the Core server machine at: `http://HPCA_Host:3466/docs`, where `HPCA_Host` is the name of the server where HPCA is installed.

Abbreviations and Variables

Table 1   Abbreviations Used in this Guide

Abbreviation	Definition
HPCA	HP Client Automation
Core and Satellite	HPCA environment consisting of one Core server and zero or more Satellite servers. All features are installed as part of the Core or Satellite server installation.
Portal	HPCA Portal

Table 2   Variables Used in this Guide

Variable	Description	Default Value
InstallDir	Location where the HPCA server is installed	Core and Satellite installation: For a 32-bit OS: `C:\Program Files\Hewlett-Packard\HPCA` For a 64-bit OS: `C:\Program Files(x86)\Hewlett-Packard\HPCA`
SystemDrive	Drive label for the drive where the HPCA server is installed	`C:\`

2 Installing HPCA

This chapter explains how to install and configure the HP Client Automation servers (Core and Satellite) and their components. The following sections contain pre-installation information and requirements, and installation instructions for the HPCA servers. It also details the optional, manual installation of the HPCA Administrator which, by default, is automatically installed with the HPCA Core server.

- HPCA Server Pre-installation Information on page 28
- Create the HPCA Database on page 34
- Installing the HPCA Server on page 37
- Configuring Core Server on Windows 2003 on page 45
- Manually Installing the HPCA Administrator on page 46
- Using HPCA to Manage Windows Operating Systems on page 48
- Out of Band Management on page 48
- Windows Services on page 49

HPCA Server Pre-installation Information

The pre-installation information that is presented in this section should be reviewed before installing any HPCA product for which you have a license.

Core Servers

The **HPCA Core** server is the primary repository of data for an HP Client Automation environment. At least one Core server is necessary in order to establish a viable HPCA environment.

The Core server cannot be installed on a machine that already hosts an HPCA Satellite server. If this is attempted, an error message will result and the installation program will abort.

After the installation, you will have to use the HPCA Administrator to prepare software applications for deployment throughout your enterprise.

The HPCA Administrator

The HPCA Administrator is automatically installed as part of the Core server installation. It points to the Core server's database and includes a set of administrative tools that can be used to configure and maintain an HPCA environment.

For information on manually installing the HPCA Administrator, see Manually Installing the HPCA Administrator on page 46.

> ► The Standard and Starter editions automatically install a streamlined version of the HPCA Administrator—containing only the *HPCA Publisher* and *HPCA Agent Explorer*.

Satellite Servers

The **HPCA Satellite** server is an access point to the HP Client Automation infrastructure for all HPCA agents. It is dependent on and subservient to the HPCA Core server, and functions as an intermediary between the Core and the HPCA agents.

The Satellite server cannot be installed on a machine that already hosts an HPCA Core server. If this is attempted, an error message will result and the installation program will abort.

A Satellite Server can be installed manually on a device or can be deployed from the Console. For information about manually installing a Satellite, see HPCA Core Server Installation on page 39.

Platform Support

For the operating system requirements for this release, refer to the HPCA Support Matrix available at the HP Software Product Manuals web site. See the Documentation Updates section in the front matter of this guide for the URL and information about how to access this web site. The matrix is also located on the distribution media for this product in the \Documentation directory.

System Requirements

This section details the system requirements for Core and Satellite server installations.

▶ It is important to keep in mind that some of these requirements are for initial HPCA-environment setups (program data only), and that as your HPCA environment grows, these space requirements will inherently grow as well, in order to accommodate database expansion and caching.

The recommended starting minimum is 20 GB.

Core Servers

The following are the system requirements for Core servers.

- 2 GB RAM (minimum); 4 GB RAM (preferred)
- Dedicated server with dual-core processor
- 2 GHz CPU speed
- 3 GB free disk space

Satellite Servers

The following are the system requirements for Satellite servers.

- 512 MB RAM (minimum); 1 GB RAM (preferred)
- Dual-core processor
- 1.6 GHz CPU speed
- 2 GB free disk space

Web Browsers

The HPCA servers have Consoles through which various administrative and configuration tasks can be performed. For these Consoles, only the following web browsers and versions are supported.

- Microsoft Internet Explorer, versions 7.0, 8.0, and 9.0.

  > The browser's Security should be set no higher than **Medium**.

- Mozilla Firefox, version 3.6, 4.0, 5.0, and 6.0.

Monitor Settings

HP recommends the following minimum settings in order to ensure proper display of the HPCA Consoles.

- Screen Resolution: 1024x768
- Color Quality: Medium (16 bit)

HPCA Database

Prior to installing the Core server, you must create an ODBC-compliant database to be used by HPCA for management-reporting objects. This database must be a Microsoft SQL Server Database. See Create the HPCA Database on page 34 for information about creating these databases specifically for the Core server.

Communications Ports

HPCA servers communicate with one another and their managed devices on the ports that are detailed in this section; these ports must be available. The system query that automatically runs at the start of the installation will verify the availability of these ports. If they are not available, the installation will fail.

If a firewall is in place on the HPCA server's host machine, these ports must be added to the firewall "exceptions" list.

Mandatory Ports

When SSL is not enabled, ports **3464** and **3466** are the primary ports used for Core and Satellite communications, so they must be enabled in order to ensure the necessary remote communications between HPCA devices. An HPCA environment will not function if these two ports are not enabled.

These ports can be automatically enabled with an option (**Modify Windows Firewall to allow communications through these ports**) in the HPCA server installation. If you select this option in the installation, no additional port configuration is required.

Some environments have specialized firewalls in place and prefer to not select this option. If this is the case, you must ensure that these two primary ports are excluded from any firewall filtering, otherwise HPCA will not function correctly—remote devices will not be able to communicate with HPCA servers.

When SSL is enabled on a satellite, SSL is used for all inbound communications.

HPCA Ports

- **TCP 3464**: This is the default port of the HPCA Configuration Server; it must be available for Core servers.

- **TCP 3465**: This port is used by HPCA agents to receive incoming notify requests from Core servers.

- **TCP 3466**: This is the main HTTP port that this server will use for communications with other HPCA (Core and Satellite) servers, as well as HPCA agents. All unicast data downloads are handled on this port.

- **UDP 9100**: This is the default port of the HPCA Multicast Server.

- **TCP 443** (SSL): This port is used for "secure HTTP" (**HTTPS**) communications.

- **TCP 444** (SSL): This port is used for "secure TCP" (**TCPS**) communications when the HPCA Configuration Server is enabled.

> This port must be available on all Core server host machines.

Out of Band Management Ports

If you will be using Out of Band Management, the following additional ports must be available to allow for inbound and outbound traffic.

For OOB Management Console-to-vPro Device Communications

- **162**: For alert management. Note that port 162 is a standard SNMP port this will conflict if you are already running an SNMP receiver on the HPCA Core server.

- **9999**: The default starting port for communication between the SOL display applet and the server's web application. This can be configured by editing the *<HPCA_Install_Dir>*\OOBM\conf\config.properties file.

- **16692**: For web service traffic over TCP.

- **16693**: For web service traffic over TLS (with client authentication).

- **16694**: For SOL/IDE-R over TCP.

- **16695**: For SOL/IDE-R over TLS (with client authentication).

- **9999**: For applet-to-server socket communications for SOL. This port must also be available on the client browser system as well.

- **9998**: For communications between the OOB Management Console and the local agent during Remote Configuration of vPro devices.

- **623**: For communications with DASH devices.

VMware Requirements

If you are installing HPCA to a VMware environment with a Windows XP Professional host operating system, the installation might hang. Disabling **Acceleration** in the VMware **Advanced Options** should allow the installation to continue. **Acceleration** can then be re-enabled after the installation completes.

▶ HPCA installed to a VMware environment should be used for testing or evaluation purposes, only.

If you are installing HPCA to a VMware environment, the following requirements must be met.

- VMware, minimum version 6.02
- 2 GB Memory allocated
- 8 GB HDD space allocated (additional space might be required for migration)
- Host OS: Windows 2003 Server or Windows 2008 Server
- Guest OS: Windows 2003 Server or Windows 2008 Server
- Host system: dual processors (minimum 2 GHz CPU) so that VMware can set affinity to 1, if needed.
- See the System Requirements on page 29 for additional HPCA server requirements.

The HPCA Agent

The HPCA agent is the client machine-based HPCA component that gets installed on end-user machines. This component has several sub-features that enhance its capabilities. The HPCA agent can be deployed to end-user machines from the Core Console, or it can be manually installed on these machines.

Windows AIK Installation

If you plan to use HPCA to manage Windows operating systems, you will need to install the Windows AIK on the machine that will host the HPCA Core and ensure that copies of these utilities are placed in the proper location.

You can download the Windows AIK from the Microsoft Download Center (http://www.microsoft.com/downloads).

⚠ Be sure to install the Windows 7 version of the Windows AIK in the default location:

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

It is best to install the Windows AIK before you install the HPCA Core.

Create the HPCA Database

Prior to installing the Core, you must create an ODBC-compliant database to be used by HPCA.

▶ If you do not know how to create an ODBC-compliant database, contact your database administrator.

The following provides information on the pre-requisites and procedures for creating a Microsoft SQL Server database.

Create a SQL Server Database for the HPCA Core on page 35

> You must also define an ODBC DSN for each database you create.
>
> If you do not know how to create an ODBC DSN, contact your database administrator.

Create a SQL Server Database for the HPCA Core

Follow the instructions in this section to create a Microsoft SQL Server database for the reporting objects for the Core server. If you do not have security rights to create the database, contact your SQL database administrator.

SQL Server Database Prerequisites and Notes

- Microsoft SQL Server 2005 or Microsoft SQL Server 2008 must be locally installed or remotely accessible from the HPCA server.

  Microsoft SQL Server Express Edition is supported with HP Client Automation for small environments. Microsoft limits this edition in both performance (CPU and memory usage) and database size. Very small environments using HPCA can use SQL Server Express Edition but will need to monitor the performance and size of the database. If performance is unacceptable or if the database nears the maximum size, you should upgrade to one of the other SQL Server editions. Refer to the Microsoft SQL Server web site for details of each SQL Server edition.

- SQL Server must be configured to use **mixed-mode authentication** and must have TCP/IP support enabled.

- **Windows 64-bit ODBC DSNs Require 32-bit Drivers**: HP Client Automation components that are running on Windows 64-bit operating systems run in **32-bit emulation mode**. So, when using ODBC drivers on a Windows 64-bit operating system, create the ODBC System DSN for the database using 32-bit drivers.

  On a 64-bit operating system, access the 32-bit ODBC Data Source Administrator by running `C:\Windows\SysWOW64\odbcad32.exe` to create or modify the System DSNs that are required by HPCA products.

- The "storage" sizes that are documented in this section are recommendations only. Customize these values based on the number of managed devices in your environment and the type of information that will be collected.

SQL Server Communications with HPCA

- If SQL Server is installed on a server other than that which houses the HPCA server, firewall rules might need to be added in order to enable communications between them. Refer to the Microsoft KnowledgeBase article **841251** at **http://support.microsoft.com/kb** for information on opening required ports for SQL Server.

- SQL Server must be configured to use static ports. For information on how to use static ports, refer to your SQL Server documentation.

To create a SQL Server database for the HPCA Core

⚠ If you do not know how to create a SQL Server database, contact your database administrator.

If you do not know how to create an ODBC DSN, contact your database administrator.

1   On the Microsoft SQL Server, create a database with the following recommended settings.

General tab	Name: a name of your choice, no blanks or underscores (for example, **HPCACORE**)
Data Files tab	Initial Size: 500 MB
	Select Autogrow by 20%
Transaction Log tab	Change initial size: 100 MB

2   Use SQL Server Authentication.

3   Change the default database to the database name that you used in step 1

▶ The SQL Server name, admin user ID, and password are required during HPCA installation.

4   Provide the user with the minimum role membership of db_datareader, db_datawriter, and db_ddladmin for the SQL Server database.

5   On the computer that will host the Core server, create an ODBC System DSN with a name of your choice (for example, **HPCAODBC**) and point it to the new Core database on the SQL Server.

The database is now attached and you can proceed with the installation of the HPCA server. It is documented in HPCA Core Server Installation on page 39.

Installing the HPCA Server

This section details the installation of the HPCA Core server and the Satellite server using the HPCA Installer.

Installation Checklist Information

This section details some additional information that you should review before conducting the installation.

Installation Restrictions

The Core server cannot be installed on a machine that already hosts an HPCA Satellite server; the Satellite server cannot be installed on a machine that already hosts an HPCA Core server.

If either of these installations are attempted, an error message will result and the installation program will abort.

Core Domain Name

HP recommends always specifying the fully qualified domain name when prompted for HPCA server names. This practice will ensure the proper mapping to the servers when "downstream" Satellites and HPCA agents are installed.

Database Setup

Before installing an HPCA server, you must set up your Microsoft SQL Server database for the HPCA Core server. See the section, Create a SQL Server Database for the HPCA Core on page 35 for database setup instructions.

Default Installation Directories

The HPCA Core and Satellite servers' installations create the following directories by default; alternative directories for the server and data files can be selected during the installation.

▶ The directories that are listed in this section are specific to English language-based operating systems. On non-English language-based operating systems, the HPCA server installation will create these directories in the appropriate default locations.

- The Core and Satellite server files are installed to Hewlett-Packard\HPCA in the default 32-bit \Program Files directory.

- The Core and Satellite server data files are installed to Hewlett-Packard\HPCA\Data in the default 32-bit \Program Files directory.

- The Core and Satellite server installations each spawn two log files, both of which are placed in the Local Settings\Temp directory of the user who ran the installation.

    — The file, hpca-install.log, is always created for both installations.

    — A server-specific log file (either HPCACore_setup.log or HPCASatellite_setup.log) will also be created—regardless of whether the installation was run with the .msi or .exe file.

Log File Considerations

- If setup.exe is used to run the installation, the location can be altered in setup.ini (with the log.filename entry in the options section) prior to the installation.

Windows Services

After the Core and Satellite servers are installed, they will be running as Windows services. For additional information, see Windows Services on page 49.

Modifying Installation Files

Files used during the installation can be modified. For example, if newer versions of the files are available from an update, they can be included during the installation using the following procedure.

1   Copy the HPCA installation files to a new location.

2   Create new sub-directories.

   a   To modify installation files, create a new directory called `Updates` in the same directory as the `.msi` file.

   b   To apply additional export decks to the HPCA database after all other standard decks are applied, create a new directory called `Decks`.

3   Add any files you would like to be used during the installation. For example, if you want to run the Core installation with a different `em.war` file, create the following directory path:

   `<source dir>\Updates\tomcat\webapps\em.war`

4   Run the installation. The new files will be used.

HPCA Core Server Installation

Install the HPCA server to a dedicated server in your environment. Before you proceed with the installation, make sure to read the Installation Checklist Information on page 37.

If you are upgrading the HPCA server, use the migration scripts for the backup and restore of files. For more information on migration and restore, see the *HP Client Automation Starter and Standard Editions Migration Guide*.

▶   HP recommends specifying the fully qualified domain name when prompted for HPCA server names. This practice will ensure proper mapping to the servers when "downstream" Satellites and HPCA agents are installed.

Installing the HPCA server

1   Log on as a user with `Administrative` privileges on the system where you plan to install the HPCA Core server.

2   Insert the installation media into the DVD drive. Navigate to the
    `Setup-Core` directory to access the Core server installation files.

3   Double-click the **setup.exe** file. The HP Client Automation Core Installer
    window opens.

4   Click **Next**. The HP Client Automation Software License Agreement page
    opens.

5   Review the HP Client Automation Core license terms, select **I accept the
    license agreement**, and then click **Next**. The HP Client Automation
    Installation Folder page opens.

6   The Installation Folder page displays the default installation directory for
    the HPCA Core server (listed in Default Installation Directories on
    page 38).

    Accept the default location, or click **Browse** to select a different location,
    and then click **Next**. The HP Client Automation Data Folder page opens.

7   The Data Folder page displays the default directory for the HPCA Core
    server data files (listed in Default Installation Directories on page 38).

    Accept the default location, or click **Browse** to select a different location,
    and then click **Next**. The HP Client Automation Host Name page opens.

8   Select a name for this HPCA server and click **Next**. The HP Client
    Automation Server Ports window opens.

9   Accept the default ports, or specify web server and Configuration Server
    ports, and then click **Next**. The HP Client Automation Installation
    Confirmation page opens.

    ➤   The default ports cannot be changed in the Standard and
            Starter editions of HPCA.

    Optionally, select **Modify Windows Firewall to allow communications through
    these ports** if you want to automatically enable ports 3464 and 3466. For
    more information, see Mandatory Ports on page 31.

10 Click **Next** to start the installation. The installation process initiates the
    different configuration scripts that can run for several minutes.

11 Click **Finish** to complete the HP Client Automation Core server installation.

> After installation, it is normal to see some errors reported in the log files. These errors can be safely ignored. They will self-correct once the First Time Setup Wizard has run completing the setup of the product.

The HPCA Console will automatically open, and the login window will be displayed in your default browser.

12 On the login window, specify the default user name, password, and directory source.

— The default user name is **admin** and the password is **secret**.

> HP recommends changing the default user name and password. This can be done on the Configuration panel of the HP Client Automation Console by selecting **Access Control** -> **Users**, and clicking the **Create New User** icon in the Users area.

13 Click **Sign In**. The First Time Setup Wizard opens and prompts you for initial configuration settings for your HPCA environment. You can modify these settings in the various panels of the HPCA Console also.

14 Click **Next** on the Introduction page to begin the wizard.

15 On the License page, copy and paste the contents of your HP-issued, product-specific license file into the License Data box and click **Next**.

If you do not have a license at this point, a temporary Client Automation Standard edition evaluation license is generated that is valid for 90 days after you install HP Client Automation. This license provides limited functionality within the Console.

16 On the Database Source page, click **Use an existing ODBC connection already on the server** and click **Next**.

17 On the Database Settings page, specify the appropriate values in the various mandatory fields and click **Next**.

18 On the Services page, select the HPCA services that this HPCA server will provide and click **Next**. The configuration selections are saved.

▶ The services that are presented in this window are recommended for HPCA environments but they do not have to be enabled here. They can subsequently be enabled on the Configuration panel of the HPCA Console.

19 On the Complete page, click **Finish** to complete the configuration tasks.

For more information on configuring these services in the HPCA Console, refer to the *Configuration* chapter.

HPCA Satellite Server Installation

Installing the HPCA server

1 Log on as a user with Administrative privileges on the system where you plan to install the HPCA Satellite server.

2 Insert the installation media and navigate to the `Setup-Satellite` directory to access the Satellite server installation files.

3 Double-click **setup.exe**. The HP Client Automation Satellite Installer window opens.

4 Click **Next**. The HP Client Automation Software License Agreement page opens.

5 Review the HP Client Automation Satellite license terms, select **I accept the license agreement**, and then click **Next**. The HP Client Automation Installation Folder page opens.

6 The Installation Folder page displays the default installation directory for the HPCA Satellite server (listed in Default Installation Directories on page 38).

Accept the default location, or click **Browse** to select a different location, and then click **Next**. The HP Client Automation Data Folder window opens.

7 The Data Folder page displays the default directory for the HPCA Satellite server data files (listed in Default Installation Directories on page 38).

Accept the default location, or click **Browse** to select a different location, and then click **Next**. The HP Client Automation Host Name page opens.

8 Select a name for this HPCA server and click **Next**. The HP Client Automation Server Ports page opens.

9 Accept the default ports, or specify web server and Configuration Server ports.

> ▶ The default ports cannot be changed in the Standard and Starter editions of HPCA.

Optionally, select **Modify Windows Firewall to allow communications through these ports** if you want to automatically enable ports 3464 and 3466. For more information, see Mandatory Ports on page 31.

10 Click **Next** to start the installation. The installation process initiates the different configuration scripts that can run for several minutes.

11 Click **Finish** to complete the HP Client Automation Satellite server installation.

> ▶ After installation, it is normal to see some errors reported in the log files. These errors can be safely ignored. They will self-correct once the First Time Setup Wizard has run completing the setup of the product.

The Windows Security login window opens in your default browser.

12 On the login window, specify the default user name and password. The default user name is **admin** and the password is **secret**.

> ▶ HP recommends changing the default user name and password. This can be done on the Configuration panel of the HP Client Automation Console by selecting **Access Control** -> **Users**, and clicking the **Create New User** icon in the Users area.

13 Click **OK**. The First Time Setup Wizard opens that prompts you for initial configuration settings for your HPCA environment. You can modify these settings in the various panels of the HPCA Satellite Console also.

14 Click **Next** on the Introduction page to begin the wizard. The Upstream Server page opens.

15 Specify a valid upstream host, and click **Next**. The Upstream Host field accepts textual hostnames and IP addresses (in the standard IP-address format). The License page opens, which is pre-populated with license information from the Satellite's upstream server.

16 Click **Next** to continue to the Services page.

17 Select the HPCA services that this HPCA server will provide and click **Next**. The configuration selections are saved.

> The services that are presented in this window are recommended for HPCA environments but they do not have to be enabled here. They can subsequently be enabled on the Configuration panel of the HPCA Satellite Console.

18 Click **Next**. The configuration selections are saved.

19 On the Complete page, click **Finish** to complete the configuration tasks.

HPCA Documentation

The HPCA documentation that is available on the media is also installed during the Core installation. These documents are available as PDFs and can be accessed on the Core server using the Windows **Start** menu, the shortcut link on the desktop, and by using a browser from any device with access to the Core server machine at `http://HPCA_Host:3466/docs`, where *HPCA_Host* is the name of the server on which HPCA is installed.

Removing HPCA

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

If you use the Windows Control Panel applet **Add/Remove Programs** to remove HPCA, some files and folders (for example, the directory `C:\Program Files\Hewlett-Packard\HPCA` and any files that were added or changed since the initial installation) will be left on the server and will have to be manually removed.

To remove HPCA

1 On the HPCA media, double-click **HPCACore.msi**.

2   Select **Remove the HP Client Automation Core from this computer** and click **Next**.

> If you are removing a Satellite server, the references to "Core" in steps 1 and 2 will be replaced with "Satellite."

3   At the Removal Confirmation message click **Next**.

HPCA is removed from your server.

Repairing HPCA

Use the HPCA installation program to repair HPCA on your server.

To repair HPCA

1   On the HPCA media, double-click **HPCACore.msi**.

2   Select **Repair the HP Client Automation Core files, registry values, and shortcuts on this computer** and click **Next**.

> If you are repairing a Satellite server, the references to "Core" in steps 1 and 2 will be replaced with "Satellite."

3   At the Repair Confirmation message click **Next**.

HPCA is repaired on your server.

Configuring Core Server on Windows 2003

If you have installed the Core on a Windows Server 2003, you must set some switches in the boot.ini file to improve the performance of the Core Server.

The switches that need to be added to the boot.ini file are the following:

- /3GB - It allocates 1 GB to the kernel and 3 GB to the user mode space.

- /userva=2900 - It is used with the /3GB switch for more precise tuning of user and kernel virtual memory space in the Windows Server 2003 family.

- /PAE - It is used on systems with more than 4 GB of RAM. It permits a computer that supports the physical address extension (PAE) mode to start normally.

For more information about setting switches in the boot.ini file, go to **http://support.microsoft.com/kb/316739** and **http://support.microsoft.com/kb/833721** at the Microsoft web site.

Manually Installing the HPCA Administrator

To install the HPCA Administrator on a machine other than that which hosts the Core server, you will need to manually install it. The manual installation can be done by using either of the methods that are described in the sections:

- Installing the HPCA Administrator using the installation program on page 46
- To install the HPCA Administrator using the Software Publisher service (Starter and Standard users) on page 47

Installing the HPCA Administrator using the installation program

1 On the device on which you want to install the HPCA Administrator, open the HPCA media to the Media\admin\default\win32 directory and double-click **setup.exe** (or the .msi file).

   The Welcome window opens.

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 HPCA Core server. The default port 3464 should not be changed.

6 Click **Next**. The License Dialog window opens.

7 Click **Browse** to select the license file for your edition of HPCA.

8 Click **Next**. The Select Features window opens.

9 Select the features to install, and then click **Next**.

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

11 When the installation is complete, click **Finish**.

To install the HPCA Administrator using the Software Publisher service (Starter and Standard users)

1 Manage the target device by deploying the Management Agent.

2 Entitle the Software Publisher service to the device. First add the device to a group and assign entitlement.

3 Deploy the Software Publisher service that is available in the HPCA Software Library.

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

Using HPCA to Manage Windows Operating Systems

HPCA uses two utilities from the Microsoft Windows Automated Installation Kit (AIK) for operating system (OS) management:

- The `bootsec.exe` utility repairs the boot sector of the Windows partition.
- The `imagex.exe` utility is used to capture, modify, and apply file-based disk images for deployment.

If you plan to use HPCA to manage Windows operating systems, you will need to install the Windows AIK on the machine that will host the HPCA Core. Refer to Windows AIK Installation on page 34.

Out of Band Management

If HPCA OOBM is going to be enabled and used, review the following notes.

- If you are uninstalling or upgrading an HPCA server and want to retain the OOBM configuration and data files for later use, you must use the migration scripts for the backup and restore of files.

  For more information on migration and restore, refer to the *HP Client Automation Starter and Standard Editions Migration Guide*.

- In order for vPro devices to work correctly with HPCA OOBM, you must install and configure the Intel™ AMT **Setup and Configuration Service** (**SCS**).

  — The **SCS** is supported on Windows 2003 Server (32-bit) operating systems only, and can be installed on a machine other than that which houses the HPCA components.

  — If the HPCA components are installed on any Windows 2008 Server platform, the **SCS** must be installed on a separate server.

  — If you choose to integrate HPCA OOBM features with Active Directory, the Active Directory domain controller must be installed on Windows 2003 Server (32-bit) operating systems.

  For additional information, refer to the *HP Client Automation Out of Band Management User Guide* and the most recent Intel™ SCS documentation.

Windows Services

After the installation, the HPCA Core service will be listed in the Windows services as `HPCA Core`; its start mode will be set to "Automatic." As this service is an internal part of the HPCA Core, it should not be stopped while the Core is running.

If the HPCA Satellite server is installed, its service, `HPCA Satellite`, will be listed in the Windows services also; its start mode will be set to "Automatic." As this service is an internal part of the HPCA Satellite, it should not be stopped while the Satellite is running.

In addition to the HPCA services, several sub-services are automatically installed with the HPCA server. These are easily identified in Windows services because they are labeled "HPCA." The start mode for these sub-services is "Manual."

HP recommends using only the Console to stop and start these sub-services because of cross-service dependencies. If the HPCA Core or Satellite service is stopped, the sub-services will automatically stop as well.

3 Getting Started

After you have installed and configured HPCA, you are ready to use the web-based HPCA Console (the Console) to manage the client machines in your environment.

This chapter introduces you to the essential tasks that you need to complete to begin to use HPCA to manage your enterprise.

- Accessing the Web-based HPCA Console on page 51
- Quick Start Tasks on page 52

Accessing the Web-based HPCA Console

The HPCA server has a Console through which various administrative and configuration tasks can be performed. For more information on these tasks, see Operations on page 181 and Configuration on page 215.

You can use one of three methods to launch and access the HPCA Console:

- Double-click the **HP Client Automation Console** desktop icon on the machine where the server was installed.
- Navigate the Windows **Start** menu path of the machine on which the HPCA server was installed:

  HP Client Automation > **Client Automation Console**
- Open a Web browser on any device in your environment and go to:

  `http://HPCA_host:3466/`

  where `HPCA_host` is the name of the server on which HPCA is installed.

Each method launches the HPCA Console, which prompts you for log-in credentials.

When prompted, specify your user name and password and click **Sign In**. The default user name is **admin** and the default password is **secret**.

See Configuration on page 215 to learn how to change the default user name and password and how to add users to the Console-access authority list. See SSL on page 227 to learn how to enable SSL in the Console to secure communication.

Important Notes

- The HPCA console may open additional browser instances when you run wizards or display alerts. To access these wizards and alerts, be sure to include HPCA as an Allowed Site in your browser's pop-up blocker settings.

- For security, HPCA automatically logs out the current user after 20 minutes of inactivity; you need to log in again to continue using the Console.

- To view the graphical reports in the **Reporting** section of the Console, you need either Java Runtime or Java Virtual Machine. Java can be installed from **http://java.com/en/index.jsp**.

- **Windows 2003 Server**: To allow local access to HPCA on a device with the Windows 2003 Server operating system, you must enable **Bypass proxy server for local address** in the Local Area Network (LAN) settings.

Quick Start Tasks

This chapter presents a series of tasks that enable you to quickly set up your environment and immediately use HPCA to manage your client devices. Additional administrative, reporting, patch-management, deployment, and operational functions are available, but these initial quick-start tasks are designed to introduce you to the capabilities of HPCA and have you start using it as soon as possible after installation.

The quick-start tasks are listed below. These must be completed in the order in which they are presented.

Task 1: Import Devices on page 54

Import your client devices into the HPCA environment so that they are "known" to the HPCA server.

Deploy and install the HPCA agent to the client devices in order to bring them under the control of HPCA.

Configure schedules for inventory checking and patch management.

Prepare software packages for deployment to your HPCA-managed devices, and automatically download patches according to the patch-acquisition schedule. Software packages and patches are then stored in their respective libraries.

Create groups of target devices to more efficiently deploy software and patches.

By entitling users and devices to software packages, you allow users to choose which software to download, and when. Patches are usually downloaded without user intervention or knowledge.

Generate and view reports that can be printed and distributed. The reports can be customized and based on a variety of information about your HPCA-managed devices.

Figure 1   Quick Start tasks at a glance
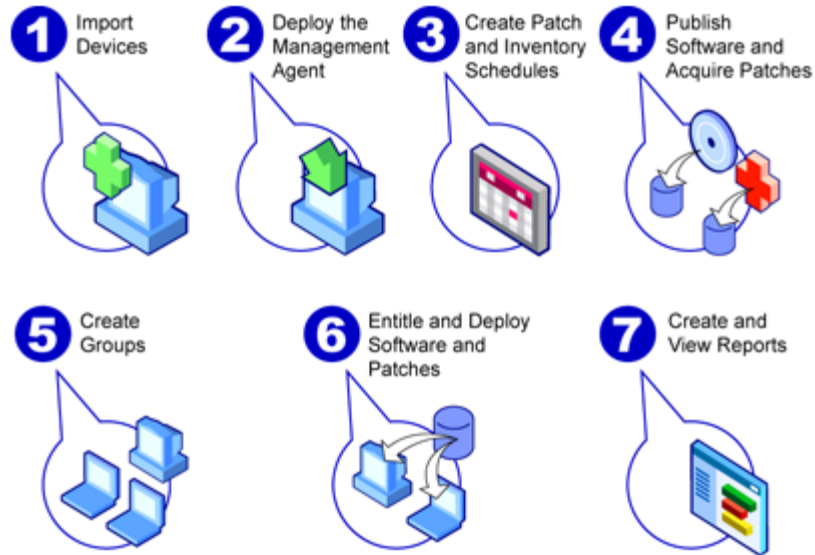
Task 1: Import Devices

You must import (into HPCA) the devices in your environment that you want to have managed by HPCA. Doing so will make HPCA aware of them, and will enable you to collect inventory information and deploy software and patches.

1   On the Management tab, select Device Management then the General tab and click **Import** to launch the Import Device Wizard.

2   Follow the steps in the wizard to import devices.

When devices have been imported, go to Task 2: Deploy the HPCA Agent to manage software, patches, and inventory.

Task 2: Deploy the HPCA Agent

When devices are imported, deploy the HPCA agent.

1   On the Management tab, select Device Management then the General tab and click **Deploy** to launch the Agent Deployment Wizard.

2   Follow the steps in the wizard to deploy the HPCA agent to your imported devices.

▶   **Windows Vista Note**

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 HPCA agent deployment though the HPCA console.

If the devices are not part of a domain, additional steps (detailed in the Microsoft Knowledge Base article, *Error message when you try to access an administrative share on a Windows Vista-based computer*) are required in order to allow access for local administrators.

After making these changes, reboot the device.

Now that you have begun to manage devices, go to Task 3: 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 tab.

To configure the inventory schedule

1   On the Devices tab in the Device Management area, select one or more devices by clicking the check box to the left of a device.

2   Click **Inventory Collections** and then select **Discover Software/Hardware Inventory** to launch the Software/Hardware Inventory Wizard.

3   Follow the steps in Software/Hardware Inventory Wizard on page 283 to define software and hardware inventory collection for your devices and groups.

To configure patch acquisition schedule and settings

Use the Operations tab, Patch Management section to configure patch acquisition settings and schedule.

1   Expand the Patch Management section and click **Acquisition**.

2   Use the Schedule tab to specify a schedule for patch acquisitions.

3   In the Settings tab, specify the required Microsoft Bulletin and HP Softpaq acquisition settings.

> ► Patch Management using Metadata is enabled by default for Microsoft patches. This feature reduces the time it takes to acquire patches and the overall load on the Core Configuration Server. For details, see Chapter 11, Patch Management Using Metadata.

To configure a patch compliance discovery schedule

1   On the Devices tab in the Device Management area, select one or more devices by clicking the checkbox to the left of the device.

2   Click **Inventory Collections** and then select **Discover Patch Compliance** to launch the Patch Compliance Discovery Wizard.

3   Follow the steps in the wizard to create a patch compliance schedule for your devices and groups.

When schedules are configured, go to Task 4: 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.

1   Use the Publisher to publish software into the HPCA database.

— Launch the Publisher on the machine from which you plan to configure and publish software services. Refer to the Publisher online help or Publishing on page 347 for more information.

> ► The Starter license contains options for publishing HP Softpaqs, BIOS settings, and, for thin clients only, options for publishing software and OS images.
>
> The Standard license contains these options as well as options for publishing software and operating system images.

2   Populate the Patch Library by acquiring patches from HP and Microsoft
    sources.

—   On the Management tab, Patch Management section, General tab,
    click **Acquire**. Patches are downloaded and added to the Patch Library.
    Patches are automatically downloaded according to the acquisition
    schedule configured in the previous step, .

> Patches should be acquired initially to an HPCA server in a
> non-production lab environment for evaluation to prevent
> possible performance issues.

When software and patches are available in each library, go to 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.

•   On the General tab of the Group Management area, click **Create a New
    Static Group**. This will launch the Group Creation Wizard. Follow the steps
    in the wizard to create a static group.

    HPCA also supports dynamic device groups that are based, optionally, on
    discovered devices (discovery group) or selected inventory criteria
    (reporting groups). These groups are also created using the Group
    Creation Wizard. See for more
    information.

When the group has been created, go to to the devices in the group.

Task 6: Entitle and Deploy Software or Patches

In the Group Management area, Groups tab, click the Group display name to open the Group Details window. Here, you can entitle and deploy software and 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 and deploy software.

1   Click **Add Software Entitlement** to select software services and make them available to that group. Entitled software is displayed in the Software Entitlement table on the Software tab 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 that allows users to determine which optional software services to deploy and when.

2   To deploy software, select the software to deploy and click the **Deploy Software** button. This opens the Software Deployment Wizard. Follow the steps in the wizard 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.

1   Click **Add Patch Entitlement** to select patches and make them available to that group. Entitled patches are then displayed in the Patch Entitlement table.

2   To deploy patches, select the patches to deploy and click **Deploy Patches** . This opens the Patch Deployment Wizard. Follow the steps in the wizard 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 successfully used HPCA to deploy software and patches. Learn about creating reports by following the instructions in the section, Task 7: Generate and View Reports.

Task 7: Generate and View Reports

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

*   To generate a quick sample report, click **View Managed Devices** in the **Inventory Information** area to display a list of all devices that have the HPCA 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 **Create a new Dynamic Reporting Group** to create a dynamic group of devices in the report. This will open the Group Creation Wizard. Follow the steps in the wizard to create the Reporting Group.

4 Using the Dashboards

The Dashboards enable you to quickly assess the status of your environment in various ways. The Dashboards offer a visual representation of certain types of information provided in the Reporting area. The specific dashboards available to you depend on the type of HPCA license that you have. This chapter includes the following topics:

- Dashboard Overview on page 62
- HPCA Operations Dashboard on page 66
- Patch Management Dashboard on page 73

Dashboard Overview

The HPCA Console includes dashboards that enable you to view and assess the status of your enterprise at a glance:

- The HPCA Operations Dashboard on page 66 shows you how much work is being done by the HPCA infrastructure.

- The Patch Management Dashboard on page 73 shows you information about any patch vulnerabilities that are detected on the devices in your network

Each dashboard includes two views:

Table 3   Types of Dashboard Views

Type	Description
Executive View	High-level summaries designed for managers. This include historical information about the enterprise.
Operational View	Detailed information designed for people who use HPCA in their day to day activities. This includes information about specific devices, subnets, vulnerabilities, and specific compliance or security tool issues.

Each view includes a number of information panes. You can configure HPCA to show you all or a subset of these panes. See Dashboards on page 275 for more information.

Each dashboard also includes a home page with summary statistics and links to related reports. When you click one of these links, a separate browser window opens, and HPCA displays the report.

In most dashboard panes, you can display the information in either a chart or grid format. In the grid view, the current sort parameter is indicated by the ▼ icon in the column heading. To change the sort parameter, click a different column heading. To reverse the sort order, click the column heading again. To move a column, click the background in the column heading cell, and drag the column to a new location.

In most dashboard panes, you can rest the cursor on a colored area on a bar or pie chart—or a data point on a line chart—to see additional information. Most panes also enable you to drill down into reports that provide more detailed information.

The time stamp in the lower left corner of each pane indicates when the data in the pane was most recently refreshed from its source.

Figure 2   Time Stamp
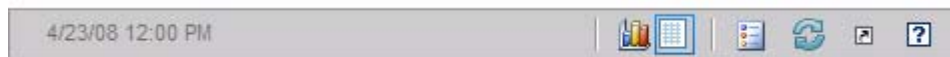
▶ The dashboard panes use your local time zone to display the date and time. The reports available on the Reporting tab use Greenwich Mean Time (GMT) by default. Individual report packs, however, can be configured to use either GMT or local time.

You can perform the following actions in the dashboard panes:

Table 4   Dashboard Pane Actions

Icon	Description
	Display the information in chart format.
	Display the information in grid format.
	Display the legend for this chart.
	Refreshes the data from its source. Click the refresh icon in an individual pane to refresh the data for that pane. Click the refresh icon in the upper right corner of the dashboard to refresh all panes. The dashboard panes are not automatically refreshed if your HPCA Console session times out. You must manually refresh the panes after you sign in again if you want to get the latest information from the database.
	Resets the appearance of all panes within the dashboard to their factory default settings.

Table 4   Dashboard Pane Actions

Icon	Description
↗	For panes containing HPCA data, show the corresponding report. For panes containing information from external web sites or RSS feeds, go to the source web site.
?	Opens a "quick help" box or tool tip. Click this button once to see a brief description of the dashboard pane. Click it again to hide the quick help text.
?	Opens a context sensitive online help topic for this pane. This control is only available when the quick help text is visible.
▭	Minimize a dashboard pane.
▭	Maximize a dashboard pane.
▱	After maximizing, restore the pane to its original size.

If you minimize a dashboard pane, the other panes will expand in size to fill the dashboard window. Likewise, if you maximize a dashboard pane, the other panes will be covered. To restore a pane that has been minimized, click the gray button containing its name at the bottom of the dashboard. In this example, the 24 Hour Service Events pane has been minimized:

Figure 3   Button that Restores a Dashboard Pane

24 Hour Service Events

You can drag and drop the panes to rearrange them within the dashboard window. You cannot, however, drag a pane outside of the dashboard.

When you customize the appearance of a dashboard by resizing or rearranging its panes—or switching between the chart and grid view in one or more panes—this customization is applied the next time you sign in to the HPCA Console. The dashboard layout settings are stored as a local Flash shared

object (like a browser cookie) on your computer. The settings are saved unless you explicitly delete them. See Delete Dashboard Layout Settings on page 436 for instructions.

> If you press the **F5** function key while viewing one of the dashboards, you will return to that dashboard page after your browser reloads the HPCA Console.

Dashboard Perspectives

Perspectives enable you to limit the information displayed in the dashboard panes to certain types of devices. The following three perspectives are available by default:

- Global – All devices (no filter is applied).
- Mobile – Laptops and other mobile computing devices. This includes all devices with the following chassis types:
  — Portable
  — Laptop
  — Notebook
  — Hand Held
  — Sub Notebook
- Virtual – Virtual devices. This includes all devices whose Vendor and Model properties indicate VMware or Xen (including Citrix).

To apply a perspective, select it in the Perspectives box in the upper left corner of the console:

Due to the nature of the data that they display, certain dashboard panes are not affected by the perspectives. When you select either the Mobile or Virtual perspective, a highlighted message appears at the top of any pane that is *not* affected:

Filter or Perspective Not Applicable

Panes that are not affected are also outlined in orange.

When you select a perspective, it is applied to all the dashboard panes in the HPCA Console except those that indicate, **Filter or Perspective Not Applicable**, as shown above. You cannot apply a perspective to an individual dashboard pane.

HPCA Operations Dashboard

This dashboard shows you the work that the HPCA infrastructure is doing in your enterprise. It shows you three things:

- The number of HPCA client connections
- The number of service events (installs, uninstalls, updates, repairs, and verifies) that have occurred
- The types of operations (OS, security, patch or application) that HPCA has performed

The client connection and service event metrics are reported in two time frames. The Executive View shows the last 12 months. The Operational View shows the last 24 hours. Both views contain the following information panes:

Client Connections on page 67

Service Events on page 69

The Executive View also includes the following pane:

12 Month Service Events by Domain on page 71

All of these panes are visible by default. You can configure the dashboard to show or hide any of these panes. For more information, see Dashboards on page 275.

▶ When you click HPCA Operations in the left navigation pane, the HPCA Operations home page is displayed. This page contains statistics and links to pertinent reports.

Client Connections

The chart view of this pane shows you the number of HPCA agent client connections that have occurred over the last twelve months (Executive View) or 24 hours (Operational View). When you rest the cursor on a data point, you can see the total number of connections for that month (Executive View) or hour (Operational View).

Figure 4   12 Month Client Connections
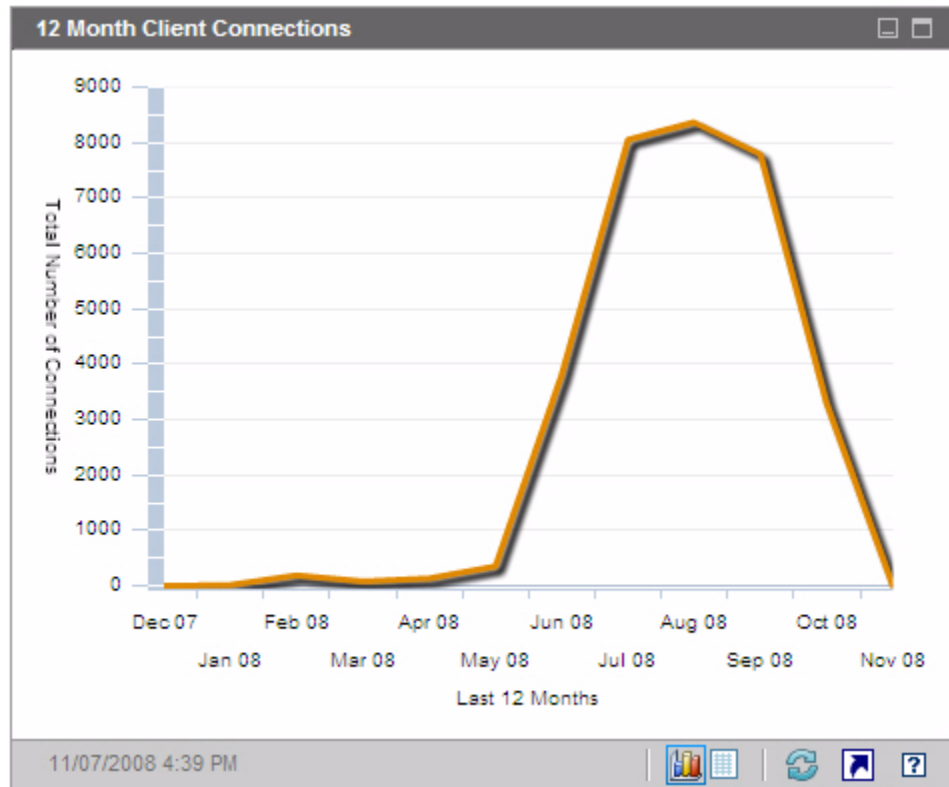
The grid view for this pane lists the total number of client connections completed during each of the last twelve months.

Figure 5   24 Hour Client Connections
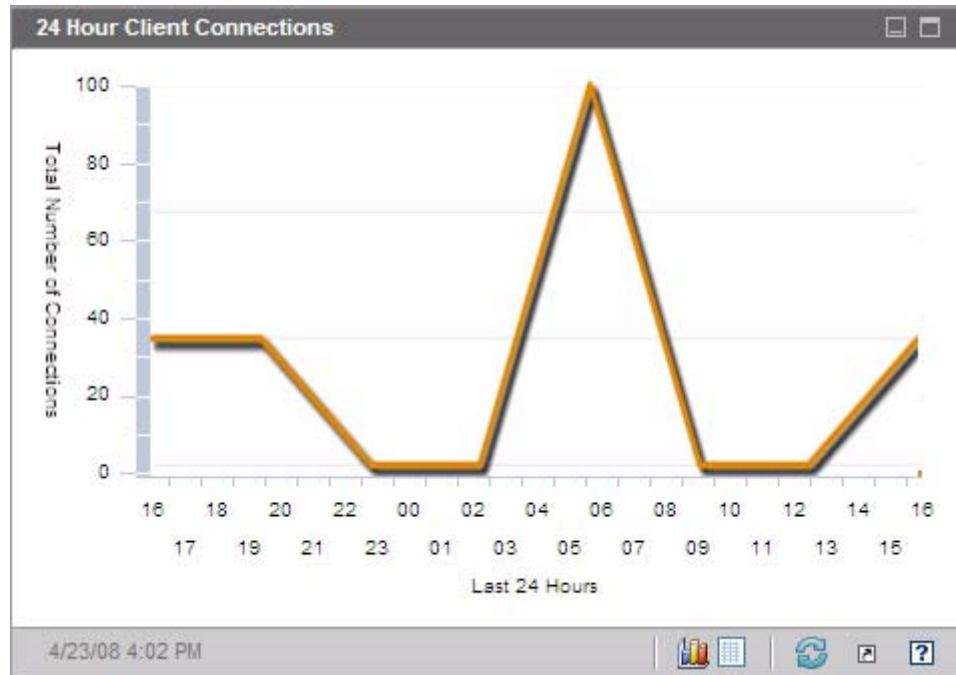
▶ The dashboard panes use your local time zone to display the date and time. The reports available on the Reporting tab use Greenwich Mean Time (GMT) by default. Individual report packs, however, can be configured to use either GMT or local time.

The grid view for this pane lists the number of client connections completed during each of the last 24 hours.

Service Events

The chart view of this pane shows the number of service events that HPCA has completed over the last twelve months (Executive View) or 24 hours (Operational View) on the client devices in your enterprise. These include the number of applications that HPCA has:

• Installed

• Uninstalled

- Updated
- Repaired
- Verified

When you rest the cursor on a data point, you can see the number of service events that were completed during a particular month or hour.

Figure 6   12 Month Service Events
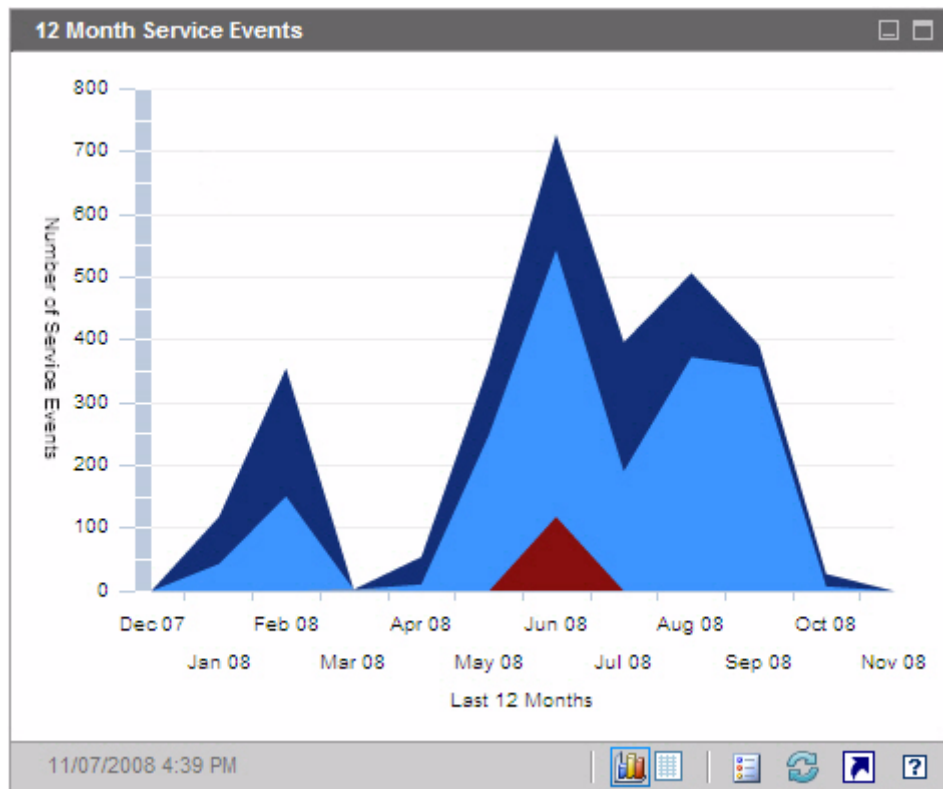
The grid view for this pane lists the number of each type of service event that was completed by HPCA during each of the last twelve months.

Figure 7   24 Hour Service Events
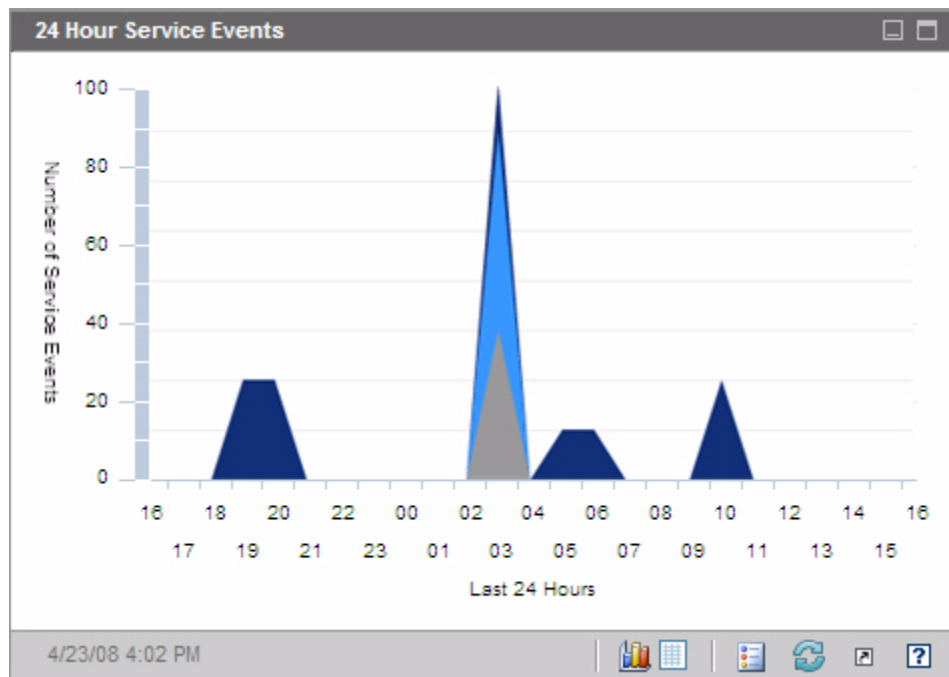
▶ The dashboard panes use your local time zone to display the date and time. The reports available on the Reporting tab use Greenwich Mean Time (GMT) by default. Individual report packs, however, can be configured to use either GMT or local time.

The grid view for this pane lists the number of each type of service event that was initiated by HPCA during each of the last 24 hours.

12 Month Service Events by Domain

The chart view of this pane shows you how many of each of the following services that HPCA performed during each of the last 12 months:

- Operating system (OS) operations
- Security operations
- Patch operations

- Application operations

If fewer than 12 months of data are available, the chart will contain fewer bars.

Figure 8   12 Month Service Events by Domain
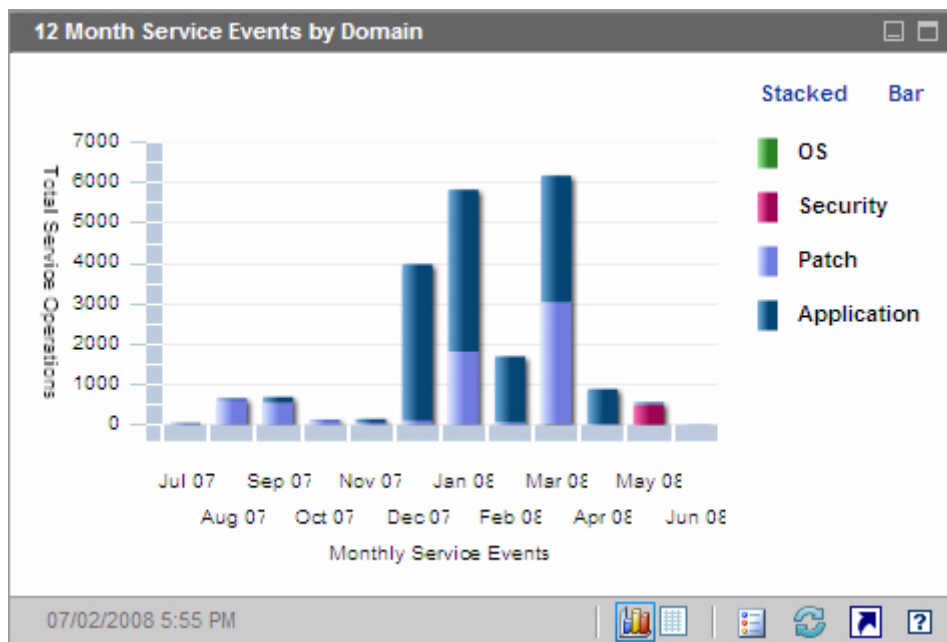
You can view the data presented in this chart in two ways.

- Stacked – the different types of service events are stacked vertically in a single bar for each month, as shown here.

- Bar – a separate bar for each type of service event is shown for each month.

The grid view lists the number of each type of service that HPCA performed during each of the last twelve months.

Patch Management Dashboard

The Patch Management dashboard provides information about any patch vulnerabilities that are detected on managed devices in your network.

The Executive View of the Patch Management dashboard includes three information panes:

The Operational View includes the following information panes:

You can configure the dashboard to show or hide any of these panes. See Dashboards on page 275.

▶ When you click Patch Management in the left navigation pane on the Home tab, the Patch Management home page is displayed. This page contains statistics and links to pertinent reports.

Device Compliance by Status (Executive View)

The chart view of this pane shows you the percentage of devices in your network that are currently in compliance with your patch policy. The colored wedges in the pie chart represent the following possible states:

- Patched (green)
- Not patched (red)

The Device Compliance by Status (Operational View) on page 79 is similar but has finer-grained detail:

Table 5   Device Compliance By Status Views

Executive View	Operational View
Patched	Patched Warning
Not patched	Not patched Reboot Pending Other

Figure 9   Device Compliance by Status (Executive View)
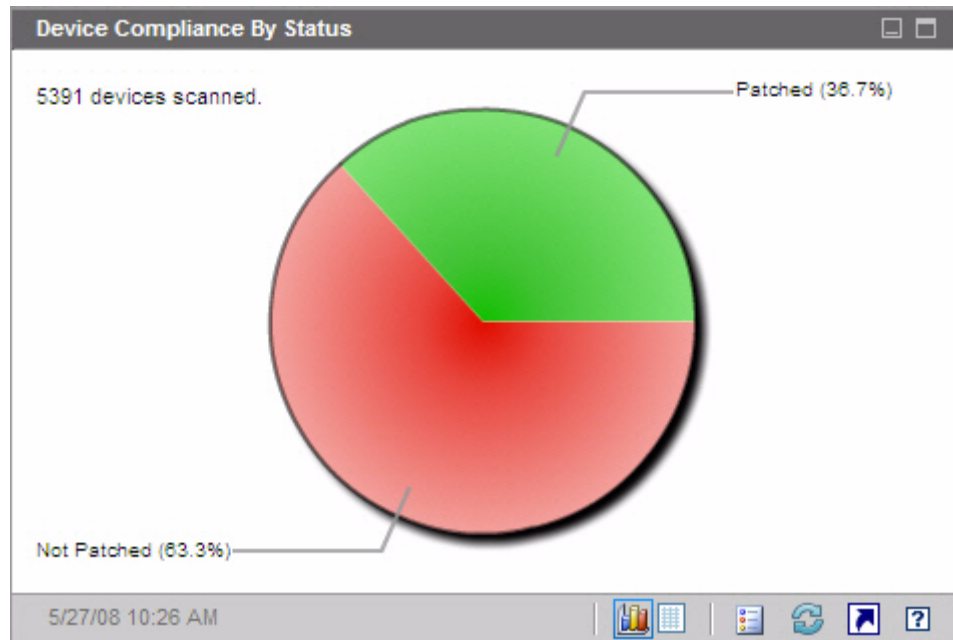
To see the number of devices in a particular category, rest the cursor over a colored sector in the pie chart.

If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.

The grid view for this pane shows the number of network devices in each of the compliance states shown in the pie chart.

Device Compliance by Bulletin

The chart view of this pane shows you the ten patch vulnerabilities that affect the greatest number of devices in your network. The vertical axis lists the patch bulletin numbers for these vulnerabilities. The horizontal axis represents the number of devices not patched and uses a logarithmic scale.

▶ If a particular bulletin affects only one device, no data is shown for that bulletin in the chart view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

To see the name of the bulletin and the number of devices affected, rest the cursor on one of the colored bars.

Figure 10 Device Compliance by Bulletin
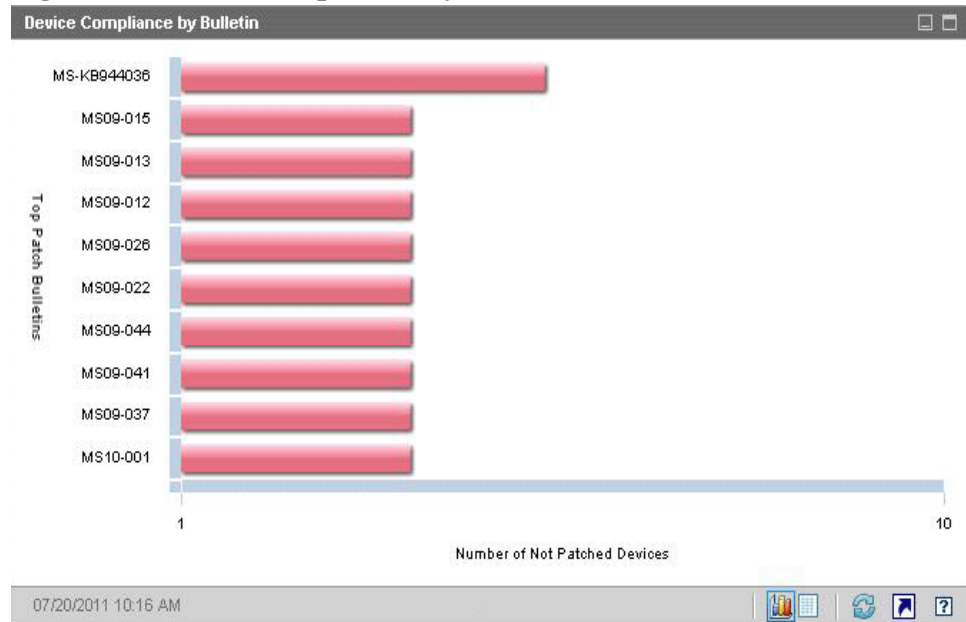
If you click one of the colored bars in the chart, a new browser window opens, and a filtered report is displayed. This report shows which managed devices have this patch vulnerability.

The grid view provides the following information for the top ten patch vulnerabilities detected:

- Bulletin – The Microsoft Security Bulletin identifier for this vulnerability
- Description – Title of the bulletin
- Not Patched – Number of devices with this patch vulnerability

The table is initially sorted by Not Patched. To change the sort parameter, click the pertinent column heading.

To find more information about a particular bulletin, click the bulletin number.

Top Ten Vulnerabilities

The chart view of this pane shows the compliance state of the top ten vulnerabilities that affect the maximum number of devices in the network. The chart displays the number of devices that have been patched or not for each of the vulnerability. These devices are represented as follows:

- Patched devices (green)
- Non-patched devices (red)

You can view the statistics of these devices for last 7 days, 14 days, 21 days, 30 days, and greater than 30 days. You can also filter the vulnerabilities by **Recently Released** to view statistics for top ten bulletins released by Microsoft and acquired by Patch Manager that affect the maximum number of devices in the network.

The vertical axis of the chart lists the top ten patch bulletins. The horizontal axis represents the number of devices affected by these bulletins.

To see the number of devices affected and the compliance state of a particular bulletin, position the cursor on one of the colored bars.

Figure 11 Top Ten Vulnerabilities
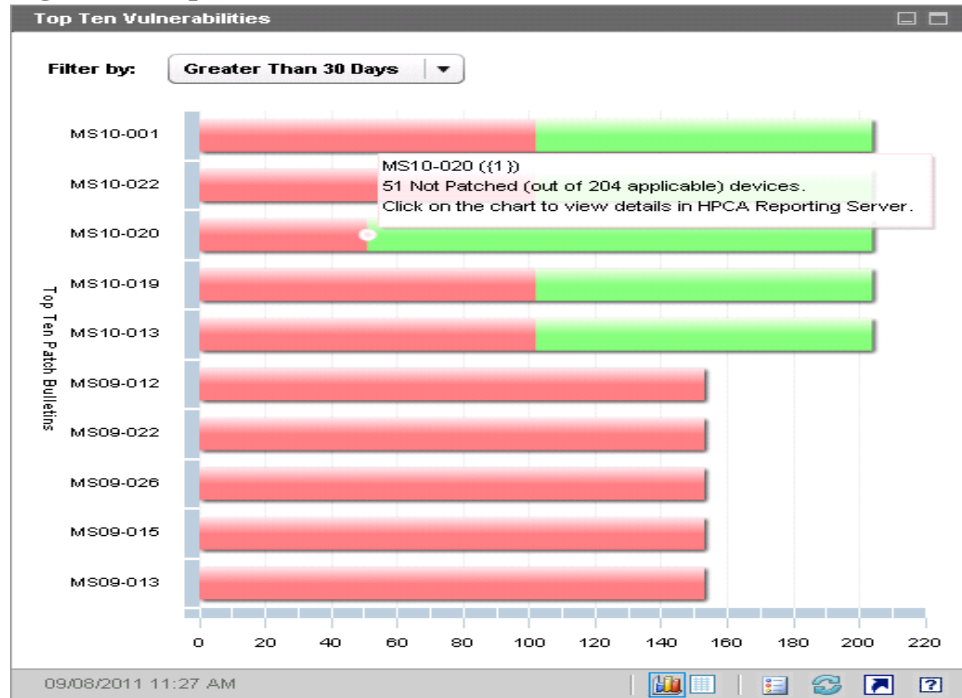
The grid view provides the following information for the top ten vulnerabilities:

- Bulletin – The Microsoft Security Bulletin identifier

- Not Patched – Number of devices not compliant with a particular bulletin

- Patched – Number of devices compliant with a particular bulletin

- Devices – Total number of devices affected due to a particular bulletin

The table is initially sorted by **Devices**. To change the sort parameter, click the pertinent column heading.

To find more information about a particular bulletin, click the bulletin name.

HP Live Network Patch Manager Announcements

This pane contains the most recently published HP Live Network Patch Manager announcements. This information is provided by an RSS feed from the HP Live Network subscription site. Refer to Chapter 5, HPCA and HP Live Network. By default, this pane is not enabled, because it requires HP Live Network credentials to be specified before it can display information. See Dashboards on page 275 for information about configuring your HP Live Network credentials.

Figure 12 HP Live Network Patch Manager Announcements
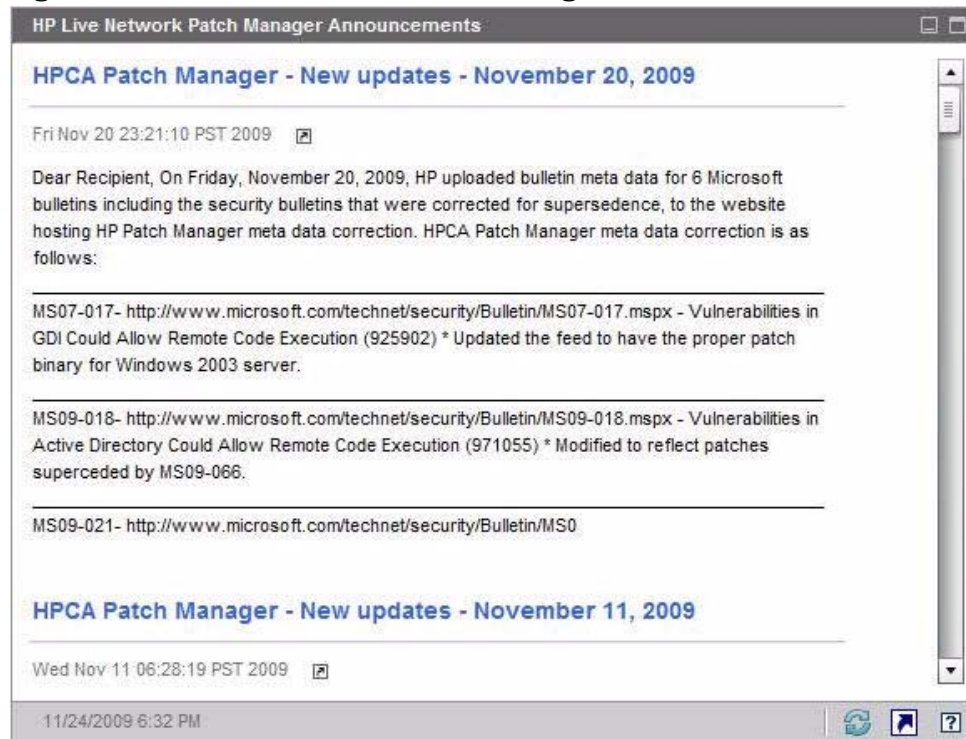
To find more information about a particular announcement, click the ⊡ icon just below its title. The HP Live Network subscription support site opens in a new browser window. You must have an active HP Live Network subscription to access this site.

This pane does not have a chart view.

When you enable this pane on the Configuration tab, you can change the URL for the RSS feed, as well as the location of the HP Live Network authentication server (see Dashboards on page 275). You may also need to enable a proxy server (see Configure the Connection to the HP Live Network Server on page 249 and Proxy Settings on page 226).

Device Compliance by Status (Operational View)

The chart view of this pane shows you the percentage of devices in your network that are currently in compliance with your patch policy. To see the number of devices in a particular category, rest the cursor over a colored sector in the pie chart.

This pane is similar to the Device Compliance by Status (Executive View) pane but shows a finer level of detail and uses the same colors used by the Patch Manager:

- Patched (light green)
- Not Patched (red)
- Reboot Pending (light gray)
- Warning (dark green)
- Other (yellow)
- Not Applicable (dark gray)

Figure 13 Device Compliance by Status (Operational View)
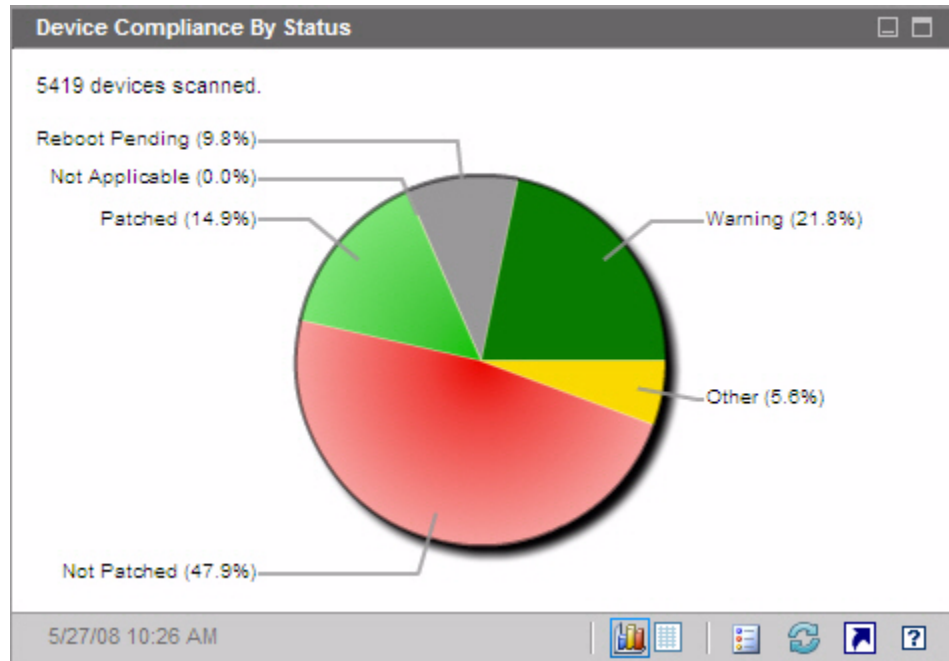
If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.

The grid view shows the number of network devices in each of the compliance states shown in the pie chart.

Microsoft Security Bulletins

This pane shows you the most recent Microsoft Security Bulletins. By default, this information is provided by an RSS feed from Microsoft Corporation. You can change the URL for the feed by using the Configuration tab (see Dashboards on page 275).

Figure 14 Microsoft Security Bulletins
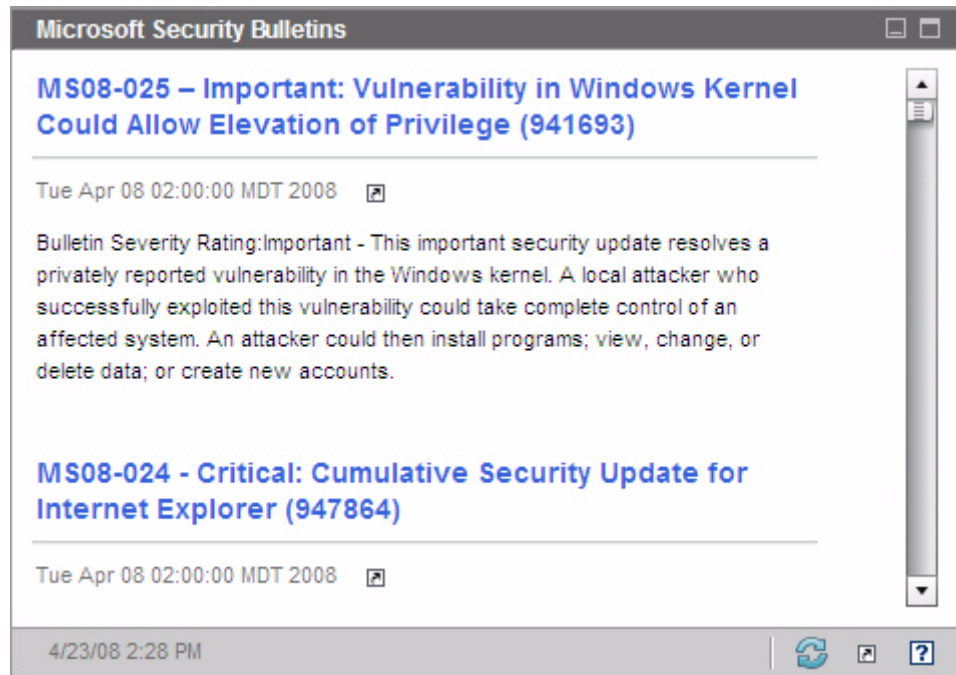
To view detailed information about a particular bulletin, click the ⊡ icon just below the bulletin name.

This pane does not have a chart view.

Most Vulnerable Products

This pane is disabled by default. To enable it, see Dashboards on page 275.

The chart view of this pane shows you the software products in your network for which there are the greatest number of not patched devices. The vertical axis lists the software products. The horizontal axis reflects the total number of not patched devices for the software product.

Because this chart uses a logarithmic scale, if the number of not patched devices for a particular product equals one, no data is shown for that product in the chart view. This is a known limitation of logarithmic scales. However,

the data is visible in the grid view. To see the number of devices on which a particular software product is not patched, rest the cursor over one of the colored bars.

Figure 15 Most Vulnerable Products
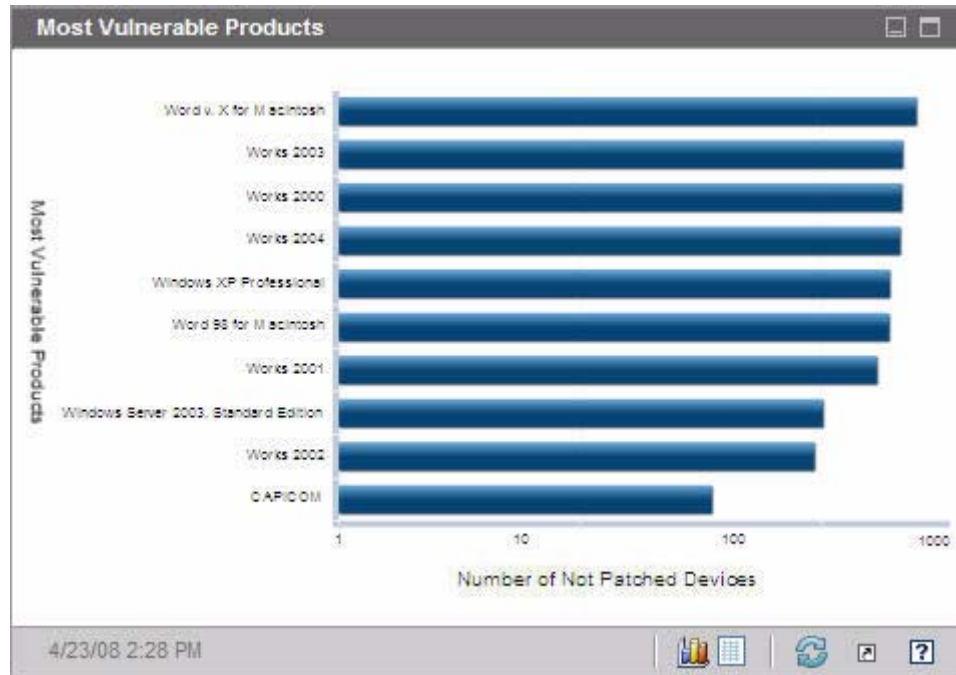
The grid view provides the following information for each product:

- Product – Name of the software product
- Not Patched – Number of not patched devices for a particular product
- Applicable Devices – Number of devices on which this product is installed

The table is initially sorted by Not Patched. To change the sort parameter, click the pertinent column heading.

5 HPCA and HP Live Network

Overview

HP Live Network is a subscription service that enables you to obtain the most current content for HPCA. The type of content available from HP Live Network varies depending on your HPCA license.

For HPCA Standard, it provides the latest content for settings profiles. Report enhancements can also be delivered over Live Network. When available, you can obtain these enhancements by performing an HP Live Network update. Any customizations that you have made to your reports will not be overwritten when you download the latest reports from the Live Network site.

To obtain updated content, you must have an active HP Software Support contract with valid Live Network Subscription credentials for this content. You will then receive a user ID, password, and content server URL that you can use to configure the Live Network settings on the Configuration tab.

➤ The HP Live Network content server URL that you receive with your subscription may be different than the default URL shown on the Live Network settings page on the Configuration tab in the HPCA Console. Be sure to use the URL that comes with your subscription. For more information, see Live Network on page 249 for details.

You *must* use current HP Passport credentials for HP Live Network Announcements to see the HP Live Network Announcements dashboard pane. To update the HP Passport credentials for HP Live Network Announcements, do the following:

1 Visit HP BSA Essentials Network web site at **https://www.www2.hp.com/** and complete the one time confirmation step before using the HP Live Network announcements widget.

2   If you continue to see a connection failure for the HP Live Network
     Announcements widget:

   a   Visit the HP Live Network RSS Feed at: **https://
       h20033.www2.hp.com/servlets/
       WebFeed?artifact=news&version=rss_2.0&cookieCheck=off**.

   b   Complete the one-time confirmation step if you are asked for it.

License Requirements

To obtain the latest content from HP Live Network, you will need the
following:

- License for HPCA Standard Edition

- Active HP Software Support contract with valid Live Network
  Subscription credentials

If you do not have these items, the pertinent dashboards will be empty, and
the applicable content will be unavailable for download and use.

Updating HP Live Network Content

When HPCA updates your content from the HP Live Network site (or from the
file system), it uses a tool called the HP Live Network Connector (LNC).

To obtain Live Network content, you must use the HP Live Network
Connector and know How to Update HP Live Network Content.

HP Live Network Connector

The HP Live Network Connector is a tool used by HPCA to create a secure
connection to the HP Live Network content distribution server and download
the updated content. When accessing the HP Live Network content, the HP
Live Network Connector first determines what content is available and then
downloads the appropriate content from the HP Live Network subscription
site.

A default version of the HP Live Network Connector is installed and configured when HPCA is installed. It is self-updating. Any changes to the connector are automatically downloaded when you update your HP Live Network content. In certain circumstances, you may want to install a new copy of the LNC. If you want to re-install the HP Live Network Connector for any reason, you can download a new copy at any time. For more information, see

➤ The HP Live Network Connector performs authentication to HP Live Network and downloads content. By itself, the Connector does not install anything into the HPCA infrastructure. HPCA manages the loading of the updated HP Live Network content.

When you update your HPCA content – either from HP Live Network or from the file system – the following actions typically happen:

1 The content is copied into a temporary directory.

2 The content is loaded into the HPCA database. This primes the database for processing collected data, enables HPCA to deploy the pertinent services, and drives the detailed reports.

3 The HPCA console is updated with relevant UI content.

Download the HP Live Network Connector

The HP Live Network Connector (LNC) is provided with HPCA and is installed automatically when you configure the Live Network settings for the first time. The LNC is self-updating. Whenever you update your HP Live Network content, the LNC checks for and installs any available LNC updates. This way, you are always guaranteed to have the most recent version of the LNC after each Live Network update.

If you need to re-install the LNC for any reason—for example, if someone inadvertently uninstalls it—follow these steps.

To download a new copy of the HP Live Network Connector:

1 On the Configuration tab, expand the Infrastructure Management area, and click **Live Network**.

2   Click the **Download** link to the right of the HP Live Network Connector
     box. The HP Live Network subscription support site opens in a new
     browser window. You can download the LNC executable from this site.
     You will need your HP Live Network subscription user name and
     password to log in.

3   Follow the instructions on the HP Live Network site to download and
     install the LNC.

➤   If you install the LNC in a location other than the original installation
     location, be sure to update the **HP Live Network Connector** path on the Live
     Network configuration page accordingly.

How to Update HP Live Network Content

To update your HP Live Network content from the HP Live Network
subscription web site, do the following:

• Use the Schedule Updates tab on the HP Live Network operations page to
  configure the HPCA Console to periodically download updated content, or
  use the Update Now tab to initiate an immediate update from the HP Live
  Network subscription site.

  See Live Network on page 183 for detailed instructions.

You should always update your HP Live Network content after you install or
upgrade your HPCA software to ensure that you have the most recent content
available.

➤   When you download new HP Live Network content, you may simply get
     updates to existing services, or you may be able to access brand new services.
     To use any new services, be sure to explicitly entitle your client devices to
     these services.

➤   The display names of the services downloaded from HP Live Network have
     angle brackets (< >) surrounding them, uniquely identifying these as
     HP-supported services from the Live Network site. Be aware that if you
     modify the services in your environment, your changes may be lost the next
     time that you update your HP Live Network content.

6 Management

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

- Device Management on page 88
- Group Management on page 114
- Software Management on page 128
- Settings Management on page 136
- Patch Management on page 140
- OS Management on page 149
- Job Management on page 161

Device Management

Use the Device Management section to import devices, deploy the HPCA 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:

Information about target device requirements and manual installation steps are included in these sections:

Target Device Prerequisites

Before you deploy the HPCA Agent to target devices, review the information in this section. For information about supported platforms of target devices, refer to the *Release Notes* document that accompanies this release.

- **File and Print Sharing** should be enabled.
- Devices that are running Windows XP Professional and which are not part of an Active Directory must have **Simple File Sharing** disabled.
- TPM-enabled systems require Infineon Driver, version 2.00 (minimum).
- If the target client device has a personal firewall installed then the following ports must be excluded for inbound traffic:

  TCP 3463 and TCP 3465

- 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 *<InstallDir>*\Agent:

  RadUIShell.exe

  Radexecd.exe

  nvdkit.exe

  nvdtk.exe

- And in *<InstallDir>*\ManagementAgent:

  nvdkit.exe

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

Windows XPE Requirements for HPCA

When Windows XPe thin client devices are shipped on non-HP hardware, two rules must be created to allow HPCA to operate—one for the HPCA executables and one for the ports.

To create the HPCA executables rule

If you are running File-Based Write Filter, you must disable the write filter and reboot prior to this procedure. To do this, run the following command:

fbwfmgr.exe /disable

1 Log on to Windows XPe as **Administrator**.

2 Right-click the Symantec icon in the system tray and select **Advanced Rules**.

3 Click **Add**.

4 On the General tab:

   — Add description **Allow HPCA Agent**.

   — Select **Allow this traffic**.

5   On the Applications tab, click **Browse** to add the following applications
    from `<InstallDir>\Agent`.

    —   `Nvdkit`

    —   `Radconct`

    —   `Radpinit`

    —   `Radexecd`

    —   `Radstgrq`

    —   `Radsched`

    —   `Radgetproxy`

    —   `Radntfyc`

    —   `Radidgrp`

    —   `Ralf`

    —   `prepwiz.exe`

    ▶   The `prepwiz` executable is available only from the HPCA Image
        Capture CD, which is created from the Image Capture ISO on the
        HPCA media. This .iso must be available in order to add the
        executable.

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

7   Click **OK** to exit.

To create the HPCA ports rule

1   Right-click the Symantec icon in the system tray and select **Advanced
    Rules**.

2   Click **Add**.

3   On the General tab:

    —   Add description **Allow HPCA Ports**.

    —   Select **Allow this traffic**.

4   On the Ports and Protocols tab, select **Protocol**: **TCP** and add Local: 3463
    and 3465.

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

6 Click **OK** to exit.

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

If you are using the File-Based Write Filter, you must enable the write filter and reboot. To do this, run the following command:

```
fbwfmgr.exe /enable
```

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

General

Use the General tab to add devices, deploy HPCA agents, view current and past Device Management jobs.

➤ An alternative to deploying the HPCA agent from the Console is to manually install it on the end-user machine that you want to manage. For more information, see Manually Installing the HPCA Agent on page 106.

The Summary section of the workspace shows the number of devices in your database, the number of managed devices (devices that have an HPCA 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 280 to add new devices to HPCA.

To deploy the HPCA agent

• In the Common Tasks area, click **Deploy**. This will launch the Agent Deployment Wizard.

    Follow the steps in the wizard on page 282 to deploy the HPCA agent to devices in your database.

- The HPCA agent is deployed to Windows Vista and Windows Server 2008 devices in *silent mode* only.

- To deploy the HPCA 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, you must turn off SFS to allow installation of the HPCA agent. For details on how to configure SFS, see the Microsoft Knowledge Base article *How to configure file sharing in Windows XP*.

Devices

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

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

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

➤ Not all device information is available in the Devices list until an HPCA agent is deployed.

Use the Devices toolbar to import devices, deploy or remove the HPCA agent, mange device power options, control devices remotely, and discover inventory, application usage or patch compliance.

➤ An alternative to deploying the HPCA agent from the Console is to manually install it on the end-user machine that you want to manage. For more information, see Manually Installing the HPCA Agent on page 106.

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 HPCA to deploy the HPCA 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, **Microsoft NetBIOS Computer Naming Conventions**.

Use the **Search** function to narrow the list of devices. The first search box will always contain the available column headings 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 6   Devices toolbar tasks

Button	Description
	Refresh Data – Refreshes the Device list.
	Export to CSV – Creates a comma-separated list that you can open or save.
	Import Devices to Manage – Launches the Import Device Wizard.
	Deploy the Management Agent – Launches the Agent Deployment Wizard.
	Remove the Management Agent – Launches the Agent Removal Wizard.

Table 6   Devices toolbar tasks

Button	Description
	Inventory Collections:
	Discover Software/Hardware Inventory – Launches the Software/ Hardware Inventory Wizard.
	Discover Patch Compliance – Launches the Patch Compliance Discovery Wizard.
	Discover Application Usage – Launches the Application Usage Collection Wizard.
	Power Management – Launches the Power Management Wizard.
	Remote Control – Launches the Remote Control interface window.
	View Out of Band Device Details – Launches the Out of Band Device details window for the selected device. This option is available only when Out of Band Management is enabled. See Out of Band Management on page 263 for enablement information. For more detailed information, refer to the *HP Client Automation Out of Band Management User Guide.*
	Delete Devices – 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 Database Maintenance on page 186 for details.

The following tasks are available from the Devices tab.

- Importing Devices on page 95
- Deploying the HPCA Agent from the Devices Tab on page 95
- Removing the HPCA Agent on page 96
- Discovering Software/Hardware Inventory on page 96
- Discovering Patch Compliance on page 97
- Discovering Application Usage on page 97

- Remote Control on page 98
- Power Management on page 102
- Out of Band Management on page 102
- Removing Devices on page 103
- Device Details on page 104

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 devices into HPCA, click **Import Devices to Manage** 🔲 button. This will launch the Import Device Wizard.

    Follow the steps on page 280 to add new devices to HPCA.

Deploying the HPCA Agent from the Devices Tab

Use the Agent Deployment Wizard to deploy the HPCA agent to devices in your environment.

➤ Deploying the HPCA 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 HPCA agent deployment though the HPCA Console. If the devices are not part of a domain, you must perform additional steps to allow access for local administrators. See the Microsoft Knowledge Base article, *Error message when you try to access an administrative share on a Windows Vista-based computer*.

To deploy the HPCA agent

1 Use the check boxes in the first column to select the devices to which you want to deploy the HPCA agent.

— Click the **Deploy the Management Agent** button to launch the Agent Deployment Wizard.

2   Follow the steps in the wizard on page 282 to deploy the HPCA agent to the selected devices.

Removing the HPCA Agent

Use the Agent Removal Wizard to remove the HPCA agent from devices in your HPCA database.

To remove the HPCA agent

1   Use the check boxes in the first column to select the devices from which you want to remove the HPCA agent.

2   Click the **Remove the Management Agent** button to launch the Agent Removal Wizard.

3   Follow the steps on page 283 to remove the HPCA agent from the selected devices.

Discovering Software/Hardware Inventory

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

To discover software and hardware inventory

1   Use the check boxes in the first column to select the devices for which you want to discover inventory.

2   Click the **Inventory Collections** button and select **Discover Software/Hardware Inventory** to launch the Software/Hardware Inventory Wizard.

3   Follow the steps in the wizard to discover inventory for the selected devices.

4   Use the Reporting tab to view inventory reports.

Discovering Patch Compliance

Use the Patch Compliance Discovery Wizard to determine the compliance status of devices in your HPCA environment.

To discover patch compliance

1   Use the check boxes in the first column to select the devices that you want to query for patch compliance.

2   Click the **Inventory Collections** button and select **Discover Patch Compliance** to launch the Patch Compliance Discovery Wizard.

3   Follow the steps in the wizard to check the patch compliance for the selected devices.

4   Use the Reporting tab to view patch-compliance reports.

Discovering Application Usage

Use the Application Usage Collection Wizard to discover application usage for devices in your HPCA 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 Usage Management on page 274 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 for a Group on page 120 for information on collecting usage data for groups.

To discover application usage

1   Use the check boxes in the first column to select the devices that you want to target for application usage discovery.

2   Click the **Inventory Collections** button and select **Discover Application Usage** to launch the Application Usage Collection Wizard.

3   Follow the steps in the wizard 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. This interface allows you to connect to devices that have one of the following programs installed and enabled:

- Virtual Network Computing (VNC)
- Windows Remote Desktop Protocol (RDP)
- Windows Remote Assistance

HPCA will detect whether VNC, RDP, or Remote Assistance is installed on the remote system by connecting to the following ports: 5800 for VNC, and 3389 for RDP and Remote Assistance (see Firewall Considerations on page 102). If a connection is made on a particular port, HPCA will assume that the pertinent program is installed and running and will present that option as an available remote connection method.

Windows 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). HPCA detects this program by connecting to port 3389 on the remote device. See Requirements for Windows Remote Desktop on page 99.

VNC 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. See Requirements for VNC on page 100.

Windows Remote Assistance creates a special type of connection that enables you to offer help to users of managed client systems. In the connection, you serve as the "Expert," and the client system user serves as the "Novice." You can view the desktop of the client system and, with the permission of the Novice, you can control the client to resolve issues remotely. See Requirements for Windows Remote Assistance on page 100.

To launch a remote session

1 Select the device from the list, and then click the **Remote Control** 🖥️ button. This launches the Remote Control interface window.

2 Select the **Remote Control Method** from the available options. Only the programs detected by HPCA are available.

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.

Requirements for Remote Connections

The following requirements apply to any target devices that will be accessed remotely using the HPCA Console:

• The remote device must be powered on.

• If the firewall is enabled, the remote access port on the remote device must be open.

• The remote device must be accessible both to the HPCA server and to the client system initiating the request.

In addition, there are specific requirements for each type of remote access.

Requirements for Windows Remote Desktop

Windows Remote Desktop must be enabled on any target device that will be accessed remotely using this connection type. By default, this feature is not enabled.

To use Windows Remote Desktop, you must access the HPCA Console using Internet Explorer (version 7.0 or later). This is because the Console launches a wrapper that uses an ActiveX component when this type of connection is requested.

▶ 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.

For more information about Windows Remote Desktop, refer to the following Microsoft support document:

http://www.microsoft.com/windowsxp/using/mobility/getstarted/ remoteintro.mspx

Requirements for VNC

For VNC connections, target devices must have a VNC server process running, it must be listening on the specified port, and support for URL (HTTP) based remote control sessions must be enabled.

To establish a VNC connection, the HPCA Console launches the remote URL as a Java applet in your browser. For this reason, the Java Runtime Environment (JRE) version 1.5 (or later) must be installed on the system from which you are accessing the HPCA Console (the system where the browser is running). You can download the JRE at **www.java.com**.

The port number for the remote URL must match the port on which the VNC server on the remote system is listening. By default, this port is 5800. For example:

```
http://<RemoteSystem>:5800
```

In this case, a connection is made to the <*RemoteSystem*> using port 5800, the VNC remote control applet opens in your browser, and then you can control the <*RemoteSystem*> remotely.

HP does not provide a VNC server program. The HPCA Console, however, supports any VNC server that includes the web-based integration feature. This feature is available in UltraVNC, RealVNC, and TightVNC. VNC servers typically run on port 5800 and can be accessed through any web browser.

Requirements for Windows Remote Assistance

You can only create a Windows Remote Assistance connection when accessing the HPCA Console from a Windows Vista, Windows Server 2008, or Windows 7 system. You can connect to target devices running the following operating systems:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 Release 2 (R2) x64

When you initiate a Windows Remote Assistance connection to a target device, the user of the target device must accept the connection. You cannot create a Windows Remote Assistance connection to an unattended device.

Windows Remote Assistance must be enabled on any target device that will be accessed remotely using this connection type. For instructions, consult your network administrator, or refer to the following Microsoft support document:

http://support.microsoft.com/kb/305608/en-us

There are three additional requirements that must be met before Windows Remote Assistance connections can be used:

- Both the system where you are accessing the HPCA Console and the target devices must be joined to the same domain.

- The system where you are accessing the HPCA Console (the "Expert" system in the Windows Remote Assistance interaction) must have the following software installed:

   — Java Runtime Environment (JRE) version 5 (or later)

   — If the operating system is Windows 2008 Server, the Remote Instance feature must be installed. For more information, refer to the following article:

      http://technet.microsoft.com/en-us/library/cc753881.aspx

- The Offer Remote Assistance group policy must be enabled on all target devices. You must also specify a list of "helpers" who are allowed to access the target devices. Helpers can be either users or groups and must be specified as follows:

   ```
   domain_name\user_name
   ```

   ```
   domain_name\groupname
   ```

   In order to create a Windows Remote Assistance connection to a target device, you—or a group to which you belong—must be included in this list of helpers.

- The Remote Assistance exception in Windows Firewall must be enabled on all target devices.

For additional information about Windows Remote Assistance, refer to the following Microsoft support document:

http://technet.microsoft.com/en-us/library/cc753881.aspx

Firewall Considerations

If there is a firewall between the server hosting the HPCA Console and your remote devices, you must ensure that the appropriate ports are open.

Windows Remote Desktop Connection requires TCP port 3389.

By default, Windows Remote Assistance requires TCP port 3389 when connecting to Windows XP or Windows Server 2003 target devices. It requires port 135 (the DCOM port) when connecting to Windows Vista, Windows Server 2008, or Windows 7 devices.

VNC requires TCP port 5800 for the initial connection. In addition, it requires TCP ports 5900 + [as many ports as necessary, depending on the type of systems involved]. For example:

- On Windows systems, only TCP port 5900 is required.

- On a Linux system, say that the VNC Server is running at host:1. In this case, a firewall between the server and remote devices would need to allow access to TCP port 5901.

Similarly, the Java VNC viewer requires TCP ports 5800 + [as many ports as necessary, depending on the type of systems involved].

For additional information about using VNC with a firewall, refer to:

http://www.realvnc.com/support/faq.html#firewall

Power Management

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

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

  Follow the steps in the wizard to create a Power Management job for the selected devices.

Out of Band Management

The Out of Band Management (OOBM) features available in the HPCA Console enable you to perform out of band management operations regardless of system power or operating system state.

In band management refers to operations performed when a computer is powered on with a running operating system.

Out of band management refers to operations performed when a computer is in one of the following states:

- The computer is plugged in but not actively running (off, standby, hibernating)
- The operating system is not loaded (software or boot failure)
- The software-based management agent is not available

The HPCA Console supports Out of Band Management of Intel vPro devices and DASH-enabled devices.

To view Out of Band details for a device:

1 On the Management tab, go to the Device Management and click the Devices tab.

2 Select the device you want to work with, and click the **View Out of Band Device Details** toolbar icon.

The Out of Band Device Details window opens for the selected device.

This option is only available when Out of Band Management is enabled. See Out of Band Management on page 263 for instructions. For more detailed information, refer to the *HP Client Automation Out of Band Management User Guide*.

Removing Devices

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

To remove devices from HPCA

1 Use the check boxes in the first column to choose the devices that you want to remove.

2   Click the **Delete Device(s)** ✖ button to remove the devices from HPCA.

> ▶ Removing a device from the Device List does not remove device reporting data. Reporting data must be removed using the Configuration tab. See Database Maintenance on page 186 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 HPCA agent
- create device management jobs

The following areas are available at 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. Some of this information will not be available until the HPCA agent has been deployed.

▶ Last Logged on User reports the most recent user account to have logged on to the device using a Console login. If multiple users are logged on, only the last log on is recorded. Last Logged on User will not be updated by Remote Desktop Connection logins or by switching between current users.

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

Groups

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

OS

The OS tab displays all operating systems to which the device is entitled, 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 that are specific to the device you are viewing. For detailed reports, use the Reporting tab in the main HPCA console.

Current Jobs

Current Jobs displays all active and scheduled Device Management jobs. Device Management jobs target individual devices and can be used to deploy and remove an HPCA agent and administer software to devices in the HPCA 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 on page 161.

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.

Manually Installing the HPCA Agent

Typically, the HPCA Console is used to deploy the HPCA agent to target client devices that can then be managed by HPCA.

To manage client devices that are not always connected to the network, you can manually install the HPCA agent. For this, a separate installation file is included with the HPCA media. After the HPCA agent is installed on a client device it is automatically added to the HPCA database.

1   On the target device, insert the HPCA media.

2   Use a command line and go to the `Media\client\default\win32` directory of the HPCA media.

> On a system with User Access Control or User Account Control enabled, the command prompt must be run in Administrator mode. You can start a command prompt in Administrator mode by right clicking the Command Prompt entry in the Start Menu and selecting Run as administrator.

3   Type **setup-standard.cmd** *host*, where *host* is the hostname or IP address of your HPCA server.

4   Press **Enter**. The HPCA agent is installed and the device is ready to be managed by HPCA.

Installing the HPCA Agent on HP Thin Clients

With the HP **Registration and Loading Facility** (**RALF**) (see HP Registration and Loading Facility on page 110) installed and registered with the HPCA infrastructure, you can deploy the HPCA agent to thin client devices as you normally would. See Deploying the HPCA Agent from the Devices Tab on page 95 or Deploying the HPCA Agent to a Group on page 118.

However, if you are manually installing the HPCA agent, you will also need to install RALF (if it is not present) after the HPCA agent installation using the files provided on the HPCA media.

The HPCA agent installation for Windows XPE will automatically install RALF. For other thin client devices, first install the agent, then install RALF. The following sections contain detailed instructions.

> For RALF installations, "hpcaserver" or the host name defined using the RALF installation parameters must be included in DNS. The host name of the HPCA server must also be included in DNS when the agent is installed from the HPCA Console.

- Manually Installing the Agent on HP Thin Client Devices on page 108
- HP Registration and Loading Facility on page 110

Manually Installing the Agent on HP Thin Client Devices

To manually install the HPCA agent on a ThinPro client

The HPCA agent requires minimum free space of 5 MB on the /opt file system.

1 Login to the target HP thin client device as root. You may have to create a custom connection for xterm (as described in To create a custom connection for xterm on page 108).

2 Create a new directory called **/opt/hpca**.

3 Copy the installation media from the appropriate ThinPro client subdirectory on the HPCA media to a temporary directory on the /tmp file system.

4 Change the working directory to the new temporary directory and run the installation by typing:

   ./install –i *HPCA_Server*

   Where ***HPCA_Server*** is the hostname or IP address of the HPCA server.

   The HPCA agent is installed.

5 If RALF is already present on the device, reboot the device when the agent installation is complete.

   If RALF is not present, install RALF on the device. See To manually install RALF on Linux (Debian or ThinPro) on page 111.

To remove the HPCA agent from a ThinPro client

1 Login to the target HP thin client device as root.

2 Change the current directory to /opt/hpca/agent.

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

   The agent is removed.

To create a custom connection for xterm

You may need to create a custom connection to create an xterm connection.

1 From the HP menu in the lower left corner, select **Shutdown**.

2   From the **Thin Client Action** drop down, select **Switch to admin mode** and specify the administrator password (default password is root). Note: Control Center background will change from blue to red.

3   From the **Control Center**, click the **Add** drop-down list and select the **custom** option.

4   Set Name to **xterm**.

5   Set Command to run to:

```
sudo xterm -e bash &
```

6   Click **Finish**.

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

To manually install the HPCA agent to a Windows XPE thin client

The agent installation for Windows XPE automatically installs RALF. You do not need to install RALF separately after the agent installation is complete.

If RALF is already present on the device, stop the RALF service before running the agent installation.

1   Access the HPCA media from the Windows XPE thin client device.

2   On the HPCA media, go to Media\client\default\win32xpe.

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

4   Follow the steps in the installation.

5   When prompted, specify the IP address and port number of your HPCA server.

The HPCA agent is installed.

To install the agent to Windows XPE in silent mode, use the following command:

```
Setup.exe  NVDOBJZMASTER_ZIPADDR=<server_ip>
NVDOBJZMASTER_ZDSTSOCK=<server_port>  /qn
```

The following optional logging parameter can be added:

```
/l*v <log file>
```

To remove the HPCA agent from a Windows XPE thin client

Use the installation program `setup.exe` to remove the HPCA agent from
Windows XPE.

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

2 Select **Remove**.

3 Click **OK**.

    The HPCA agent is removed.

To manually install the HPCA agent to a Windows CE thin client

1 Access the HPCA media from the Windows CE thin client device.

2 On the HPCA media, go to `Media\client\default\win32ce`.

3 Double-click **Standard.X86.CAB**.

4 Type the hostname or IP address of the HPCA server and click **OK**.

    The HPCA agent is installed.

5 If RALF is already present on the device, reboot the device when the agent
    installation is complete.

    If RALF is not present, install RALF on the Windows CE device. See To
    install RALF for Windows CE 6.0 on page 112.

To remove the HPCA agent from a Windows CE thin client

• Use the Windows Control Panel applet **Add/Remove Programs** to remove
    the HPCA agent from Windows CE.

HP Registration and Loading Facility

The HPCA Registration and Loading Facility (RALF) is an agent component
available for thin client devices managed by an HPCA Core infrastructure.
RALF auto-registers the device with the HPCA infrastructure, and manages
the HPCA agent install which is initiated from the main Console. While RALF
is part of the HPCA agent, RALF may be available pre-installed on the HP
thin client factory images, so registration can occur upon startup. If it is not on
the factory image being used, RALF can be installed and configured on the
gold image used for subsequent OS deployments. If installing RALF, the
HPCA agent should also be installed prior to OS deployment.

RALF Configuration and Operation

Depending on the HP thin client image being used, RALF may be pre-installed. If so, it is configured using a default HPCA server hostname defined as "hpcaserver." While the HPCA server can be installed to match this name, it is more common to use this name as a DNS alias in defining the actual HPCA server host name. RALF can also be re-configured to define a different hostname using the command line options described below.

Once installed, RALF runs as a Windows service or Linux daemon that will periodically probe for the HPCA server. This probing will continue for 24 hours, and then RALF will shutdown. It will start this 24-hour probe again upon reboot. Once the server is contacted, RALF will register the device with the HPCA infrastructure and wait to accept the request to install the HPCA agent. Once the agent is installed, RALF will periodically contact the server and verify device registration attributes.

To manually install RALF on Linux (Debian or ThinPro)

You must have root authority to install RALF to Linux devices.

1 On the HPCA media, go to the `Media\client\default\linuxtc\hpcaralf` directory.

2 Copy the install media to `/tmp` on the Linux device.

3 Change the current directory to the `/tmp` directory.

4 Run the installation command.

    a On **Debian** devices:

        – run **`dpkg -i hpcaralf.deb`**.

    b On **ThinPro** devices (with read only root file system):

        – Run **`fsunlock`** (to mount the file system as writable).

        – Run **`/usr/share/hpkg/.hpkg_util -i hpcaralf.deb`**.

        – Run **`fslock`** (to remount the file system as read only).

5 After the installation is complete, either reboot the device or run **`/etc/init.d/hpcaralf`** to start and initialize RALF.

You can use this script (`/etc/init.d/hpcaralf`) to start and stop the RALF daemon on the device.

To manually install RALF to XPE and WES (Windows Embedded Standard)

The HPCA agent installation for Windows XPE will also install RALF; you do not need to install RALF separately.

1 On the HPCA media, go to the `media\client\default\win32xpe\HPCARALF` directory.

2 Use the `HPCARalf.msi` file to install RALF to Windows XPE devices.

   To perform a silent installation, use the following command line:

   ```
   msiexec /i HPCARalf.msi RALF_HOST=<HOSTNAME>
   RALF_PORT=<portnumber> /qn
   ```

To install RALF for Windows CE 6.0

1 On the HPCA media, go to the `media\client\default\win32ce\HPCARALF` directory.

2 Use the `ralf.X86.cab` file to install RALF to Windows CE devices.

3 When prompted, enter the HPCA server IP address and port (**hpcaserver** and **3466**, by default).

RALF Command Line Parameters

RALF supports the following command line options. These are here for documentation purposes, as most are used internally:

```
ralf.exe [-probe] [-host <host>] [-port <port>] [-debug]
[-trace] [-version]
```

[-confinit] (Linux)

[-reginit] (Windows)

```
[-help]
```

Table 7   RALF command line options

Option	Description
probe	Triggers the HPCA probe.
host	Specifies the optional HPCA server host for probing and registration.
port	Specifies the optional HPCA server port for probing and registration.
reginit	(Windows) Defines the RALF Application Registry entries for test environments.
confinit	(Linux) Defines the RALF Application configuration file entries for test environments.
debug	Specify a debugging logging level.
trace	Specify a tracing logging level.
version	Displays the version of RALF.
help	Displays the RALF information.

Group Management

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

The Group Management tabs are described in the following sections:

- General on page 114
- Groups on page 116
- Current Jobs on page 127
- Past Jobs on page 127

General

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

Groups can consist of managed and unmanaged devices.

To create a new Static Group

- In the Common Tasks area, click **Create a New Static Group** to launch the Group Creation Wizard.

  Follow the steps in the wizard to create a new device group.

To create a new Dynamic Discovery Group

- In the Common Tasks area, click **Create a New Dynamic Discovery Group** to launch the Group Creation Wizard.

  Follow the steps in the wizard to create a new device discovery group.

To create a new Dynamic Reporting Group

- Use the Reporting tab of the HPCA Console to define a query, then click the **Create a new Dynamic Reporting Group** button to begin the Group Creation Wizard.

The next section, Group Types, describes the different types of groups available in HPCA.

Group Types

HPCA uses the following group types to manage devices.

Internal

Internal groups are provided by HPCA. 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, manually modify the group membership using the Group Details window. Static group's memberships cannot be changed by using a schedule or other group parameters.

Discovery

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

Reporting

Create a reporting group from a list of devices returned in a report query. Reporting groups are automatically updated using a group management job.

The following Reporting groups are included with HPCA 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 that they find and that meet the dynamic group requirements.

Groups

The Groups tab lists all created groups. Groups that were created within the past seven days display the word 'new' in parentheses to the right of the group name.

- Click the display name 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 available column headings depending on which section of the Console you are in. The second box contains search parameters to customize your query. **Filtered Results** is displayed at the bottom of the table when you are viewing query results.

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

Table 8   Groups toolbar tasks

Button	Description
	Refresh Data – Refreshes the Groups list.
	Export to CSV – Creates a comma-separated list that you can open, view, and save.
	Create a New Group – Launches the Group Creation Wizard.
	Deploy the Management Agent – Launches the Agent Deployment Wizard.
	Remove the Management Agent – Launches the Agent Removal Wizard.

Table 8   Groups toolbar tasks

Button	Description
	Inventory Collections:
	Discover Software/Hardware Inventory – Launches the Software/Hardware Inventory Wizard.
	Discover Patch Compliance – Launches the Patch Compliance Discovery Wizard.
	Discover Application Usage – Launches the Application Usage Collection Wizard.
	Power Management – Launches the Power Management Wizard.
	Delete Devices – 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 Database Maintenance on page 186 for details.

The following tasks are available on the Groups tab.

Creating a Group

To create a Static group

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

  Follow the steps in the wizard to create a new Static group for software and patch deployment.

To create a Dynamic Discovery group

- Click the **Create a New Group** button, then select **Create a New Dynamic Discovery Group**. This will launch the Group Creation Wizard.

  Follow the steps in the wizard to create a new Dynamic Discovery group for software and patch deployment.

Deploying the HPCA Agent to a Group

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

HPCA Agent Notes

- Deploying the HPCA agent requires device authentication information (user name and password with administrator access). To deploy the HPCA agent to a group, all devices in the group must have the same authentication information.

- The HPCA agent cannot be remotely deployed to most thin client devices; it must be manually installed using the appropriate installation programs that are included in the \Media\client\default directory on the HPCA media.

To deploy the HPCA agent to a group of devices

1 Select the check box in the first column to select the group to which you want to either manage or re-deploy the HPCA agent.

2 Click the **Deploy the Management Agent** button to launch the Agent Deployment Wizard.

3 Follow the steps in the wizard to deploy the HPCA agent.

Removing the HPCA Agent from a Group

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

To remove the HPCA agent from a group of devices

1 Use the check boxes in the first column to choose the groups from which you want to remove the Agent.

2 Click the **Remove the Management Agent** button to launch the Agent Removal Wizard.

3 Follow the steps in the wizard to remove the HPCA 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 Use the check boxes in the first column to select the groups for which you want to discover inventory.

2 Click the **Inventory Collections** button, then select **Discover Software/ Hardware Inventory** to launch the Software/Hardware Inventory Wizard.

3 Follow the steps in the wizard to determine the inventory status for the devices in each group.

4   Use the Reporting tab of the HPCA Console to view inventory reports for
    the selected groups.

Discovering Patch Compliance for 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   Use the check boxes in the first column to select the groups that you want
    to target for patch compliance discovery.

2   Click the **Inventory Collections** 📟 button, then select **Discover Patch
    Compliance** to launch the Agent Deployment Wizard.

3   Follow the steps in the wizard to discover patch compliance for the devices
    within the selected groups.

4   Use the Reporting tab of the HPCA Console to view patch compliance
    reports for the selected groups.

Discovering Application Usage Data for a Group

Use the Application Usage Collection Wizard to discover application usage for
devices in your HPCA database. The wizard installs the Collection Agent,
which then returns usage data as defined by filters that you create and
enable. Also, if required, usage data can be hidden to ensure privacy. See
Usage Management on page 274 for more information.

To discover application usage

1   Use the check boxes in the first column to select the groups that you want
    to target for application usage discovery.

2   Click the **Inventory Collections** 📟 button, and select **Discover Application
    Usage** to launch the Application Usage Collection Wizard.

3   Follow the steps in the wizard to discover application usage for the
    selected groups.

4   Use the Reporting tab of the HPCA Console to view the usage reports.

Power Management

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

1   Select the group that you want to manage and click the **Power Management**

    button to launch the Power Management Wizard.

2   Follow the steps in the wizard to create a Power Management job for the
    selected group.

Removing Groups

Use the Groups toolbar to remove groups from HPCA. Removing a group will
not remove the devices that belong to that group.

To remove Groups from HPCA

1   Use the check boxes in the first column to select the groups to be removed.

2   Click the **Delete Group(s)** button to remove the group from HPCA.

Group Details

Click any Group name to open the Group Details window.

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

General

The General tab displays common tasks that are 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. Valid group types are:

— **Static**: manually update device membership 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 that are 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 that is listed in the Software tab is entitled to the group. Adding and removing software entitlements affects all existing device members as well as any devices added to the group.

Use the toolbar buttons to add and remove entitlements, synchronize software, and deploy and 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 that are entitled to the group.

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

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

Settings Profiles

The Settings Profile tab displays all settings profiles that are entitled to the group.

Use the toolbar buttons to add and remove settings profile entitlement for the group, and to deploy a settings profile to devices in the group.

Reporting

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

Current Jobs

The Current Jobs tab displays all currently active and 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 124
- Adding and Removing Software Entitlement from Groups on page 124

Adding and Removing Devices from Static Groups

Use the Group Details window to update memberships in a Static group.

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 to be added, and click **Add Devices**.

To remove devices from a Static group

Removing devices from a group only removes the group membership; the device is not removed from the device list.

1 In the Group Details window, click the **Devices** tab.

2 Select the devices to be removed, and click **Delete Device(s)** .

Adding and Removing Software Entitlement from Groups

Use the Group Details window to add and 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 Software Entitlement** . The Software Entitlement window opens.

3 Select the software to be entitled to the group and click **Add Software Entitlement**.

1   In the Group Details window, click the **Software** tab.

2   Select the software for which you want to remove entitlement, and click

    Remove Software Entitlement .

Deploying, Removing, and Synchronizing Software from Groups

Use the Group Details window to deploy, remove, and 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 to be deployed and click **Deploy Software** .

3   To deploy the software to the managed devices in the group, follow the steps in the Software Deployment Wizard on page 289.

To remove software from a group

1   In the Group Details window, click the **Software** tab.

2   Select the software to be removed from the managed devices in the group

    and click **Remove Software** .

3   To remove the software from the managed devices in the group, follow the steps in the Software Removal Wizard on page 298.

To synchronize software

1   In the Group Details window, click the **Software** tab.

2   Click **Synchronize Software** to launch the Software Synchronization Wizard.

3   Follow the steps in the wizard to set a software synchronization schedule for the group.

    This will ensure that all entitled software is installed to current members of the group, as well as any members subsequently added to the group.

Adding and Removing Patch Entitlement from Groups

Use the Group Details window to add and 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 Patch Entitlement** ![icon] to launch the Patch Entitlement window.

   ▶ 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.

3 Select the patches that you want to entitle to the group and click **Add Patch Entitlement**.

To remove patch entitlement from a group

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

2 Select the patches for which you want to remove entitlement, then click **Remove Patch Entitlement** ![icon].

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 that you want to deploy and click **Deploy Patches** ![icon] to launch the Patch Deployment Wizard.

3 Follow the steps in the wizard on page 296 to deploy the patches to the managed devices in the group.

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

Current Jobs

Current Jobs displays all active and scheduled Group Management jobs. Group Management jobs target specific groups and are used to administer software to devices in those groups, and to refresh the devices in the Dynamic Reporting and 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 Job Controls and Job Status, see Job Management, Current Jobs on page 161.

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 area to manage software services and software management jobs. Software is entitled to managed devices (or groups of managed devices) and then either deployed by the administrator using the HPCA console, or installed by the end-user using the Application Self-Service Manager.

The Software Management tabs are:

- General Tab on page 128
- Software Tab on page 129
- Current Jobs Tab on page 135
- Past Jobs Tab on page 135

▶ To view or modify settings for a particular software service, see the Software Details Window (Management Tab) on page 131.

General Tab

Use the General tab on the Software Management page to do the following:

- Find information about how to publish software
- Entitle and deploy software to managed devices
- View current and past Software Management jobs

The Summary section shows you how many software services are currently available in the HPCA Software Library as well as the number of current Software Management jobs.

To publish software

Use the Publisher to publish software into HPCA. Published software is displayed in the Software Library.

Install the Publisher on the machine where you will be selecting and configuring software services. See Publishing on page 347 for information about how to publish software into HPCA.

1   In the Common Tasks area, click **Deploy.** This will launch the Software Deployment Wizard.

2   Follow the steps in the wizard to entitle and deploy software to managed devices.

Software Tab

The Software tab lists all software applications that have been published into HPCA. Use the tools available on this tab to entitle groups of managed devices to one or more software services or deploy software to managed devices.

See the following topics for details:

• Deploy Software on page 129

• Add or Modify Group Entitlement on page 130

➤   To view or modify settings for a particular software service, see the Software Details Window (Management Tab) on page 131.

Deploy Software

Use the Software Deployment Wizard to deploy software to individual managed client devices or groups of devices.

To entitle and deploy software

1   Select the software that you want to deploy, and click **Deploy Software** to launch the Software Deployment Wizard.

2   Follow the steps in the wizard to entitle and deploy software to managed devices.

To run applications in the active session on Windows Vista devices

Use the **runasuser** method modifier to allow deployment of applications that require user interaction on Vista devices.

1   Click the Service ID to open the Software Details window for a service.

2   Open the Properties tab.

3   Add the modifier **runasuser** to the beginning of the Install Command
    Line. For example:

    ```
    runasuser setup.exe
    ```

    Alternatively, this modifier can be included during publishing by adding it
    to the Method property, Method to Install Resource.

> The method modifier **runasuser** cannot be used with the
> modifier **hide**; these are mutually exclusive.

Add or Modify Group Entitlement

You can entitle groups of managed devices to any services listed in the
Software Library.

To add group entitlement

1   Select the check box in the first column to select one or more software
    services for group entitlement.

2   Click **Add Group Entitlement** to launch the Service Entitlement Wizard.

3   Follow the steps in the wizard to entitle one or more groups of devices to
    this software service.

Default Software

HPCA contains the following default software services.

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

• **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, publish BIOS settings, or publish HP
  Softpaqs.

• **TPM_ENABLEMENT** – TPM Enablement.

This service initializes the use and ownership of the **TPM** (**Trusted Platform Module**) chip on compatible HP devices. It does so using the settings from the Configuration tab, Device Management section. See Trusted Platform Module on page 257 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 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. For more information, review the HP documentation for your device.

Software Details Window (Management Tab)

To open the Software Details window for a particular software service, go to the Software tab, and click the Service ID. From the Software Details window, you can view software properties, view and modify entitlements, deploy or remove software, perform power management operations, initiate a remote control session, or view a reporting summary.

General Tab

The General tab displays the common tasks that are available for the software. The following links take you to the other tabs in the Software Details window:

- Properties Tab on page 132
- Groups Tab on page 132
- Devices Tab on page 134
- Reporting Tab on page 135

The **Deploy Software** link launches the Software Deployment Wizard, which enables you to do the following:

1   Entitle one or more groups of managed devices to this software.

2   Deploy the software to these groups.

See the Software Deployment Wizard on page 289 for more information.

▶   You can also deploy the software by using the Groups or Devices tabs. In this case, the groups (or devices) must have been previously entitled to this software.

Properties Tab

Use the Properties tab to view information about the software, including the software category and install/un-install commands.

▶   This information is read-only in this context. You can modify these settings by using the Software Management area on the Operations tab. See Software Management on page 186 for more information.

Groups Tab

The Groups tab lists all groups of managed client devices that are entitled to this software. Use the toolbar buttons to manage group entitlements, deploy or remove the software, launch a data collection operation, or perform power management operations.

Table 9   Actions Available on the Groups Tab

Button	Functions	Action
	Refresh Data	Refreshes the list of groups.
	Export to CSV	Creates a comma-separated list of the groups in the table, which you can then open or save.
	Add Group Entitlement	Entitle one more groups of managed client devices to this software.
	Remove Group Entitlement	Remove a group's entitlement to this software.

Table 9   Actions Available on the Groups Tab

Button	Functions	Action
	Deploy Software	Deploy this software to the selected group (or groups) of devices. See the Software Deployment Wizard on page 289.
	Remove Software	Remove this software from the selected group (or groups) of devices. See the Software Removal Wizard on page 298.

	Inventory Collections	Launch a wizard that schedules one of the following data collection jobs for the selected group (or groups) of devices and creates a report:
		• **Discover Software/Hardware Inventory**
		  See the Software/Hardware Inventory Wizard on page 283.
		• **Discover Patch Compliance**
		  See the Patch Compliance Discovery Wizard on page 284.
		• **Discover Application Usage**
		See the Application Usage Collection Wizard on page 307.

	Power Management	Turn on, turn off, or reboot a group of devices. See the Power Management Wizard on page 285.

The Devices tab displays all devices that are currently entitled to the selected software. Use the toolbar buttons to deploy and remove software from a device, launch a data collection operation, perform power management operations, or control a device remotely.

Table 10   Actions Available on the Devices Tab

Button	Function	Action
	Refresh Data	Refreshes the list of devices.
	Export to CSV	Creates a comma-separated list of the devices in the table, which you can then open or save.
	Deploy Software	Deploy this software to the selected devices. See the Software Deployment Wizard on page 289.
	Remove Software	Remove this software from the selected devices. See the Software Removal Wizard on page 298.
	Inventory Collections	Launch a wizard that schedules one of the following data collection jobs for the selected devices and creates a report: • **Discover Software/Hardware Inventory** See the Software/Hardware Inventory Wizard on page 283. • **Discover Patch Compliance** See the Patch Compliance Discovery Wizard on page 284. • **Discover Application Usage** See the Application Usage Collection Wizard on page 307. You can access the reports on the Reporting Tab tab.

Table 10   Actions Available on the Devices Tab

Button	Function	Action
⏻	Power Management	Turn on, turn off, or reboot the selected devices. See the Power Management Wizard on page 285.
🖳	Remote Control	Launch a Remote Control session to the selected device. See Remote Control on page 98.

Reporting Tab

The Reporting tab in the Software Details window contains summary reports that are specific to the software that you are viewing. For detailed reports, use the Reporting tab in the main HPCA console.

Current Jobs Tab

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

Click a 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 on page 161.

Past Jobs Tab

Past Jobs displays all completed software management jobs.

Click a 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.

Settings Management

Settings profiles allow you to manage and deploy configuration settings for specific software supported by HPCA. Once you have created or modified settings profiles, you can deploy them to the targeted systems where the relevant software is installed. Creating settings profiles is performed in the Operations area on the HPCA Console. Your log-in account must have the appropriate role to access the Operations area of the console.

See Settings Management on page 210 for information about how to create and modify profiles.

Use the Settings Management section in the Management area to manage settings profile services and settings profile management jobs. Settings profile services are entitled to groups of managed devices and then deployed by the administrator using the HPCA Console. In this section, you are able to deploy settings profiles, to view settings profile details, and to add group entitlement to the services.

The Settings Management tabs are:

- General on page 136
- Settings Profiles on page 137
- Current Jobs on page 139
- Past Jobs on page 139

General

Use the General tab to deploy settings profiles and to view current and past settings profile management jobs.

The Summary section displays how many settings profile services are currently available in the HPCA database as well as the number of current settings profile management jobs scheduled.

Settings Profiles

The Settings Profiles tab displays all of the settings profiles available for specific HPCA-supported applications. The icons on this tab are summarized in the following table:

Table 11   Settings Profiles Management toolbar tasks

Button	Description
	Refresh Data – Refreshes the settings profiles listed.
	Export to CSV – Creates a comma-separated list that you can open, view, and save.
	Deploy Settings Profile – Launches the Settings Profile Deployment Wizard.
	Add Group Entitlement – Launches the Service Entitlement Wizard.

The following tasks are available from the Settings Profiles tab:

- Deploying Settings Profiles on page 137
- Adding Group Entitlement on page 138

Deploying Settings Profiles

The deployment of settings profiles is a task that you can perform on the Management tab of the HPCA console. You can deploy profiles by first entitling a group of devices for this profile. To create a group of devices for settings profile entitlement, refer to Group Management on page 114. You will want to populate this group with devices that are relevant to the settings profile.

Use the Settings Profile Deployment Wizard to deploy or remove settings profiles to groups of devices.

1   Select the check box in the first column to select the settings profile(s) you

    want to deploy or remove and click **Deploy Settings Profile** to launch
    the Settings Profile Deployment Wizard.

2   Follow the steps in the wizard on page 291 to deploy or remove settings
    profiles to/from the managed devices in your environment.

Adding Group Entitlement

Settings profiles can be entitled to groups of devices.

To add group entitlement

1   Select the check box in the first column to select the settings profile for
    group entitlement.

2   Click **Add Group Entitlement** to launch the Service Entitlement
    Wizard.

3   Follow the steps in the wizard to entitle the settings profile to groups of
    devices that you will select using the wizard.

Settings Profiles Details

Click any Display Name for a settings profile to open the Settings Profile
Details window. Use the Settings Profile Details window to view settings
profile service properties, view and modify entitlements, deploy and remove
settings profiles, and view a reporting summary.

•   On the General tab, you can confirm that the summary information
    reflects the newly established group/device entitlement. You can also use
    the shortcut links that provide easy access to common settings profile
    management tasks.

•   On the Properties tab, you can view the properties for the settings profile.

•   On the Groups tab, you can deploy or remove the settings profile, and you
    can add or remove entitlement. See Settings Profile Deployment Wizard
    on page 291.

- On the Devices tab, you can deploy or remove the settings profile. See Settings Profile Deployment Wizard on page 291.

- On the Reporting tab, you can view a contextual report based on the selected settings profile.

Current Jobs

Current Jobs displays all currently active and scheduled settings profile management jobs. Settings profile management jobs are used to entitle, deploy, and remove settings profiles from managed devices in your HPCA database.

Click a 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 Current Jobs on page 106.

Past Jobs

Past Jobs displays all completed settings profile management jobs.

Click a 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 Microsoft patches, HP Softpaqs, and patch management jobs.

Microsoft patches and HP Softpaqs are entitled and deployed to groups of managed devices by an HPCA administrator. The deployment can be done automatically, based on an administrator-defined compliance schedule. See Patch Management on page 258.

HP Softpaqs that are *published* using the Publisher are contained in the Software Library; *acquired* HP Softpaqs are contained in the Patch Library.

The Patch Management tabs are:

- General Tab on page 142
- Patches Tab on page 144
- Current Jobs Tab on page 147
- Past Jobs Tab on page 148

To view or modify settings for a particular patch, see the Patch Details Window (Management Tab) on page 145.

Microsoft Update Catalog: Minimum OS and Service Pack Requirements

All hyperlinks that are documented in this section are current and viable at time of publication.

Refer to Microsoft's web site for specific information on the minimum operating system and service pack requirements for the **Microsoft Update Catalog** and **Windows Update** technologies that are leveraged by HPCA

Patch Management. As of this writing, the supported Microsoft operating system versions and languages can be viewed at the Microsoft Update home page, **http://update.microsoft.com/microsoftupdate/v6/default.aspx**.

► Windows Installer, version 3.1 is required on HPCA agent machines because newer Microsoft security patches require this to install more recent security patches. Additional information on Windows Installer 3.1 is available at the Microsoft Knowledge Base article, **Windows Installer 3.1 v2 is available**.

Important Information about Microsoft Automatic Updates

Automatic Updates is a feature of Microsoft Windows operating systems that enables users to scan their system in order to determine whether it is missing any updates or patches. It also allows for the download and installation of the updates and patches. This feature currently supports the following configuration options.

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

    ► HP recommends using the **Turn off Automatic Updates** option.

⚠ It is important that you understand the implications and consequences of each of these options. Review the following section before choosing one of these options on a system.

Automatic Updates Considerations

Automatic Updates and HPCA Patch Manager use an underlying Windows component, **Windows Update Agent** (**WUA**), to scan a device and install updates. As of this writing, there is a known issue that arises when WUA is being used by multiple patch-management products. Therefore, if you are using Patch Manager to distribute and install updates, use the information in this section to configure Automatic Updates; otherwise a problem situation could arise.

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 HPCA agent is scanning or installing updates. If the Automatic Updates process is manually initiated, it could result in *either* process failing to download and install the updates on the managed device.

This behavior is not specific to Patch Manager; it is also exhibited when other patch-management products attempt to use WUA when WUA is already in use. Microsoft is expected to correct this problem. As of this writing, relevant Microsoft Knowledge Base articles include:

- Microsoft Knowledge Base article 910748, **SMS 2003 Inventory Tool for Microsoft Updates....**

- Microsoft Knowledge Base article 931127, **You receive an error message in the WindowsUpdate.log file...**.

- If virus scanners are installed and enabled in your enterprise, refer to Microsoft Knowledge Base article 922358 (**Microsoft Systems Management Server 2003 Inventory Tool for Microsoft Updates cannot run when a McAfee antivirus program is installed on the same computer**) which documents the 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 that is using HPCA Patch Manager, which leverages Windows Update Agent technologies.

- If you select **Turn off Automatic Updates**, it is possible that you will not be informed of all available updates because Automatic Updates supports some products that are not supported by HPCA

WUA uses the Automatic Updates Windows service, which must be set to either **Automatic** or **Manual** on target devices. The Automatic Updates Windows service can be in a stopped state because WUA will start it as needed. Refer to the Microsoft Knowledge Base article, **How to configure and use Automatic Updates in Windows XP**, for more information about Automatic Updates.

General Tab

Use the General tab to acquire and deploy patches, and view current and completed Patch Management Jobs.

The Summary section displays the patches that are currently available in the HPCA database and the number of current Patch Management jobs.

The acquisition of Microsoft patches and HP Softpaqs from their sources is based on information that is specified in the Patch Management section of the Configuration tab. See Patch Management on page 258 for more information.

To acquire patches

- In the Common Tasks area, click **Acquire**.

  Patches are downloaded and added to the Patch Library. HPCA will automatically download additional patches according to the acquisition schedule that was configured by an administrator.

  Patches are deployed to managed devices from the HPCA Console only; they are not available in the Application Self-service Manager software catalog.

To deploy patches

1 In the Common Tasks area, click **Deploy** to launch the Patch Deployment Wizard.

2 Follow the steps in the wizard to deploy patches to devices in selected groups.

Patches Tab

The Patch Library contains the patches and HP Softpaqs that were acquired based on the settings in the Patch Management section of the Configuration tab. These patches and HP Softpaqs are available for entitlement and deployment to managed devices. See Patch Management on page 258 for more information.

Table 12   Patch Library toolbar tasks

Button	Description
	Refresh Data – Refreshes the Patch Library.
	Export to CSV – Creates a comma-separated list that you can open, view, and save.
	Deploy Patches – Launches the Patch Deployment Wizard.
	Add Group Entitlement – Launches the Service Entitlement Wizard.

The following tasks are available on the Patches tab.

- Deploying Patches on page 144
- Adding Group Entitlement on page 145
- Patch Details Window (Management Tab) on page 145

Deploying Patches

Patches that are available in the Patch Library can be deployed to managed devices.

To deploy patches

1   Use the check boxes in the first column to select a patch for deployment.

2   Click the **Deploy Patches** button to launch the Patch Deployment Wizard.

3   Follow the steps in the wizard to deploy the patch.

Adding Group Entitlement

Patches that are available in the Patch Library can be entitled to groups of devices. Entitlement allows patch compliance to be enforced using the schedule that is configured in the Patch Deployment Wizard.

To add group entitlement

1   Use the check boxes in the first column to select a patch for group entitlement.

2   Click the **Add Group Entitlement** 🐾 button to launch the Service Entitlement Wizard.

3   Follow the steps in the wizard to entitle the patch to groups of devices that you will select.

Patch Details Window (Management Tab)

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

General

The General tab displays the common tasks that are 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.

▶   This information on this tab is read-only. You cannot modify these settings.

Groups

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

- To entitle a group, click **Add Group Entitlement** ![icon].

- To remove entitlement from a group, select the group and click the **Remove Group Entitlement** ![icon] button.

- To deploy the patch to a group, select the group and click **Deploy Patches** ![icon].

  Follow the steps in the Patch Deployment Wizard to deploy the selected patch.

- To discover software and hardware inventory for a group of devices, select the group and click the **Inventory Collections** ![icon] button, then select **Discover Software/Hardware Inventory**.

  Follow the steps in the Software/Hardware Inventory Wizard to discover software and hardware inventory.

- To discover patch compliance for a group of devices, select the group and click the **Inventory Collections** ![icon] button, then select **Discover Patch Compliance**.

  Follow the steps in the Patch Compliance Discovery Wizard to discover patch compliance.

- To discover application usage for a group of devices, select the group and click **Inventory Collections** ![icon], and then select **Discover Application Usage**.

  Follow the steps in the Application Usage Collection Wizard to discover application usage data.

- To turn on, turn off, and reboot a group of devices, select the group and click the **Power Management** ![icon] button.

  Follow the steps in the Power Management Wizard to manage the devices.

Devices

Devices that are listed in the Devices tab have been entitled to the selected patch. Use the toolbar buttons to deploy the patch to a device.

- To deploy a patch to a device, select the device and click the **Deploy Patches** ![icon] button.

Follow the steps in the Patch Deployment Wizard to deploy the patch.

➤ After a patch is deployed it cannot be removed.

- To discover software and hardware inventory for devices, select the devices and click **Inventory Collections** 🖳, then select **Discover Software/Hardware Inventory**.

  Follow the steps in the Software/Hardware Inventory Wizard to discover software and hardware inventory.

- To discover patch compliance for devices, select the devices and click the **Inventory Collections** 🖳 button, then select **Discover Patch Compliance**.

  Follow the steps in the Patch Compliance Discovery Wizard to discover patch compliance.

- To discover application usage for devices, select the devices and click the **Inventory Collections** 🖳 button, then select **Discover Application Usage**.

  Follow the steps in the Application Usage Collection Wizard to discover application usage data.

- To turn on, turn off, and reboot devices, select the devices and click the **Power Management** ⏻ button.

  Follow the steps in the Power Management Wizard to manage the devices.

Reporting

The Reporting tab contains summary reports that are specific to the patch you are viewing. For detailed reports, use the Reporting tab in the main HPCA console.

Current Jobs Tab

Patch Management jobs are used to deploy security patches to devices. Current Jobs shows a list of active and scheduled jobs. Click the description of a job to display more details about its status.

Use the toolbars to administer currently scheduled and active jobs.

For information about Job Controls and Job Status, see Job Management, Current Jobs on page 161.

Past Jobs Tab

Past Jobs displays all completed Patch Management jobs. Click the
description of a job to display more details about its status.

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

OS Management

Use the OS Management area on the Management tab to manage the operating systems used by your managed devices. The areas in this section enable you to deploy operating systems and manage entitlements.

The following sections describe each OS Management tab:

▶

General Tab

Use the General tab on the OS Management page to do the following:

- Find information about how to publish operating systems
- Manage entitlements
- Deploy operating systems to managed devices
- View current and past OS Management jobs

The Summary section shows you how many operating systems are currently available in the HPCA OS Library as well as the number of current OS Management jobs.

To capture and publish OS images

HPCA provides tools that you can use to prepare and capture OS images. See for more information.

For OS images to be available in the OS Library, they must first be published. See for more information.

1 In the Common Tasks area, click **Deploy Operating System.** This launches the OS Deployment Wizard.

2 Follow the steps in the wizard 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 Deploy an Operating System on page 151.

Operating Systems Tab

The Operating Systems tab lists all available operating systems that have been published into HPCA.

Use the tools provided to deploy operating systems to managed devices or entitle groups of devices to them.

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 13   OS Library Toolbar Actions

Button	Description
	Refresh Data – Refreshes the list of operating systems in the OS Library.
	Export to CSV – Creates a comma-separated list of the operating systems in the table, which you can then open, view, and save.
	Deploy Operating System – Launches the OS Deployment Wizard.
	Add Group Entitlement – Launches the Service Entitlement Wizard.

The following tasks are available from the Operating System tab:

- Deploy an Operating System on page 151
- Deploy an OS Image Using LSB on page 153

Deploy an Operating System

To entitle and deploy an operating system

1 Select the operating system service to deploy, then click the **Deploy Operating System** 🔁 button. This will launch the OS Deployment Wizard.

2 Follow the steps in the wizard 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 on page 268 to select the deployment mode.

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

Deployment Scenarios

How you deploy 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 14   Deployment Scenarios

Device State	Instructions for deployment
Managed (agent installed)	If the device is already managed: • Add the device to a group. • Entitle the group to an operating system (if not already entitled). • Use the OS Deployment Wizard to deploy the OS. Note: If you use LSB during the OS deployment process, you will not need to make preparations for PXE or the Service CD.
Un-managed (agent not installed)	If the unmanaged device has an OS installed: • Deploy the HPCA agent to the device. • See instructions for Managed device above. If the unmanaged device does *not* have an OS installed: • See the instructions below for how to deploy an OS to a bare-metal device.

Table 14 Deployment Scenarios

Device State	Instructions for deployment

Bare-metal (no OS installed)	If the device was previously managed (for hard drive recovery, for example):
	
	• Group membership and any OS entitlements should still be valid. Deploy the OS using PXE or the Service CD.
	
	If the device was not previously managed:
	
	• Boot the device with PXE or the Service CD.
	
	  The device is added to HPCA using a variation on the MAC address as its device name.
	
	• Add the new device to a group with OS entitlement.
	
	  The device is rebooted, and the Service CD or PXE will continue with the OS deployment.
	
	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.
	
	Note: LSB cannot be used for deploying an OS to a bare-metal device.

Deploying Thin Client Factory Images

Before you can deploy a factory image of a supported thin client operating system, (Windows XP Embedded (XPE), Windows CE, or ThinPro) to a device, you must first capture and publish that client image before you can deploy it. See the Preparing and Capturing OS Images chapter for more information.

Deploy an OS Image Using LSB

Local Service Boot (LSB) allows HPCA to assume management of the OS on devices that are not booted from the network.

When LSB is used, 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 152 for prerequisite instructions for OS deployment.

1   Select the image for deployment, and click the **Deploy Operating System** 🔄 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 that you selected. If the device is entitled to multiple OS images, you will be prompted to select which OS to install.

Deploy an OS Image Using PXE

The PXE-based environment allows HPCA to assume management of the OS on target devices that are booted from the network. See Deployment Scenarios on page 152 for prerequisite instructions for OS deployment.

Using PXE consists of configuring your DHCP server to provide clients booting from the network with two things:

- A boot image
- 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.

When PXE is configured, make sure that your target devices boot from the network or have PXE-enabled as the primary boot device. Make the necessary configuration adjustments to ensure that this will happen—for example, with some BIOS versions, you can press **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 button 🗜 to launch the OS Deployment Wizard.

3   Follow the steps in the wizard, and when prompted for deployment method, select **Local CD or PXE Server**.

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

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

Deploy 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 HPCA media in the \Media\iso\roms\ 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 152 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 from the CD.

2   When prompted, enter your HPCA server IP address (or host name) and port number, and then press **Enter** to continue. For example:

HPCA.acmecorp.com:3466

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

The device connects to the HPCA 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 HPCA 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 HPCA 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** 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.

Add Group Entitlement

Before you can deploy an operating system to a group of target devices, that group must be entitled to use that operating system.

To add group entitlement

1   Use the check boxes in the first column to select the OS image for group entitlement.

2   Click the **Add Group Entitlement** button to launch the Service Entitlement Wizard.

3   Follow the steps in the wizard to entitle the selected images to groups of devices that you will select using the wizard.

Restore an Operating System

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

OS Details Window (Management Tab)

Click any operating system Service ID to open the OS Details window. Use the OS Details window to view OS properties, view or modify entitlements, deploy an operating system, or view a reporting summary. 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.

The Summary area shows you how many groups and devices are entitled to this OS.

Properties

Use the Properties tab to view information about the operating system.

▶ This information is read-only in this context. You can modify these settings by using the OS Management area on the Operations tab. See OS Details Window (Operations Tab) on page 206 for more information.

Groups

The Groups tab lists all groups of managed client devices that are entitled to this OS. Use the toolbar buttons to manage entitlements, deploy the OS, launch a data collection operation, or perform power management operations.

Table 15   Actions Available on the Groups Tab

Button	Function	Action
⟳	Refresh Data	Refreshes the list of groups.

Table 15   Actions Available on the Groups Tab

Button	Function	Action
	Export to CSV	Creates a comma-separated list of the groups in the table, which you can then open or save.
	Add Group Entitlement	Entitle one or more additional groups of managed client devices to this OS.
	Remove Group Entitlement	Remove a group's entitlement to this OS.
	Deploy Software	Deploy this OS to the selected group (or groups) of devices. See the OS Deployment Wizard on page 300.
	Inventory Collections	Launch a wizard that schedules one of the following data collection jobs for the selected group (or groups) of devices and creates a report: • **Discover Software/Hardware Inventory** See the Software/Hardware Inventory Wizard on page 283. • **Discover Patch Compliance** See the Patch Compliance Discovery Wizard on page 284. • **Discover Application Usage** See the Application Usage Collection Wizard on page 307. You can access the reports on the Reporting Tab tab.
	Power Management	Turn on, turn off, or reboot a group of devices. See the Power Management Wizard on page 285.

The Devices tab displays all devices that are currently entitled to the selected OS. You can deploy the OS to a device, launch a data collection operation, perform power management operations, or control a device remotely by using the toolbar buttons.

Table 16   Actions Available on the Devices Tab

Button	Function	Action
	Refresh Data	Refreshes the list of devices.
	Export to CSV	Creates a comma-separated list of the devices in the table, which you can then open or save.
	Deploy Operating System	Deploy this software to the selected devices. See the OS Deployment Wizard on page 300.
	Inventory Collections	Launch a wizard that schedules one of the following data collection jobs for the selected devices and creates a report: • **Discover Software/Hardware Inventory** See the Software/Hardware Inventory Wizard on page 283. • **Discover Patch Compliance** See the Patch Compliance Discovery Wizard on page 284. • **Discover Application Usage** See the Application Usage Collection Wizard on page 307. You can access the reports on the Reporting Tab tab.

Table 16   Actions Available on the Devices Tab

Button	Function	Action
⏻	Power Management	Turn on, turn off, or reboot the selected devices. See the Power Management Wizard on page 285.
🖳	Remote Control	Launch a Remote Control session to the selected device. See Remote Control on page 98.

Reporting

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

Current Jobs Tab

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 HPCA 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 on page 161.

Past Jobs Tab

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

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 ID link 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

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 17   Actions Available on the Jobs Toolbar

Icon	Description
	Refresh Data – Refreshes the jobs list.
	Export to CSV – Creates a comma-separated list that you can open or save.
	Start Job(s).
	Resume Job(s) that were Disabled or Paused.
	Pause Job(s) that are Currently Active, Waiting to Start, and Waiting to Stop. Job status is set to Paused.
	Stop Job(s) that are currently Active or Paused. Job status is set to Waiting to Stop.
	Reschedule Job(s).
	Delete Job(s).

Job Status

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

Table 18 Job status descriptions

Icon	Status	Description
❌	Ended with Errors	Job completed but with errors. Click the job ID link for more information.
✅	Successful	Job completed successfully without errors.
▶	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.
ℹ	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 19   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
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

Table 19   Job Status and expected Job Control action

	Start	Resume	Pause	Stop	Reschedule	Delete
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 job ID link. 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 ID 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.

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 Chapter 18, Troubleshooting for some additional information about Job messages.

Past Jobs

Past Jobs shows all completed Management jobs. Click the job ID link 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.

7 Using Reports

The Reporting area contains summary and detailed reports of many kinds. The specific reports available to you depends on the type of HPCA license that you have. The following topics are discussed in this chapter:

- Reports Overview on page 168

- Navigating the Reports on page 169

- Types of Reports on page 171

- Filtering Reports on page 176

- Creating Dynamic Reporting Groups on page 179

Reports Overview

On the Reporting tab in the HPCA Console, there are links to several collections of reports as described in

Each collection contains groups of reports that focus on a particular type of data or a specific audience. These reports also provide the data used to populate the dashboards.

The following reports are available in all editions of HPCA:

Report Pack	Report Type	Description
rpm.kit	Patch Management	Devices in and out of compliance with patch policy
rim.kit	Inventory	Devices currently managed by HPCA

▶ In order to view the Reporting section's graphical reports, a Java Runtime Environment (JRE) or Java Virtual Machine (JVM) is required. For more information, go to:

http://java.com/en/index.jsp

Navigating the Reports

When you click the Reporting tab, the Reporting home page is displayed. The home page provides a snapshot of the enterprise with respect to inventory management, patch management (if installed and enabled), and usage management (if enabled).

There are three ways to find more detailed information on the Reporting home page:

- Use Report Quicklinks to open frequently requested reports.

- Use Quick Search to find inventory information about a specific device or service. This feature *only* applies to inventory reports – for example, Managed Devices.

- Use the links in the Reporting Views section of the left navigation tree to open a specific report.

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

The following actions are available on the Reports page when a report is displayed:

Table 20   Report Actions

Icon	Description
	Go back one page in the reports view.
	Return to the Reports home page.
	Refresh the data. A refresh also occurs when you apply or remove a filter.
	Add this report to your list of favorites.

Table 20   Report Actions

Icon	Description
✉	Email a link to this report.
?	Open a "quick help" box or tool tip. This applies only to filters.
🖨	Print this report.
▤	Collapses the data portion of the report view.
▤	Expands the data portion of the report view.
📊	Show the graphical view of this report
▦	Show the grid (detailed) view of this report.
📑	Export report contents to a comma-separated value (CSV) file. The data in this file is actually delimited by tabs, not commas. The file extension is CSV, however.
📑	Export report contents to a Web query (IQY) file.

Items that appear in blue text in a report have various functions:

- Show Details – drill down to greater detail pertaining to this item

- Launch this Reporting View – open a new report based on this item

- Add to Search Criteria – apply an additional filter to the current report based on this item

- Go to Vendor Site – go to the web site of the vendor who posted this bulletin

When you rest your mouse over a blue text item, the tool tip tells you what will happen when you click the item.

By default, the reports use Greenwich Mean Time (GMT). Individual report packs can be configured to use either GMT or local time.

Types of Reports

The following types of reports are available in the HPCA Console:

Each is briefly described here.

Inventory Management Reports

Inventory Management reports display hardware and software information for all devices in HPCA. This includes reports for HP specific hardware, device components, blade servers, TPM Chipset information 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. To be included in these reports, devices must be entitled to AUDIT.ZSERVICE.DISCOVER.INVENTORY. Certain data is only available after HPCA is fully configured. Refer to Device Management on page 253 for configuration details.

A typical Managed Devices report includes the following table headings:

- **Details** – opens a Device Summary page for this device.
- **Last Connect** – when the device last connected.
- **HPCA Agent ID** – device name.
- **HPCA Agent Version** – the currently installed Management Agent version.
- **Device** – device name.
- **Last Logged on User** – 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** – device IP address.
- **MAC Address** – device MAC address.
- **Operating System** – operating system installed on the device.
- **OS Level –** current operating system level (for example, Service Pack 2).

Inventory Management Reports consist of the following report options:

- Executive Summaries
- Operational Reports
- Hardware Reports
- Software Reports
- Readiness Reports
- Power Utilization

For more information on these reports refer *HP Client Automation Inventory Manager Reference Guide*.

Settings Management Reports

The Settings Management reports show settings profile information for those devices on which a settings profile has been deployed. A settings profile consists of configuration settings for a specific software installed on a managed device in your environment. Once settings profiles have been created and deployed, it is possible to see summary reports about the software giving administrators visibility to the run-time data of this software.

The Settings Management reports allow you to drill down and see detailed settings profile information by device, profile service ID, and category when you click on individual columns in the provided reports.

Expand the Settings Management reporting view to see the report options. Under Settings Management, there are the following reports:

- **Profile Status by Device** - Displays detailed profile information ordered by device for each device that has the software installed. This report includes profile deployment status for each device and scheduled deployment job information.

- **Profile Status by Service** - Displays detailed profile information ordered by the Profile Service ID of the settings profile. This report includes a description of the service, the number of devices on which the service is deployed, as well as profile deployment status and scheduled deployment job information.

- **Profile Status by Category** - Displays detailed profile information ordered by the type of software. This report allows you to view a list of categories along with profile deployment status and scheduled job deployment information for each category. Categories are broad descriptions of software functionality.

   Examples include HP Power Management, Wireless Settings, and Security settings. Each category may have profiles, which are specific configurations for that category's settings. For example, the HP Power Management category could have power profile settings for Low, Medium, or High.

- **Acquisition Details** - Displays the status of the content updates from HP Live Network.

HPCA Management Reports

The HPCA Management Reports contain management information for various HPCA functions. Expand this view to see the following reporting options:

- **Live Network** - Under this option, you can view the Acquisition History report. It displays a list of acquisition events, the date of each acquisition, acquisition details (allows you to drill down to another report), acquisition sources, and acquisition status.

- **Auditing** - Under this option you can view the Remote Control report. It contains an entry for each remote control session attempted from the HPCA Console to a managed client device.

Patch Management Reports

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

- **Executive Summaries** – Executive Summary reports offer pie or bar charts to provide a visual snapshot of patch-compliance for the devices and bulletins being managed in your environment. The reports summarize compliance for all devices, for devices by patched-state, for bulletins, and bulletins by vendors. From the summary reports you can drill down to the detailed compliance reports which offer additional filtering.

- **Patch Compliance Details** – The HPCA Agent sends product and patch information to HPCA. 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.

- **Acquisition Reports** – Acquisition-based reports show the success and failures of the patch acquisition process from the vendor's web site. They include the following reports:

  — The **Acquisition Summary** report shows the number of bulletins, patches, and errors for each acquisition session. In addition, it provides links to the acquisition reports for all bulletins and patches. The date and time of the publishing session is also listed.

  — The **Acquisition by Bulletin** report shows a summary of the bulletin's acquisition. From this report, you can click on the number for Applicable Patches to see the files associated with the bulletin. Note that one bulletin may have multiple patches based on platform.

  — The **Acquisition by Patch** report shows a summary of each patch's acquisition. You can click on an item in the Product/Release column for a specific bulletin to drill down for full details on the patch. The icon in the Severity column indicates the severity for Windows patches.

- **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.

For details on using the Patch Management reports, refer to Patch Management on page 140.

Usage Management Reports

Usage Management 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.

- **Top 10 Used Products Reports** – Displays the usage for the top 10 products that are used by the User Accounts and the Computer Accounts.

- **Executive Summaries** – Display graphical representation of devices collected and usages by vendor and product.

- **Device Reports** – Display usage specific information such as details of devices and users using the application.

- **Monthly Usage Reports** – Display usage information by vendor, product, and application in a month.

- **Inventory Reports** – Display inventory information by vendor, product, and application.

- **Operational Reports** – Display the number of devices from which data has been collected or has not been collected in last 30 days.

▶ After the Usage 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, and the 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.

Drilling Down to Detailed Information

Many reports enable you to drill down to very detailed information about a particular device, vulnerability, compliance benchmark, or security product.

Whenever you see the Details (🔍) icon in the data grid, you can click it to display more detailed information.

You can also drill down to more detailed information by clicking the device counts in certain columns in some reports.

Filtering Reports

Many reports contain large amounts of data. You can apply one or more filters to a report to reduce the amount of data displayed. If you apply a filter, that filter will remain in effect until you explicitly remove it.

There are three basic types of filters:

- Directory/Group Filters enable you to display data for a specific device or group of devices.

- Inventory Management Filters enable you to display data for a group of devices with common characteristics, such as hardware, software, operating system, or HPCA operational status.

- Report specific filters apply only to data available within a specific Reporting View. For example, Patch Management filters apply only to Patch Management reports.

A filter only works if the type of data that it filters appears in the report.

If you attempt to apply a filter that does not pertain to the data in the current report, the filter will have no effect. Conversely, if the data in a report does not look correct, check to ensure that an incorrect filter has not been applied.

Because they contain small amounts of data to begin with, most Executive Summary reports cannot be filtered.

▶ AUM Admin is not supported in the HPCA Standard Edition. As a result, Usage Rule Filters cannot be created.

To apply a filter to a report

1 In the Data Filters section of the left navigation tree, expand the filter group that you want to use.

2 *Optional*: For the specific filter that you want to apply, click the 🔎 (show/hide) button to show the filter controls:

3 Specify the filter criteria in the text box, or click the 🔎 (criteria) button to select the criteria from a list (if available—not all filters have lists).

You can use wildcard characters when creating filters. The following table describes the characters you can use to build search strings.

Table 21   Special Characters and Wildcards

Character	Function	Device Vendor Filter Example	Records Matched
* or %	Matches all records containing a specific text string	HP*	All records that begin with "HP"
		%HP%	All records that contain "HP"
? or _	Matches any single character	Not?book	All records that begin with "Not" and end with "book"
		Note_ook	All records that begin with "Note" and end with "ook"
!	Negates a filter	!HP*	All records that do not start with "HP"

For example, if you specify HP% in the text box for a device related filter, the filter will match all devices whose Vendor names contain HP.
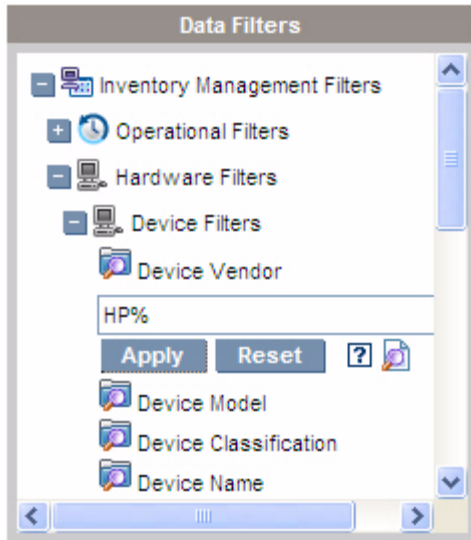
4 Click the **Apply** button. The report will refresh. To remove the filter, click the **Reset** button.

When you apply a filter to a report, the filter is listed in the report header:
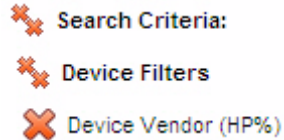
If you apply a filter, that filter will remain in effect until you explicitly remove it. You can click the ✖ (Remove button) to the left of the filter name to remove a filter from the current report.

▶ You can also create an "in-line" filter by clicking a data field in the report currently displayed.

Creating Dynamic Reporting Groups

Dynamic Reporting groups contain devices returned as the result of a reporting query. You can 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, under **Inventory Management Reports**, expand **Operational Reports**, and click **View Managed Devices**.

2 Filter the device list to include only devices you want to include in your group. See Filtering Reports on page 176 for detailed instructions.

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 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 that 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.

8 Operations

The Operations tab allows you to manage infrastructure tasks, view the status of component services, and perform some patch management tasks. Additional details are described in the following sections.

Infrastructure Management

Infrastructure Management operations are described in the following sections:

- Support on page 182
- Database Maintenance on page 186
- Live Network on page 183

Support

The Support area displays the currently installed license information and also allows you to generate and download a compressed (zipped) file that contains configuration files, log files, and operating system information.

See Downloading Log Files on page 182 for details.

These files can then be available for HP Support should they be needed for troubleshooting.

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.

     ▶   Internet Explorer security settings may prevent these files from
          being downloaded. HP recommends adding the HPCA console URL
          to your trusted sites or modifying your Internet Explorer settings to
          not prompt for file downloads.

Live Network

Use the Live Network settings to specify how and when the HP Live Network
content is updated. You can set up a schedule for automatic updates or initiate
an immediate update. You should always perform an update after you install
or upgrade your HPCA software to ensure that you have the most current
content.

Refer to Chapter 5, HPCA and HP Live Network.

Whether you choose to schedule automatic updates or initiate an immediate
update, you must specify the content source for the update. You have the
following choices:

- **From the HP Live Network**

  The live network content source is retrieved from the HP Live Network
  content server and published to the HPCA infrastructure. By default, this
  path is:

  `<InstallDir>\LiveNetwork\lnc\bin\live-network-connector.bat`

  This path is configured automatically by HPCA. You do not need to specify
  this path unless you have downloaded a new copy of the HP Live Network
  Connector and installed it in a different location.

  To use this option, you must have an active HP Live Network
  subscription. This is not included in your HPCA software. See your HP
  representative for details.

- **From the File System**

  A copy of the live network content is published from a location in the file
  system on the system where the HPCA Core is installed. You must specify
  the path name of the folder that contains the content, and you must
  manually download these items from the HP Live Network content server
  before you can initiate an update.

The folder structure from the file system location specified must exactly match the folder structure that is created when the HP Live Network Connector downloads content, as shown here:

📁 bundles
📁 definitions
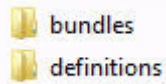
The subdirectories under each of these folders must also match exactly.

In some cases, HP Live Network updates only a subset of the content. In this case, some of these directories may not be delivered during a Live Network update.

Schedule Automatic Live Network Updates

Use the following procedure to establish a schedule for automatic HP Live Network updates from the content source of your choice.

To schedule automatic HP Live Network content updates

1 On the Operations tab, expand the Infrastructure Management area, and click **Live Network**.

2 Click the **Schedule Updates** tab.

3 In the Updates section, select the content source.

4 Specify the schedule for automatic updates:

   a **Schedule**—Select Once, Hourly, Daily, Weekly, or None

      None is what the HPCA Console shows when nothing is currently scheduled to execute—for example, when a previously scheduled Once task has already completed. You can specify None if you do not want to schedule anything new or if you want to stop an existing schedule. If there is a recurring schedule, the most recently saved schedule is shown (for example, Hourly, Daily, or Weekly).

   b **Start Time**—Time of day to start the updates.

   c **Start Date**—Date to start the automatic updates. Click the 🗓 (calendar) button, and select the date.

When the **Schedule Updates** tab is displayed, the time and date fields show the time and date of the last saved schedule. For example, if a previously scheduled Once update has already completed, the Schedule will be set to None, and you can see the time and date of the last update in the Start Time and Start Date fields.

d   If you selected Hourly, Daily or Weekly for the **Schedule**, specify the update interval in the **Every** box.

For example, if you select Daily, with an **Every** interval of two, this will run an update every two days.

5   Click **Save** to implement your changes.

▶   If you leave this tab, any information that you entered prior to clicking **Save** will be lost. Be sure to click **Save** if you want to keep this information.

▶   You can use the Reset button to restore the most recently saved settings.

Update the HP Live Network Content Now

Use the following procedure to update your HP Live Network content now. This does not affect any schedule that you have established for automatic updates.

To update the HP Live Network content immediately

1   On the **Operations** tab, expand the **Infrastructure Management** area, and click **Live Network**.

2   Click the **Update Now** tab.

3   Select the content source for this update. This will not affect any automatic updates that are currently scheduled.

4   Click the **Update Now** button. A request is issued to update your content from the content source that you specified.

An update is an asynchronous process that requires some time to complete. You can use the acquisition reports to view the results of an update or check its status.

View the Results or Status of an Update

You can use the HPCA reports to check on the status of an HP Live Network content update. You can access the reports that display this information in one of the following ways:

- Click the **Reporting** tab from **Operations** > **Infrastructure Management** > **Live Network**. This is the most convenient way to view the status of the content updates from this location.

- Click the **Reporting** tab in the HPCA Console. Go to **HPCA Management** > **Live Network** > **Acquisition History**.

Database Maintenance

The Database Maintenance area shows all of the devices that have reporting data stored in HPCA. Use the Maintenance toolbar to clean up reporting data for devices that may no longer be in your database.

To remove device reporting data

1   In the Maintenance area, select the devices for which you would like to remove reporting data.

2   Click the Delete Reporting Data ✖ button.

3   The reporting data is removed from your database.

    After reporting data is removed for a device, the data is not 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.

Software Management

Use the Software Management tools on the Operations tab to manage the catalog of software services (applications) that are available to be deployed to managed client devices. After a software service is added to the HPCA

software library, end-users of the client devices can install, update, or remove software to which they are entitled by Using the Application Self-Service Manager.

The Software Library page lists the software services that have been published into HPCA. You can use the tools on this page to import, export, or delete software services. The import and export tools are useful for moving a software service from one HPCA server to another—for example, if you want to move a service from a test environment to a production environment

To view or modify settings for a particular software service, see the Software Details Window (Operations Tab) on page 189.

Table 22   Software Library Tools

Button	Description
	Refresh Data – Refreshes the data in the Software Library table.
	Export to CSV – Creates a comma-separated list of software services that you can open, view, and save.
	Import Service – Imports a software service into HPCA. See Import a Software Service on page 188. After you import a software service, you can entitle groups or specific managed client devices to that service. You can then deploy the service to those devices.
	Export Service – Exports a published software service in a binary file format called a **service deck**. See Export a Software Service on page 188. After you export a software service, you can copy the service deck to another HPCA server, and then import the service there.
	Delete Software – Remove the selected service (or services) from the HPCA Software Library. See Delete a Software Service on page 189.

Import a Software Service

HPCA can import software services into the Software Library. To import a service, the service import deck must be located in the ServiceDecks directory on your HPCA server. By default, this directory is:

<InstallDir>\Data\ServiceDecks

This is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to the ServiceDecks directory on your production HPCA server (see Export a Software Service). Then use the Import Service wizard to import that service to your production Software Library, and deploy it to managed devices.

To import a service

1   Click **Import Service** 🖱 to launch the Service Import Wizard.

2   Follow the steps in the wizard to import the service into the Software Library.

▶   Only those services in the ServiceDecks folder that contain the word SOFTWARE in their names are available for import. For example:

PRIMARY.SOFTWARE.ZSERVICE.ORCA

Export a Software Service

Published software services can be exported to the ServiceDecks directory on your HPCA server. By default, this directory is:

<InstallDir>\Data\ServiceDecks

Exported services can be copied to any other HPCA server and then imported into that server's Software Library (see Import a Software Service).

To export a service

1   Select the check box in the first column to select the software to export as a service.

2   Click **Export Service** 🖱 to launch the Service Export Wizard.

3   Follow the steps in the wizard to export the service to the `ServiceDecks` directory on your HPCA server machine.

Delete a Software Service

Use the Software toolbar to remove software from the HPCA Software Library. This deletes the software service and removes any entitlements to that service.

To remove software from the Software Library

1   Select the software service (or services) that you want to remove.

2   Click the **Delete Software** ✖ button.

Software Details Window (Operations Tab)

Click the Service ID of any software service in the Software Library to open the Software Details window. Use the Software Details window to view or modify settings for a particular software service.

The following settings are available in the Software Details window:

- **Display Name**
  Name of this software service. This is the "friendly" name that is used in the HPCA console. This is a required field.

- **Software Category**
  Specify a category that will help define the type of software. The Software Category is displayed in the Software Library and is available as a sort option.

- **Catalog Visibility**
  Specify whether to display the software in the catalog on the managed client device. Displaying software in the catalog allows the end user to install, update, or remove the software.

- **Reboot Settings**
  Specify whether a reboot is required for the managed client device after the software is installed, and whether to prompt the end-user for the reboot.

- **Author**
  The software author (for example, Hewlett-Packard).

- **Vendor**
  The software vendor (for example, Hewlett-Packard).

- **Web Site**
  An informational URL for the software.

- **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.

- **Install Command Line**
  Command to run to install the software.

- **Un-install Command Line**
  Command to run after the software is removed from a device.

▶ Be sure to click **Save** after making any changes to the software settings.

▶ When you open the Software Details window from the Management tab, these settings are displayed in read-only format. To modify the settings for a service, be sure to open the Software Details window from the Operations tab.

Additional functions are available, however, when you open the Software Details window from the Management tab. See Software Details Window (Management Tab) on page 131.

Out of Band Management

Out of Band (OOB) Management is enabled using the Configuration tab. See Configuration on page 215 for OOB Management settings and Preferences.

For additional information on using OOB Management refer to the *HP Client Automation Out of Band Management User Guide.*

The following sections describe the OOB Management tasks available in the console:

- Provisioning and Configuration Information on page 191

- Device Management on page 192

Provisioning and Configuration Information

Your vPro and DASH devices must be provisioned before you can discover and manage them. It is possible to provision vPro devices through the HPCA console if the devices did not automatically become provisioned when originally connected to the network.

The provisioning of vPro devices through the HPCA console is described in Setting Up vPro and DASH Devices chapter of the *HP Client Automation Out of Band Management User Guide.* This option does not appear on the Operations tab under Out of Band Management if you have selected to manage DASH devices only since it is not relevant for this type of device.

Refer to the Setting Up vPro and DASH Devices chapter of the *HP Client Automation Out of Band Management User Guide* for complete details.

DASH Configuration Documentation

Provision DASH-enabled devices according to the documentation accompanying the device. For DASH-enabled devices from Hewlett-Packard, DASH configuration information is documented in the "Broadcom NetXtreme Gigabit Ethernet Plus NIC" whitepaper.

To access this documentation

1 Go to **www.hp.com**.

2 Select **Support and Drivers** > **Product Support and Troubleshooting**.

3 Enter a product that supports this NIC, for example, the dc7900.

4 Select one of the dc7900 models.

5 Select **Manuals (guides, supplements, addendums, etc)**.

6 Scroll to the White papers section and select **Broadcom NetXtreme Gigabit Ethernet Plus NIC** whitepaper.

DASH Configuration Utilities

The DASH Configuration Utility (BMCC application) is part of the Broadcom NetXtreme Gigabit Ethernet Plus NIC driver softpaq, which is found in the drivers section for each product that supports this NIC.

To access this utility

1   Go to **www.hp.com**.

2   Select **Support and Drivers** > **Drivers and Software**.

3   Enter a product that supports this NIC, for example, the dc7900.

4   Select one of the dc7900 models.

5   Select an operating system.

6   Scroll to the Driver-Network section and select to download the **Broadcom NetXtreme Gigabit Ethernet Plus NIC Drivers**.

Device Management

The Device Management area allows you to manage multiple OOB devices.

On the Operations tab, under Out of Band Management, click **Device Management**. The Device Management window opens. Using the icons on the toolbar of the device table, you can perform the following tasks on multiple devices:

• Refresh data

• Reload device information

• Discover Devices

• Power on and off and reboot devices

• Subscribe to vPro alerts

• Manage common utilities on vPro devices

• Deploy System Defense policies to selected vPro devices

• Deploy heuristics worm containment information to selected vPro devices

• Deploy agent watchdogs to selected vPro devices

• Deploy agent software list and system message to selected vPro devices

Click the hostname link in the device table to manage an individual OOB device. A management window opens that has several options in its left navigation pane. The options available are dependent on the type of device you selected to manage.

Refer to the Device Management chapter of the *HP Client Automation Out of Band Management User Guide* for complete details.

Groups Management

The Groups Management option allows you to manage groups of vPro devices as defined in the Client Automation software. You can perform OOB operations on Client Automation groups that contain vPro devices. You can manage groups of vPro devices to perform various discover, heal, and protect tasks. These include power management, alert subscription, and deployment of System Defense policies, agent watchdogs, local agent software lists, and heuristics.

On the **Operations** tab, under Out of Band Management, click **Group Management**. The Group Management window opens. From the icons on the toolbar of the group table, you can perform the following tasks on multiple groups:

- Refresh data
- Reload group information
- Power on and off and reboot groups
- Subscribe to vPro alerts
- Deploy agent software list and system message to selected vPro groups
- Provision vPro device groups
- Deploy and undeploy System Defense policies to selected vPro devices
- Deploy and undeploy agent watchdogs to selected vPro groups
- Deploy and undeploy heuristics worm containment information to selected vPro groups

To drill down to manage individual devices within a group, click the group name link under the Description column of the table. The Device Management window opens displaying a list of devices belonging to the selected group. You can manage multiple or individual devices within the group. See Managing Devices.

Refer to the Group Management chapter of the *HP Client Automation Out of Band Management User Guide* for complete details.

Alert Notifications

For vPro devices, you can view the alerts generated by provisioned vPro devices if you have an alert subscription to the device. Monitoring alert notifications gives you a good idea of the health of the devices on your network.

Refer to the Alert Notifications chapter of the *HP Client Automation Out of Band Management User Guide* for complete details.

Patch Management

Use the Patch Management tools on the Operations tab to manage the catalog of patch bulletins that are available to be deployed to managed devices.

Patch Library Operations

The Patch Library page lists the bulletins that have been published into HPCA. You can use the tools on this page to import, export, or delete bulletins. The import and export tools are useful for moving a patch from one HPCA server to another—for example, if you want to move a patch from a test environment to a production environment.

▶ To view or modify settings for a particular patch, see the Patch Details Window (Operations Tab) on page 197.

Table 23   Patch Library Tools

Button	Description
⟳	**Refresh Data** – Refreshes the data in the Patch Library table.
📝	**Export to CSV** – Creates a comma-separated list of patches that you can open, view, and save.
📥	**Import Service** – Imports a patch into HPCA. See Import a Patch Service on page 195. After you import a patch, you can entitle groups or specific managed client devices to that service. You can then deploy the patch to those devices.
📤	**Export Service** – Exports a published patch in a binary file format called a **service deck**. See Export a Patch Service on page 196. After you export a patch, you can copy the service deck to another HPCA server, and then import the patch there.
✖	**Delete Patch** – Remove the selected patch (or patches) from the HPCA Patch Library. See Delete a Patch Service on page 197.

Import a Patch Service

HPCA can import patches into the Patch Library. To import a patch, the decks (namely, the xpi, xpc, and xpr files) and the zip file must be placed in the ServiceDecks directory on your HPCA server. Also, copy the PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* files. These contain the catalog and the Agent information. If these files are not copied, or if they are old files, the import of bulletins will fail with the message - "Import Failed - Ensure the bulletin is exported recently and latest PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.* files are copied."

By default, this directory is:

<InstallDir>\Data\ServiceDecks

This is useful if you have created a testing environment. When you have approved a particular patch in your test environment, export that bulletin to the ServiceDecks directory on your production HPCA server (see Export a Patch Service). Then use the Import Service wizard to import that patch to your production Patch Library, and deploy it to managed devices.

To import a patch service

1   Click **Import Service** 📤 to launch the Service Import Wizard. This
    displays a list of the `xpi` files present in the `ServiceDecks` directory.

2   Follow the steps in the wizard to import the service into the Patch
    Library.

▶   `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi` need not be
    explicitly selected. They are implicitly selected when a bulletin is selected for
    import. If only the agent or catalog files need to be moved to the target server,
    then `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi` can be
    selected.

Export a Patch Service

Published bulletins can be exported to the `ServiceDecks` directory on your
HPCA server. By default, this directory is:

`<InstallDir>\Data\ServiceDecks`

To export a patch service

1   Select the check box in the first column to select the bulletin(s) to export
    as a service. Use the grid options to search for bulletins based on type,
    name, and so on.

2   Click **Export Service** 📤 to launch the Service Export Wizard.

3   Follow the steps in the wizard to export the bulletin(s) to the
    `ServiceDecks` directory on your HPCA server machine.

    This creates the following files for each exported bulletin in the
    `ServiceDecks` directory of your server:

    • `PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].xpi`

    • `PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].xpr`

    • `PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].xpc`

    • `PRIMARY.PATCHMGR.ZSERVICE.[BULLETIN NAME].zip`

    • `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpi`

- `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpr`

- `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.xpc`

- `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.zip`

For the metadata-based patch distribution model, the zip file contains the binaries that are present in the gateway cache and some of the metadata information. These binaries are also moved to the target server during the export/import operation. The Agent and Catalog information are present in the `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.*` files. These files also need to be moved explicitly to the target machine. Exporting a service automatically exports the latest agent, catalogs, and other related files that are needed for the discover process.

For import, all of the files with the `PRIMARY.PATCHMGR.ZSERVICE.`*`[BULLETIN NAME]`* stem along with `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH.*` should be copied to any other HPCA server and then imported into that server's Patch Library. See Import a Patch Service on page 195.

Delete a Patch Service

Use the Patch Library toolbar to remove patches from the HPCA Patch Library. This deletes the patch and removes any entitlements to that patch. This also cleans up any related binaries in the gateway cache.

To remove a patch from the Patch Library

1   Select the patch (or patches) that you want to remove.

2   Click the **Delete Patch** ✖ button.

Patch Details Window (Operations Tab)

Click the Bulletin name for any patch in the Patch Library to open the Patch Details window. Use the Patch Details window to view the following properties of a particular patch:

- **Bulletin Type**
  Type of patch (for example, Security Updates).

- **Vendor**
  The software vendor (for example, Microsoft).

- **Bulletin**
  Bulletin name assigned by the vendor. Typically a sequential code.

- **Description**
  Any descriptive text that the vendor has included with the bulletin.

- **Vendor Posted**
  Date this bulletin was originally posted by the vendor.

- **Vendor Revised**
  Most recent date that this bulletin was revised by the vendor.

- **Bulletin Information**
  URL for information about this bulletin on the vendor's web site.

- **Other Information**
  URL for any related information on the vendor' web site.

▶ The information displayed in this window is read-only and cannot be modified.

▶ Additional functions are available when you open the Patch Details window from the Management tab. See Patch Details Window (Management Tab) on page 145.

Acquisition

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 tab.

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 HPCA server.

2   When finished, click **Save** to commit your changes.

The new schedule is displayed after **Current Schedule**.

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 (*).

1   Complete the **Microsoft Bulletins** area.

   — In the **Enabled** drop-down list, select **Yes** to acquire Microsoft Bulletins.

   ▶   Patch Management using Metadata is enabled by default for Microsoft Patches. This feature reduces the time it takes to acquire patches and the overall load on the Core Configuration Server. For details, see Chapter 11, Patch Management Using Metadata.

   — 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 24   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	

— In the **Force** drop-down list, select **Yes** in the following situations:

– You previously ran an acquisition filtering for one language, and now you need to acquire bulletins for another language.

– You previously ran an acquisition specifying one product, and now you need to acquire the same bulletins for another product. For example, if you originally had only Windows 2000 computers on your network and acquired the bulletins for that operating system, but now you also have Windows XP computers and want to acquire the same bulletins for the new operating system, you will need to run the acquisition again for product {Windows XP*,Windows 2000*} with **Force** set to **Yes**. Note that **No** is the default value for this option.

— In the **Replace** drop-down list, select **Yes** to delete old bulletins specified in the bulletins parameter, and then re-acquire them. This option will supersede the value specified for the **Force** option. In other words, if you set **Replace** to **Yes**, then any bulletin specified for that acquisition will be deleted and reacquired whether **Force** is set to **Yes** of **No**.

— In the **Architecture** drop-down list, select the architectures for the acquisition of Microsoft patches. The supported architectures include:

– x86 for 32-bit Intel architectures

– x64 for AMD64 or Intel EM64T

– x86 and x64 for 32-bit Intel architectures and AMD64 or Intel EM64T

2   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 HPCA.

3   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.

4   Click **Save** to apply your changes.

▶   Initial patch acquisition may take an extended period of time.

To see the status of current and past Acquisition Jobs, go to the **Operations** tab, **Patch Management** area, **View Acquisition Jobs** page.

Perform Synchronization

This operation synchronizes the patch information stored in the Patch Library with the patch information in the SQL database.

This synchronization occurs automatically after a patch acquisition and in normal HPCA operations.

However, there may be times when you are directed by customer support to run the synchronization manually.

You can synchronize the databases manually using the HPCA Core Console.

To synchronize the databases

1   From Operations tab, expand the **Patch Management** tasks, and click **Perform Synchronization**.

2   Click **Submit**.

Acquisition History

Select a patch acquisition status page to view details from previous acquisitions.

OS Management

Use the OS Management tools on the Operations tab to manage the catalog of operating systems that are available to be deployed to managed devices.

The OS Library page lists the operating systems that have been published into HPCA. You can use the tools on this page to import, export, or delete operating systems. You can also create a deployable CD (or DVD) for any operating system in the library.

The import and export tools are useful for moving an operating system from one HPCA server to another—for example, if you want to transfer an OS from a test environment to a production environment

▶ To view or modify settings for a particular operating system, see the OS Details Window (Operations Tab) on page 206.

Table 25   OS Library Tools

Button	Description
![refresh icon]	**Refresh Data** – Refreshes the data in the OS Library table.
![export icon]	**Export to CSV** – Creates a comma-separated list of operating systems that you can open, view, and save.
![import icon]	**Import Service** – Imports an operating system into HPCA. See Import an OS Service on page 203. After you import an operating system, you can entitle groups or specific managed client devices to that OS. You can then deploy the OS to those devices.
![export service icon]	**Export Service** – Exports a published operating system in a binary file format called a **service deck**. See Export an OS Service on page 204. After you export an operating system, you can copy the service deck to another HPCA server, and then import the OS there.
![create cd icon]	**Create CD Deployment Media** – Downloads OS images that you can then burn to a DVD for operating system deployment. See Create Deployment Media on page 205.
![delete icon]	**Delete OS** – Remove the selected operating systems from the HPCA OS Library. See Delete an OS Service on page 204.

Import an OS Service

HPCA can import operating systems into the OS Library. To import a service, the service import deck must be located in the ServiceDecks directory on your HPCA server. By default, this directory is:

```
<InstallDir>\Data\ServiceDecks
```

This is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to the ServiceDecks directory on your production HPCA server (see Export an OS Service). Then use the Import Service wizard to import that service to your production OS Library, and deploy it to managed devices.

To import a service

1 Click **Import Service** 🛠 to launch the Service Import Wizard.

2 Follow the steps in the wizard to import the service into the OS Library.

▶ Only those services in the ServiceDecks folder that contain the word OS in their names are available for import. For example:

PRIMARY.OS.ZSERVICE.WIN732

Export an OS Service

Published operating systems can be exported to the ServiceDecks directory on your HPCA server. By default, this directory is:

<InstallDir>\Data\ServiceDecks

Exported services can be copied to any other HPCA server and then imported into that server's OS Library (see Export an OS Service).

To export a service

1 Select the check box in the first column to select the OS to export as a service.

2 Click **Export Service** 🛠 to launch the Service Export Wizard.

3 Follow the steps in the wizard to export the service to the ServiceDecks directory on your HPCA server machine.

Delete an OS Service

Use the OS toolbar to remove OS from the HPCA OS Library. This deletes the operating system and removes any entitlements to that service.

1 Select the operating system (or services) that you want to remove.

2 Click the **Delete OS** ✖ button.

Create Deployment Media

You can use the Create CD Deployment Media tool to download images that can then be burned to a DVD for operating system deployment.

The OS Library lists all operating systems that have been published to HPCA.

1 On the Operations tab, go to **OS Management** > **OS Library**.

2 Select an operating system from the OS Library.

3 Click the **Create CD Deployment Media** 🖥 button to launch the CD Deployment Wizard.

4 Review the summary information, and click **Download**. The OS image begins to download in the background.

5 Click **Close**.

View the download progress in the OS Library. Click the **Refresh** 🔃 button to see the current status in the CD Creation Status column.

When the download is complete, the OS image is stored, by default, in:

    <InstallDir>\Data\ServiceDecks\CDDeployment

If this directory is empty, the CD Creation Status column is blank for all operating systems listed.

▶ This feature is intended for use with DVDs, typically to store multiple images. Do not span your resources over multiple CD-ROMs or DVD-ROMs.

⚠ Your DVD-ROM must be in Joliet format.

OS Details Window (Operations Tab)

Click the Service ID of any operating system in the OS Library to open the OS Details window. Use the OS Details window to view or modify settings for a particular operating system.

The following settings are available in the OS Details window:

- **Display Name**
  The name of the OS that appears on the OS Library page. This is a required field.

- **Author**
  The OS author.

- **Vendor**
  The OS vendor.

- **Web Site**
  An informational URL for the OS.

➤ Be sure to click **Save** after making any changes to the OS settings.

➤ When you open the OS Details window from the Management tab, these settings are displayed in read-only format. To modify the settings for a service, be sure to open the OS Details window from the Operations tab.

Additional functions are available, however, when you open the OS Details window from the Management tab. See OS Details Window (Management Tab) on page 157.

Usage Management

Use the Usage Management section to configure usage collection filters.

Collection Filters

Use the Collection Filters page to create and manage usage collection filters.

▶ HP Client Automation Standard or HP Client Automation Enterprise is required to collect 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 then sent to HPCA.

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 HPCA 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 HPCA based on the schedule that you defined. Then, in June you decide to create and enable a new filter for Microsoft Excel. The next time that usage data is sent to HPCA, 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 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 207
- Defining Usage Criteria on page 209

See the Application Usage Collection Wizard to deploy the Usage Collection Agent and define a collection schedule.

Configuring Usage Collection Filters

HPCA 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.

Use the Usage Collection Filter Creation Wizard to create new usage collection filters. Use the Filter Details window to modify existing filters.

⚠️ 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. HP strongly recommends that you create filters to collect data only for those applications that you want usage information for. Avoid collecting usage data for all applications.

To create a collection filter

1 On the Collection Filters page, click the **Create New Filter** toolbar button. This launches the Usage Collection Filter Creation Wizard.

2 Follow the steps in the wizard to create and enable the new collection filter.

To enable collection filters

1 In the Filter list, select the filters that 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 **OK** to enable the selected filters. A status dialog shows you the result.

4 Click **Close** to close the status dialog.

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 209 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 file to determine whether that application meets defined filter criteria. You can use the file header information to determine what criteria to use when defining a filter.

To determine file header information

1   Right-click an executable file on your system.

2   Select **Properties** from the shortcut menu.

3   On the Properties window, click the **Version** tab.
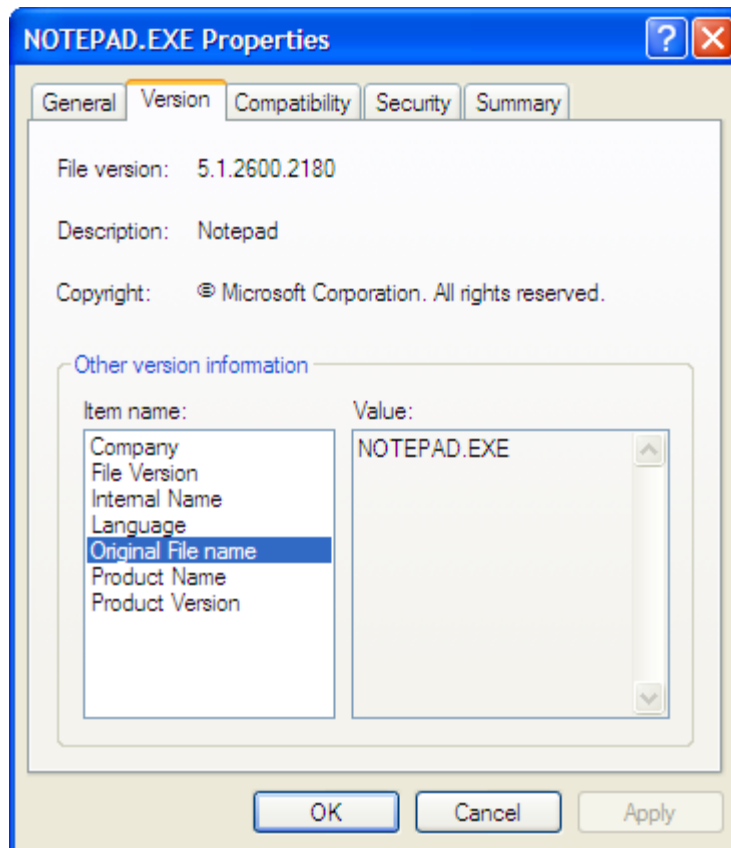
The information contained in the **Item name** and **Value** boxes is used by the Usage Collection Agent to filter the available usage data (with the exception of the Language and Internal Name items, which are not currently supported).

▶ 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 one or more managed devices. See Application Usage Collection Wizard on page 307 for instructions.

Usage data will be sent to HPCA weekly and will include all usage data for Notepad for all devices that have the Usage Collection Agent installed.

Settings Management

Use the Settings Management section to create, modify, and delete settings profiles. Settings profiles allow you to create groups of configuration settings for software installed on the managed devices in your environment. A settings profile consists of customized configuration settings for devices, which include settings related to applications, operating systems, and hardware. By creating or modifying a settings profile, you can analyze and parameterize configuration control data for targeted products.

Once you create and/or modify settings profiles, they can be deployed to the targeted systems where the relevant software is installed. In HPCA Standard, Settings Profiles must be deployed to targeted machines by using the **Settings Management** area on the Management tab of the console. See Settings Management on page 136.

Once settings profiles have been created and deployed, it is possible to see summary reports about the software giving administrators visibility to the run-time data of this software. See Settings Management Reports on page 172.

This section covers the following topics:

- Settings Templates on page 211
- Creating New Profiles on page 211
- Modifying Existing Profiles on page 213
- Deleting Profiles on page 213

Settings Templates

Settings templates are used to create instances of settings profiles. You can download the most current content for settings templates from the HP Live Network site. See HPCA and HP Live Network.

You can select any of the provided settings templates to create additional profiles or to modify existing ones. The Operations tab in the HPCA Console provides a **Settings Templates** area under Settings Management that allows you to see the software on your system that has configurable profiles.

Creating New Profiles

You can create additional profiles for the software on your system with configurable profiles. Settings templates are provided for this purpose. The template is used to create a settings profile instance for the relevant software. You can start with a blank profile or you can clone an existing one if it is similar to the one you want to create, thus making the procedure easier to perform.

1   On the Operations tab, expand Settings Management in the left
    navigation pane and click the **Settings Templates** link. Software with
    configurable profiles will be displayed in the content area on the right.

2   In the **Display Name** column, click the name of the software for which you
    want to create a new profile. A window opens that contains the following
    tabs:

    — Profiles: Displays the existing profiles for the selected software. On
      this tab, you can create, view, modify, and delete settings profiles.
      Profile names displayed with angle brackets (< >) surrounding them
      are HP-supplied profiles.

      ▶ Be aware that if you modify these profiles, your changes can be lost
         the next time you update your settings content from the HP Live
         Network site.

    — Details: Displays information about what the template does and how
      to use it.

3   On the Profiles tab, click **Create a New Profile** 📝 on the toolbar in the
    Settings Profiles table. The Settings Profile Creation Wizard opens.

    Alternatively, you can check the box next to an existing profile that you

    want to copy and click **Copy the Selected Profile** 📋 . The Copy and Modify
    Settings Profile Wizard opens in this case. This wizard allows you to clone
    the selected existing profile. If you select to copy an existing profile, all
    fields, except for the profile Display Name, will be populated with the
    values contained in the selected existing profile.

4   In either wizard, specify the following information:

    — **Display Name**: Type a name for the profile

    — **Description**: Type a description for the profile

5   Click **Next**. The next page of the wizard opens which allows you to enter
    properties specific to the particular software. In the case of copy, these
    fields will be pre-populated. Modify these fields as necessary.

    Refer to the documentation for the given software to better understand
    the relevant property settings.

6   Click **Create** or **Copy** depending on the wizard. The newly created profile is listed in the Settings Profiles table on the Profiles tab. The number of profiles in the Operations area is also updated to reflect the latest addition.

Modifying Existing Profiles

Property settings for software with configurable profiles can be viewed and modified.

To modify a settings profile

1   On the Operations tab, expand Settings Management in the left navigation pane and click the **Settings Templates** link. Software with configurable profiles will be displayed in the content area on the right.

2   In the **Display Name** column, click the name of the software that has a profile that you want to modify. A window opens displaying the existing profiles for the selected software on the Profiles tab.

3   On the Profiles tab in the **Display Name** column, click the name of the profile that you want to modify. A window opens with Summary and Properties tabs displaying all of the properties for the selected profile.

4   Modify the property values on both tabs as necessary.

5   Click **Save** to save your changes.

Deleting Profiles

Settings profiles can be deleted for software when they are no longer needed.

To delete a settings profile

1   On the Operations tab, expand Settings Management in the left navigation pane and click the **Settings Templates** link. Software with configurable profiles will be displayed in the content area on the right.

2   In the **Display Name** column, click the name of the software that has a profile that you want to delete. A window opens displaying the existing profiles for the selected software on the Profiles tab.

3   On the Profiles tab, check the box next to the profile name(s) that you
    want to delete.

4   Click **Delete Selected Profile(s)** on the toolbar. A pop-up confirmation
    window opens.

5   Click **Yes** if you want to continue. A window opens displaying the status of
    the operation.

6   Click **Close** to exit the status window. The deleted profiles are no longer
    listed in the Settings Profiles table for the given application. The number
    of profiles in the Operations area is updated to reflect the latest deletion.

9 Configuration

The Configuration area allows you to manage user access to the Console, define and configure infrastructure servers, manage patch acquisition schedules and settings, manage hardware, and configure ODBC settings.

▶ The Configuration tab is available only to users that belong to the Administrator roles group.

Use the links in the navigation area on the left side of the Configuration tab to access the various configuration options. These options are described in the following sections:

Core Configuration Options

Satellite Configuration Options

Licensing

A functional HPCA environment requires a valid HP-issued license. This area of the Console stores your license file and displays the license edition (Starter, Standard, or Enterprise) that is installed. You can use this section to review and update your HPCA license.

To apply a new license

1   Copy and paste the license information from your new `license.nvd` file into the **License Data** text box.

    ▶   When copying the license information from your license file, do not include the text that precedes the line `[MGR_LICENSE]` because this will result in the license information not being "readable" to the Console.

2   Click **Save**. Updated license information is displayed after **Current License**.

Upstream Server

On a Satellite console, use the Configuration tab **Upstream Server** area to edit the upstream host server information. The upstream server is the server this Satellite will synchronize with, as well as fetch information for requests if a service is disabled or a resource is unavailable. You may use SSL for this inter-server communication; the upstream server must be capable of receiving SSL requests.

Access Control

This panel offers different administrative controls depending on whether you are in the Core or Satellite Console.

- Access Control on the Core Console allows HPCA administrators to configure and manage user access to the Console. For more information, see Core Console Access Control on page 217.

- Access Control on the Satellite Console allows HPCA administrators to select and configure an authentication method. For more information, see Satellite Console Access Control on page 221.

Core Console Access Control

Use the Access Control section to create instances of internal **users** with unique custom IDs and passwords. Then, assign **roles** (see Roles Panel on page 219) to the users in order to manage the areas of Console that the users can access, as well as the administrative tasks for which they are authorized.

Users Panel

In the Users panel, create user instances and assign a role to each. The role determines which areas of the Console each user can access.

Management jobs contain a **Creator** field that displays the user ID under which a job is created. It is the user IDs that are created in this area that will be displayed.

- During installation, a default user, **admin**, exists with the default password of **secret**. This "failsafe" user account has full access to the Console and cannot be deleted.

- HPCA users in Console can be either **internal** or **external**, as described below.

  — **Internal**
    All users that you create in the Users panel are "internal". You can delete and update these users from the Core Console.

  — **External**
    In the Enterprise edition, HPCA administrators have the option of leveraging external directories (such as LDAP and Active Directory) to

add users and configure their access permissions and credentials. You cannot create, delete, or update these "external" users from the Core Console; an administrator must use the LDAP/AD tools in order to do so. An HPCA administrator can, however, configure a directory source for authentication. This source appears in the **Users** panel and the **Source** column references the directory from which the user originated.

The Users panel enables you to perform the following administrative tasks. All administrative tasks can be performed on internal users at the core console. For external users, only roles can be assigned at the Core Console.

- Managing a User on page 218

- Assigning Roles on page 220

Managing a User

You can perform the following tasks to manage a user:

- Create an internal user (as descibed in To Create an Internal User on page 218).

- View and change an internal user's properties (as described in To View and Modify User Properties on page 219).

- Delete an internal user (as described in To Delete an Internal User on page 219).

- Assign a role to a user (as described in the section, Roles Panel on page 219). You can assign more than one role to a user.

- Remove a role from a user (as described in the section, Roles Panel on page 219).

To Create an Internal User

1   Click **Create a New User** to launch the User Creation Wizard.

2   Specify values for the following fields:

— ID: Specify the unique identifier for the internal user. Use alphanumeric characters (A-Z, a-z, and 0-9). You can also use underscore (_).

— Display Name: Specify display name for the user.

— Description: Specify a description for the user. This is an optional field.

— Password: Specify a password for the user. Use only ASCII characters when creating passwords.

➤ If you change the password for the *current user*, you will be logged out automatically. Log in as the user with the new password.

— Confirm Password: Type the password again.

3   Click **Create**.

1   Click an internal user's ID to view its properties.

2   In the User Properties window, modify the user's properties, such as the display name and description, and access the Change Password window.

3   Click **Save** to confirm and preserve any changes.

Select the internal user's ID from the list and click **Delete the Selected User(s)** .

➤ The *current user* cannot be deleted.
In order to delete this ID, you must log out and then log in as a different Administrator to execute the deletion.

Roles Panel

There are various levels of administrative authority (**roles**) that can be assigned to users. Assign a role to a user based on the access and management-permissions that you want available to the user. The user roles in Console are:

• **Administrators**: These users have unlimited access to the Core Console, as well as the ability to perform all administrative functions. This is a "superset" role; it encompasses all of the functionality and authority of the Operator and Reporter roles.

- **Operators**: These users can perform management, operational, and reporting-related tasks in the Core Console. They cannot access the Configurations tab. This role encompasses the functionality and authority of the Reporter role.

- **Reporters**: These users' can view, compile, and print reporting data in the Core Console. Their access is limited to the Reporting and Dashboards tabs.

> You can assign more than one role to a user.

The Roles panel enables you to perform the following tasks:

-

Assigning Roles

To Assign a Role to a User

You can assign a role to a user in either of two ways in the Console:

- Using the Roles panel:

  a   Click a role in the table to invoke the Role Properties window.

  b   Click **Users** tab; this tab displays a list of the users that have been assigned this role.

  c   To assign user to the role, click **Add User(s) to this Role** . The User Selection window opens.

  d   Select user and click **Assign**. The refreshed ID column displays the remaining users that can be assigned this role.

  e   Click **Close** to return to the Role Properties window. The **Users** tab displays refreshed list of the users that have been assigned this role.

- Using the Users panel:

  a   Click an ID in the table to invoke the User Properties window.

  b   Select the **Roles** tab; this tab displays the roles currently assigned to the user.

  c   Click **Add Role(s) to this User** to launch the Role Selection window.

d   Select a role to assign to the user and click **Assign**. The refreshed Role column displays the remaining roles available to be assigned to a user.

e   Click **Close** to return to the User Properties window. The Roles tab displays all the roles currently assigned to the user.

To Remove a Role from a User

You can remove roles from a user in either of two ways in the Console:

- Using the Roles panel:

  a   Click a role in the table to invoke the Role Properties window.

  b   Select **Users** tab; this tab displays a list of the users that have been assigned this role.

  c   To delete user from the role, select user and click **Remove the Selected User(s) from this Role** . The refreshed ID column displays the remaining users that have been assigned this role.

- Using the Users panel:

  a   Click an ID in the table to invoke the User Properties window.

  b   Select the **Roles** tab; this tab displays the roles currently assigned to the user.

  c   To delete role from the user, select role and click **Remove Selected Role(s) from this User** . The refreshed Role column displays the roles currently assigned to the user.

Satellite Console Access Control

The Access Control section of the Satellite Console allows an HPCA administrator to select a Console-access authentication method (**Local Accounts** or **Directory Service Accounts**) and to configure its settings.

The Summary area of the Access Control section displays the Authentication Method that is currently enabled. The default (Local Accounts) is displayed.

To select and configure an authentication method

1   Click **Configure Authentication**. The Authentication Wizard opens.

2   In the Set Server Authentication Type area, use the Authentication Method drop-down to select either:

— **Local Accounts** – This method allows an administrator to set *administrator* and *operator* log-on credentials for the Satellite Console; these credentials restrict access to various parts of the Console. This is the default. See the section To use Local Accounts on page 222 for configuration information.

— **Directory Service Accounts** – This method allows administrator authentication using Directory Service Accounts (such as Active Directory) that are in place in the environment. For configuration information, see To use Directory Service Accounts on page 222.

3   Click **Next** to proceed to the Configuration area and specify the settings for the access method you have chosen.

To use Local Accounts

If you are using Local Accounts to secure access to the Satellite Console, change the password immediately after installing the Satellite server.

1   Configure Console access for administrators and operators in the appropriate areas.

— **Administrator** permissions allow the user to access all areas of the Console.

— **Operator** permissions restrict the user's access to only the Operations area of the Console.

2   Click **Next**.

3   When the configuration is complete, click **Close**.

The next time you log in to the Satellite Console using a Local Account, use the new password.

To use Directory Service Accounts

An external Directory Service Account can be used to authenticate a user's access to the Satellite Console.

1   In the Directory Service Settings area, specify the configuration parameters as described below.

— **Directory Host**: The hostname or IP address of the external directory server that will be used for authentication.

- **Directory Port**: The port that will be used to access the external directory server. The default is 389.

- **Base DN**: The base object in your directory at which to start searching when querying for the users.

  For example, **dc=europe,dc=acme,dc=com**.

- **Access Group DN**: The Group DN that contains all members who are entitled to access the Core Console with administrative rights.

- **Directory User ID**: A valid user ID that can access the directory server in order to verify that a person logging on to the Core is a member of the above-named Group DN. The default is administrator.

- **Directory Password**: The password that is associated with the above-listed user ID.

2 In the Test LDAP Group User area, supply the credentials of a "test user.

- **Username**: The user name of an existing Access Group DN user.

- **Password**: The password that is associated with the above-listed user name.

3 Click **Next**.

4 When the configuration is complete, click **Close**.

Administrators can now sign in to the Satellite Console using their Directory Service Account credentials.

Configuration

The Configuration option in the left navigation pane on the Configuration tab is available on Satellite Consoles, only.

Configuration services supply "model" and service information to the HPCA agents, based on their entitlements. The agents connect to the server in order to obtain this information and to satisfy changes. When this service is disabled on the Satellite server, HPCA agents will have to use a different server in order to obtain the requested information. This "fallback server" designation should be built in to your infrastructure model (as configured in the CLIENT.SAP Instances of the Configuration Server Database).

To enable the configuration services, select the **Enable** check box and click **Save**.

Data Cache

The Data Cache area is available on Satellite Console only.

Apache Server cache and Proxy Server services control the underlying HPCA cache-management service that is used to download data (such as software, patch, operating system, security, and audit) from an upstream host with which the Satellite is synchronized. This page enables you to:

- Enable and disable Apache Server cache services on this Satellite.

- Enable and disable Proxy Server preload (static cache) and Proxy Server dynamic cache.

- Set Apache Server cache limit, in megabytes.

To configure Data Cache

1 On the Configuration tab, click **Data Cache**.

2 Set the following options:

— Select the **Enable Apache Server cache** check box to enable data services for a Satellite. This is the default setting and enables HPCA agents that are connecting to the Satellite to receive their Patch Manager Gateway binaries from the Satellite data cache.

— Clear the **Enable Apache Server cache** check box to disable data services for a Satellite.

– A synchronization with the upstream host does not download the Patch Manager Gateway binaries to this Satellite.

– Requests for Patch Manager Gateway binaries from the HPCA agents that connect to the Satellite are passed to the upstream host.

— Select the **Enable Proxy Server preload (static cache)** check box to preload data services for a Satellite. This is the default setting and enables HPCA agents that are connecting to the Satellite to receive their resources from the Proxy Server static cache.

— Clear the **Enable Proxy Server preload (static cache)** check box to disable preloading the data services for a Satellite.

  – A synchronization with the upstream host does not download the resources to the Satellite.

  – Resource requests from the HPCA agents that connect to a Satellite fail if the option **Enable Proxy Server dynamic cache** is *also* disabled.

— Select **Enable Proxy Server dynamic cache** check box to enable data services from the Proxy Server dynamic cache for a Satellite. This option enables HPCA agents that are connecting to the Satellite to receive their resources from the Proxy Server dynamic cache.

— Clear the **Enable Proxy Server dynamic cache** check box to disable the data services from the Proxy Server Dynamic cache for a Satellite.

  Resource requests from the HPCA agents that connect to the Satellite fail if the option **Enable Proxy Server preload (static cache)** is *also* disabled.

— Set **Apache Server cache limit (MB)** to set a maximum size (in megabytes) of the resource cache. The default is 40000 MB.

3 Click **Save** to implement your changes.

When the Operations tab is refreshed, the status of this service is shown under Summary.

▶ The HTCACHECLEAN Windows Service runs automatically once a day to clean the Satellite Server cache of files that are no longer necessary. This time interval provides good performance for the vast majority of systems.

Infrastructure Management

The Infrastructure Management section allows you to configure various settings of your HPCA infrastructure. See the following sections for details.

Proxy Settings

The Proxy Settings configuration page is used to specify the settings for proxy servers that will be used for internet based communication between the HPCA Core Server and external data sources or recipients.

You can establish separate proxy settings for HTTP and FTP communication. The HTTP proxy server is used for Patch Manager Acquisitions, HP Live Network content updates, and Real Simple Syndication (RSS) feeds used by certain dashboard panes. Without these HTTP proxy settings, for example, Patch Manager acquisitions will fail and you will not be able to download bulletins, patches, and related items, such as Windows Update Agent (WUA) files.

The FTP proxy server is used by the Patch Manager to perform HP Softpaq acquisitions.

To configure your proxy settings:

1 On the **Configuration** tab, expand the **Infrastructure Management** area, and click **Proxy Settings**.

2 Select the tab for the proxy server that you want to configure: **HTTP** or **FTP**

3 Select the **Enable** box.

4 Provide the following information for the proxy server.

   — **Host**: network addressable name of the proxy server

   — **Port**: port on which the proxy server listens

   — **User ID**: user ID if the proxy server requires authentication

   — **Password**: password for the proxy user if the proxy server requires authentication

5 Click **Save** to implement your changes.

SSL

Enabling SSL protects access to the Core console. With SSL enabled, transactions made while connected to the console are encrypted.

Use the SSL section to enable SSL, and define server and client certificates.

- SSL Server on page 227
- SSL Client on page 227

SSL Server

The SSL Server certificate is based on the host name of the HPCA server. It allows your server to accept SSL connections. It should be signed by a well known certificate authority, such as VeriSign.

To enable and configure SSL for the HPCA Server

1   In the HPCA Console, click **Configuration** tab.

2   In the left pane, click **Infrastructure Management** > **SSL**.

3   In the SSL Server area, select the **Enable SSL** check box.

4   Select whether to **Use existing certificates** or **Upload new certificates**.

    If Upload new certificates is selected, click **Browse** to navigate to and select Private Key File and Server Certificate File.

5   Click **Save**.

SSL Client

The Certificate Authority file contains the signing certificates from trusted Certificate Authorities. They allow the HPCA server to act as an SSL client when connecting to other SSL-enabled servers. Your server installation comes with a default set of trusted authorities that should be sufficient for most organizations.

To define a CA Certificates File

1   In the HPCA Console, click **Configuration** tab.

2   In the left pane, click **Infrastructure Management** > **SSL**.

3   In the SSL Client area, click **Browse** to navigate to and select the CA
     Certificates File.

4   Select whether to append this certificates file to existing certificates, or to
     replace the existing certificate with this new file.

5   Click **Save**.

Database Settings

Use Database Settings to configure the ODBC connections to your SQL
database for the Core server objects.

Prerequisites

The Core database must be created and an ODBC connection defined for it.
Refer to the installation instructions in the product manual for details.

To configure Messaging

1   On the Configuration tab, click **Infrastructure Management** then **Database
     Settings**.

2   Set the following options.

     —   **DSN**: Select the DSN for the Core database.

     —   **User ID**: Specify the user ID for the DSN.

     —   **Password**: Specify the password that is associated with the ODBC
         user ID.

     —   **Server Host**: Specify the name of the server hosting the database.

     —   **Server Port**: Specify the server port (default is 1433)

3   Click **Save**.

Satellite Management

The Infrastructure Management, Satellite Management area on the
Configuration tab enables you to deploy and manage Satellite servers from
the HPCA Console. Satellite servers are used to optimize bandwidth and
increase network performance by providing remote services, including data
caching, for managed devices.

For HPCA Standard and Starter Editions, only Streamlined (Standard) deployment mode is available, which offers only data caching services to the Client Automation agents that the Satellite serves.

To define and configure Satellite servers, complete the following tasks:

1 Import the device into the HPCA device repository. See Importing Devices on page 95 for more information.

2 Add devices to the Servers group.

   See Add a Satellite Server on page 231.

3 Deploy the Satellite Server component to these devices. This enables remote services, including data caching, on these devices.

   See Install the Satellite Server Component on page 233.

4 Optionally, create Server Pools and assign Servers to these pools.

   See Server Pools on page 239

5 Create Locations and assign Servers or Server Pools to these Locations.

   See Locations on page 242.

6 Create Subnets and assign them to Locations.

   See Subnets on page 246.

Managed devices connect to Satellite servers based on the subnet that is assigned to Server or Server Pool Locations. For example, if a device is on subnet 208.77.1.0 and you have assigned that subnet to a specific Location, your device contacts the assigned Servers or Server Pools for this Location in priority order as defined within the Location.

If the Proxy Server dynamic caching is enabled on the Satellite server, the data requested by agents is automatically cached on the Satellite server. The Satellite servers can also be pre-populated with all data on the HPCA Core server using the synchronize feature. See Synchronize Satellite Servers Service Cache on page 236 for details.

▶ You can define and configure Satellite servers from the HPCA Core server only. You cannot do this from another Satellite server.

The Satellite Management area contains the following tabs:

• Servers on page 230

• Server Pools on page 239

Servers

The Satellite Management **Servers** tab displays all Core and Satellite servers that currently belong to the Servers group. You can select one of three possible views on this tab, namely:

- Core Server: Displays the Core server only
- Satellite Servers: Displays Satellite servers only
- All Servers: Displays both the Core and Satellite servers, as well as devices manually added to the Servers group and Legacy Proxy Servers from a previous version of the product.

You can open the Server property page for each server to view or edit server properties, to view assigned Locations, and to view or edit Server Pools assignments.

You can use the toolbar buttons on the Servers tab to define additional Satellite servers by adding devices to the Servers group and then installing the Satellite server component to those devices. Satellite servers are devices added to the Servers group, with the Satellite server component installed.

Table 26   Servers Toolbar Buttons

Button	Description
	Refresh Data – Refresh the list of servers.
	Show/Hide Filter Input – Show or Hide the Filter input area to restrict the display of Servers to only those matching user specified criteria.
	Add device(s) to Servers group – Add devices to the HPCA Satellite Servers group.
	Remove device(s) from Servers group – Remove devices from the HPCA Satellite Servers group.
	Install the Satellite Server – Launch the Satellite Server Deployment Wizard to install the Satellite server on the selected devices.

Table 26 Servers Toolbar Buttons

Button	Description
	Uninstall the Satellite Server – Launch the Satellite Server Removal Wizard to uninstall the Satellite server from the selected devices.
	Synchronize the selected Satellite Servers service cache – Synchronize the selected Satellite server's service cache with the HPCA Core server.
	Delete the Selected Device(s) – Remove the device from the HPCA device repository.

After you add servers, you can optionally assign them to Server Pools. You must assign Servers or Server Pools to Locations to enable client devices to contact these Servers.

The following sections detail what you can do using the Server property sheet and the toolbar buttons on the Servers tab:

Add a Satellite Server

Before you install the Satellite server component, add the device to the Servers group. When selecting devices to add as Satellite 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.

▶ The following ports must be excluded if a firewall is enabled on any of the Satellite Servers that you will be using:

- TCP 139, 445, 3463, 3464, 3465, and 3466

Note that 3466 is the default HPCA port. If you customized this port when you installed HPCA, be sure that the port you are using is also open.

- 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 to the Servers group

1 On the Servers toolbar in the **All Servers View**, click the **Add device(s) to Servers group** toolbar button.

   The Device Selection window opens and shows a list of all devices imported into HPCA that do not belong to the Servers group.

2 Select one or more devices from the list, and click **Add Devices**.

3 Click **Close** to close the device selection window.

   The added devices now appear in the **Servers** list in the **All Servers** view on the **Servers** tab.

Remove a Satellite Server

If you do not want a device to be managed as a Satellite server, you can remove that server from the Servers group.

▶ You must explicitly uninstall the Satellite server component from the device *before* removing the device from the Servers group. If you remove the device without uninstalling the HPCA Satellite server component, the device will automatically re-appear after a period of time since it is still an active Satellite server, and will also remain a member of the Servers group. See Uninstall the Satellite Server Component on page 234.

1 On the Servers tab, select the devices that you want to remove from the Servers group.

2 Click the **Remove device(s) from Servers group** 🗐 toolbar button. A confirmation pop-up window opens.

3 Click **Yes** to confirm.

The devices that you selected are removed from the group.

Install the Satellite Server Component

After you add a device to the HPCA Satellite Servers group, you can deploy the Satellite server component to that device. This is required to enable remote services, including data caching, on that server.

When you deploy the Satellite server component to a device from the HPCA Console, the Core completes the following background processing:

• Using the credentials that you provide, the HPCA Core server establishes a connection with the device. These credentials must provide Administrator access to the IPC$ share on the remote system. If this access level is not available in your environment, perform a manual installation of the Satellite Server component instead of deploying through the HPCA Console.

• If the HPCA Management Agent is not installed on the device, the Core installs the Management Agent on the device.

• The Management Agent downloads the Satellite server component from the Core server and installs it on the device. The Satellite server deployment process also handles the upgrade and migration scenarios. If a previous version of the Satellite server component is already installed on the device, it is automatically detected and the component is upgraded to the current release and the cache is migrated. Additionally, if the device has an Integration Server-based Proxy Server components installed, the proxy service is stopped, the Integration Server-based Proxy Server is removed, the Satellite server component is installed, and then the cache is migrated.

• The Management Agent automatically runs the First Time Setup Wizard on the device and populates the Host Device field with the name of the Core server.

1   Select one or more devices from the Satellite Servers list using the check
    boxes in the left column.

2   Click **Install the Satellite Server** 🔺 toolbar button to launch the Satellite
    Server Deployment Wizard.

3   Follow the steps in the wizard to deploy the Satellite Server component to
    the selected devices. The Satellite Server is installed to :

    SystemDrive:\Program Files\Hewlett-Packard\HPCA

Services can be preloaded to Satellite Servers using the Synchronize feature.
See Synchronize Satellite Servers Service Cache on page 236 for details.

After you have created Satellite Servers, you must define Locations and then
assign the Satellite Servers to these Locations. See Locations on page 242 for
details.

Uninstall the Satellite Server Component

If you do not want a device to function as an HPCA Satellite Server, you must
remove the Satellite server component from that device.

1   Select devices from the Satellite Servers list using the check boxes in the
    left column.

2   Click **Uninstall the Satellite Server** 🔺 toolbar button to launch the Satellite
    Server Removal Wizard.

3   Follow the steps in the wizard to remove the Satellite server component
    from the selected devices.

You can follow the progress of your Satellite Server Removal job under the Job
Management area on the Management tab. After this job completes, the
Satellite Servers list will show that the Satellite server component is not
installed on this device.

Server Details Window

To access the Server Details window, click any server name link in the Servers list on the Servers tab.

From the Server Details window, you can view detailed information about a Satellite server and perform various server management tasks. The following tabs are available on the Server Details window:

- **Summary**: The Summary tab displays the server details, such as Vendor, IP Address, Operating System, HPCA Build ID, and Service Pack.

- **Properties**: The Properties tab displays the server properties, including the server status. By default, the server is enabled, and the client devices can contact this server for resolution. You can disable the Satellite server during the maintenance phase to avoid device connects to this server.

- **Cache**: The Settings area in the Cache tab display the cache preloading options for a Satellite server. You can preload a Satellite server for Software, Patch, and Operating System service cache. The **Preload Enabled** option ensures that the files available on the upstream server cache are preloaded to the Satellite server. If Proxy Server dynamic caching is enabled, the files are cached on the Satellite server as they are requested by the agents.

  The Synchronization area displays the last time the server's service cache was synchronized with the upstream server. Click **Synchronize** to synchronize the Satellite server content with the upstream host. For more information, see the Synchronize Satellite Servers Service Cache on page 236.

- **Server Pools**: The Server Pools tab displays the Server Pool assignments for this Server. You can use the toolbar buttons on this tab to add a server to or remove it from the available Server Pools. For more information, see Server Pools on page 239.

- **Locations**: The Locations tab displays the Location assignments for this Server. For details on adding and assigning Locations, see Locations on page 242.

- **Reporting**: The Reporting tab displays the preload summary for the services that are preloaded or removed from a Satellite server. Only preloaded services are displayed.

- **Operations**: The Operations tab shows the status and state of the configurable Satellite services (Satellite Configuration Options on page 215). It also lists the basic properties of the server, including the upstream host. From this tab, you can synchronize a Satellite or flush a cache. You must provide valid HPCA Console login credentials to the Satellite server in order to access this tab.

- **Configuration**: The Configuration tab enables you to configure a subset of the Satellite Configuration Options listed on page 215. You must provide valid HPCA Console login credentials to the Satellite server to access this tab.

Add a Server to Server Pools

You can assign the selected server to an existing Server Pool. To add a server to Server Pools, complete the following steps:

1 Click the **Add Server to existing Server Pool** button on the toolbar. The Server Pool Selection window opens displaying the available Server Pools.

2 Select one or more Server Pools to which you want to add a Server.

3 Click **Add Server to Server Pools**.

4 Click **Close**.

Delete a Server from Server Pools

You can remove the selected server from Server Pool(s). To remove a Server from Server Pools, complete the following steps:

1 Select the Server Pool(s) from which you want to remove the Server.

2 Click the **Remove Server from the selected Server Pool(s)** button on the toolbar. A confirmation pop-up window opens.

3 Click **Yes** to remove the Server.

Synchronize Satellite Servers Service Cache

Each time devices request resources that are not available on the Satellite Server's local cache, the data is retrieved from the HPCA Core server. If the Proxy Server dynamic caching is enabled on the Satellite server, the requested data is stored in the cache of the Satellite server, and provided to the client devices.

A Satellite server's service cache can be preloaded with the data required by managed devices. A Satellite server automatically caches data when it is requested by a client device. Using the Synchronize feature, you can preload a Satellite server's cache with all available data on the upstream server.

You can select which data to preload using the Cache tab in the Server Details window (after the Satellite server has been deployed).

▶ Preloading consists of downloading large binary files and therefore may impact overall network performance. When possible, perform synchronizations during off-hours when optimal network performance is not a priority.

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

▶ After a Satellite Server is first synchronized, a new entry is added to the Managed Devices report with an HPCA Agent ID of RPS_<DEVICENAME>. This entry exists specifically to display the preload status of the Satellite Server services and does not contain detailed hardware information for the associated device.

To select which data to preload

1 After the Satellite Server is deployed, click the Server link in the Satellite Servers list to open the **Server Details** window.

2 Click the **Cache** tab.

3 Use the drop-down lists to enable or disable the services that you want to make available for preloading from the upstream server. By default, preloading is disabled for all services.

4 Click **Save** to commit your changes.

5 Click **Synchronize** to preload the Satellite Server with available data.

To synchronize Satellite Servers

1 On the Configuration tab, go to the Satellite Management area under Infrastructure Management.

2 On the Servers tab, select the servers that you want to synchronize.

3   Click the **Synchronize the selected Satellite Servers service cache** toolbar
    button to update all selected server's with the latest data from the HPCA
    Server. The specific services preloaded to each server depend on the
    settings configured on the **Cache** tab in each server's Server Details
    window.

▶   You can also synchronize a Satellite server from the Server Details Window.

To view a summary of preloaded services in a Satellite 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 preloaded successfully (initial
   preload).

— **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 preloaded services are displayed in the report. Services stored on a
Satellite Server through the default method (cached automatically when
requested by a managed device) are not displayed.

Delete a Server

If you no longer want a device to be in the HPCA device repository, you can
delete the device. You may want to perform this operation when a device is no
longer part of your environment. When a Server is deleted, it is automatically
removed from any Locations or Server Pools to which it may be assigned.

Deleting a device is the reverse of importing devices. See Importing Devices on page 95 for more information.

➤ You must explicitly uninstall the Satellite server component from the device *before* removing the device from the HPCA device repository. If you delete the device without uninstalling the HPCA Satellite Server component, the device will automatically re-appear after a period of time since it is still an active Satellite Server, and will remain a member of the Servers group. See Uninstall the Satellite Server Component on page 234.

To delete a Server

1 On the Servers tab, select the devices that you want to remove from the HPCA repository.

2 Click the **Delete the Selected Device(s)** toolbar button A confirmation pop-up window opens.

3 Click **Yes** to confirm.

The devices that you selected are removed from the HPCA repository.

Server Pools

The Satellite Management Server Pools tab displays all HPCA Server Pools that have been created in your environment. Server Pools are groupings of Servers (Core or Satellites) that will be contacted by devices to resolve policy and retrieve data. Servers can be assigned to Server Pools (a maximum of 30 Servers), and Servers and Server Pools are assigned to Locations to enable client devices to contact them.

A Server Pool is used to perform software load balancing of client connections. If a grouping of Servers have equal priority to handle client connections, these Servers can be grouped into a Server Pool, which can then be assigned to a Location. Clients randomly contact Servers in the Server Pool, thus distributing the load across the Servers in the pool. For example, if your environment contains three Satellite servers in the US that should be contacted with equal priority by client devices in a particular Location, these Servers can be grouped into a US Server Pool and then assigned to the Location.

By default, the HPCA Core Server Server Pool containing the HPCA Core server is installed on your system. You cannot delete this Server Pool.

You can use the Server Pools property sheet to view or edit Server Pool properties.

You can use the toolbar buttons on the Server Pools tab to add and remove Server Pools.

Table 27   Server Pools Toolbar Buttons

Button	Description
![refresh]	**Refresh Data** – To refresh the list of Server Pools.
![filter]	**Show/Hide Filter Input** – To show or hide the Filter input area to restrict the display of Server Pools to only those matching user specified criteria.
![create]	**Create a New Server Pool** – To launch the Server Pool Creation Wizard.
![delete]	**Delete the selected Server Pool(s)** – To delete selected Server Pools.

The following sections detail what you can do using the Server Pool property sheet and the toolbar buttons on the Server Pools tab:

- Create a New Server Pool on page 240
- Delete a Server Pool on page 241
- Server Pool Details Window on page 241

Create a New Server Pool

You can create Server Pools and add Core and Satellite Servers to them to create a grouping of Servers that an agent can contact for data and policy resolution.

To create a new Server Pool

1   Click **Create a New Server Pool** ![icon] toolbar button to launch the Server Pool Creation Wizard.

2   Follow the steps in the wizard to create the new Server Pool.

    The Server Pool is added to the Server Pool list on the Server Pools tab.

Delete a Server Pool

You can delete Server Pools when they are no longer needed.

To delete a Server Pool

1   Select the Server Pools that you want to delete from the Server Pool list using the checkbox in the left column.

2   Click **Delete the selected Server Pool(s)** ✖ toolbar button. A confirmation pop-up window opens.

3   Click **Yes** to confirm.

The selected Server Pools are removed from the Server Pool list on the Server Pools tab.

Server Pool Details Window

To access the Server Pool Details window, click any Server Pool name link in the Server Pools list on the Server Pools tab.

From the tabs on the Server Pool Details window, you can view detailed information about a Server Pool and perform various server management tasks. The following tabs are available on the Server Pool Details window:

• **Properties**: The Properties tab displays the properties information that you specified in the Server Pool Creation Wizard when you created this Server Pool. You can edit the properties on this tab.

• **Servers**: The Servers tab displays the Servers that are currently assigned to this Server Pool. You can use the toolbar buttons on this tab to add or remove Servers in this Server Pool.

Add Servers to a Server Pool

To add servers to a Server Pool, complete the following steps:

1   Click the **Add Servers to Server Pool** 🔲 button on the toolbar. The Server Selection window opens displaying the available Servers.

2   Select one or more Servers to add to this Server Pool. You can add a maximum of 30 servers to a Server Pool.

3   Click **Add Servers**.

4   Click **Close**.

The selected Servers are assigned to the Server Pool as displayed on the Servers tab.

Remove Servers from a Server Pool

To remove servers from a Server Pool, complete the following steps:

1   Select the Server(s) that you want to remove from this Server Pool.

2   Click the **Remove the Selected Server(s) from this Server Pool** 🖥button on the toolbar. A confirmation pop-up window opens.

3   Click **Yes** to remove the Servers.

The selected Server(s) are removed from the Server Pool as displayed on the Servers tab.

Locations

Use the Locations tab to view existing Locations or to add new Locations in your HPCA infrastructure. When you add a new Location, you define the Subnets that form this Location and then assign this Location to an ordered set of Servers or Server Pools. To resolve policies and to retrieve data resources, managed devices connect to Satellite servers based on Subnet assignment to Locations and the priority order of the Servers or Server Pools.

You can use the toolbar buttons on the Locations tab to add or remove Locations.

Table 28   Locations Toolbar Buttons

Button	Description
🔄	**Refresh Data** – Refresh the list of Locations.
🔍	**Show/Hide Filter Input** – Show or Hide the Filter input area to restrict the display of Locations to only those matching user specified criteria.
🗔	**Create a New Location** – Launch the Location Creation Wizard.
✖	**Delete the selected Location(s)** – Delete selected Locations.

The Locations list includes information about each Location in your HPCA infrastructure, including the description and the geographic information.

The following sections detail the tasks you can complete using the Locations property sheet and the toolbar buttons on the Locations tab:

Create a New Location

To create Locations, define Subnets and an ordered set of Servers and Server Pools for each Location.

To create a new location

1   Click **Create a New Location** 🖼 toolbar button to launch the Location Creation Wizard.

2   Follow the steps in the wizard to create the new Location.

    The Location is added to the Location list on the Location tab.

Delete a Location

You can delete Locations from your HPCA infrastructure if they are not required.

To delete a location

1   Select the Locations that you want to delete from the Location list using the checkbox in the left column. You cannot delete the Default Location. Additionally, when you delete a Location, any Subnets assigned to that Location will be reassigned to the Default Location.

2   Click the **Delete the selected Location(s)** ✖ toolbar button. A confirmation pop-up window opens.

3   Click **Yes** to confirm.

    The selected Locations are removed from the Location list on the Locations tab.

Location Details Window

To access the Location Details window, click any Location name link in the Locations list on the Locations tab.

From the tabs on the Location Details window, you can view detailed information about a Location and perform various server management tasks.

- **Properties**: The Properties tab displays the properties information that you specified in the Location Creation Wizard when you created this Location. You can edit the properties on this tab.

- **Connections**: The Connections tab displays the current Server or Server Pool connections for this Location. It enables you to add, import, and remove connections. The devices that are part of Subnets assigned to this Location contact the Servers or Server Pools listed in the priority specified to resolve policy and retrieve resources. The Order column indicates the priority in which the Server or Server Pool will be contacted. The Reorder column arrows enable you to reorder the connections.

- **Subnets**: The Subnets tab displays the Subnets that are currently assigned to this Location. You can use the toolbar buttons on this tab to assign additional Subnets to this Location or remove Subnets from it by reassigning them to a different Location.

- **Devices**: The Devices tab displays the devices that are in this Location. This tab is view only.

Add connections to a Location

You can add new connections to a Location. The agent connections use the resources from the Server or Server Pool you define a connection to. To add connections to a Location, complete the following steps:

1 Click **Add Connection** link. The Location Connection Selection window opens.

2 Select a resource from the available types to assign to this location.

3 Click **Add Connection**.

4 Click **Save**.

   The new connections are added to the Location as displayed on the Connections tab.

Import connections to a Location

You can import connections from an existing Location. The existing connections that are defined for this Location are removed when you import connections. To import connections to a Location, complete the following steps:

1   Click Connections tab.

2   Click **Import Connections**. The Location Selection window opens.

3   Select the Location with the connections you want to import.

4   Click **Import Connections**.

5   Click **Save**.

    The imported connections are added to the Location as displayed on the Connections tab.

Assign additional Subnets to a Location

To assign additional Subnets to a Location, complete the following steps:

1   Click the Subnets tab.

2   Click the **Assign additional Subnets to this Location** button on the toolbar. The Subnet Selection window opens displaying the Subnets that are not already assigned to this Location.

3   Select one or more Subnets to assign to this Location.

4   Click **Assign Subnets to Location**.

5   Click **Close**.

    The selected Subnets are assigned to the current Location as displayed on the Subnets tab.

Reassign Subnets to a different Location

You can reassign the Subnets for the selected Location to a different Location. To reassign Subnets to a different Location, complete the following steps:

1   Click the Subnets tab.

2   Select the Subnet(s) that you want to assign to a different Location.

3   Click the **Assign the selected Subnet(s) to a different Location** button on the toolbar. The Location Selection window opens displaying the other Locations that exist in your environment.

4   Select a Location to which you want to reassign the selected Subnets.

5   Click **Assign Subnets to Location**.

The selected Subnets are now reassigned to the Location you selected.

Subnets

The Subnets that are known to HPCA are displayed on the Subnets tab. HPCA Agents communicate their subnet configuration during client connections, enabling the Subnets in your environment to be automatically detected and displayed on the Subnets tab. Subnets can also be manually created, as described in Create a New Subnet on page 247.

Subnets are subdivisions of the IP network space and contain a network address (for example, 192.168.1.0) and subnet mask (for example, 255.255.255.0). In HPCA, Subnets are often represented in Classless Inter-Domain Routing (CIDR) notation. In CIDR notation, the previous example would be displayed as 192.168.1.0/24. Every HPCA Subnet is assigned to a single Location; typically a Location will serve multiple Subnets. For example, you might group together many Colorado Subnets into a Colorado Location. Devices that belong to a particular Subnet will contact the Servers and Server Pools associated with the Subnet's assigned Location to resolve policy and retrieve data.

The Subnets tab allows you to view and edit Subnet properties, create and delete Subnets, and assign Subnets to Locations.

You can use the toolbar buttons on the Subnets tab to add and remove Subnets.

Table 29   Subnets Toolbar Buttons

Button	Description
	Refresh Data – Refresh the list of Subnets.
	Show/Hide Filter Input – Show or Hide the Filter input area to restrict the display of Subnets to only those matching user specified criteria.
	Create a New Subnet – Launch the Subnet Creation Wizard.
	Delete the selected Subnet(s) – Delete selected Subnets.

The following sections detail the tasks that you can complete using the Subnet property sheet and the toolbar buttons on the Subnets tab:

- Create a New Subnet on page 247
- Delete a Subnet on page 248
- Subnet Details Window on page 248

Create a New Subnet

Subnets are automatically detected based on device connections, but they can also be manually created. You may want to manually create Subnets to prepare that Subnet for management with HPCA. Creating a Subnet manually enables you to assign that Subnet to the appropriate Location prior to Agents being installed on that Subnet. When Agents are later installed on that Subnet, they will already be associated with the appropriate Location.

As part of Subnet creation, you assign a Subnet to a regional Location. Devices that belong to a particular Location because of Subnet assignment will contact the Servers and Server Pools associated with that Location to resolve policy and retrieve data.

The following procedure explains how to manually create a Subnet.

1   Click **Create a New Subnet** toolbar button to launch the Subnet
    Creation Wizard.

2   Follow the steps in the wizard to create the new Subnet.

    The Subnet is added to the Subnet list on the Subnets tab.

Delete a Subnet

You can remove Subnets when they are no longer needed based on changing
network configurations within your environment.

▶   You cannot delete a Subnet that contains active devices, as the Subnet will be
immediately detected again based on device connections. If you attempt to
delete such a Subnet, the Subnet will still appear in the list but will be
reassigned to the Default Location.

1   Select the Subnets that you want to delete from the Subnet list using the
    checkbox in the left column.

2   Click **Delete the selected Subnet(s)** toolbar button. A confirmation
    pop-up window opens.

3   Click **Yes** to confirm.

    The selected Subnets are removed from the Subnet list on the Subnets
    tab.

Subnet Details Window

To access the Subnet Details window, click the link for the Subnet in the
Subnet column of the Subnet list.

From the tabs on the Subnet Details window, you can view detailed
information about a Subnet.

•   **Properties**: The Properties tab displays the properties information that
    you specified in the Subnet Creation Wizard when you created this Subnet
    or that was automatically determined based on Agent connections. You
    can edit the properties on this tab.

- **Devices**: The Devices tab displays all devices that are located on the selected Subnet. This tab is view only.

Live Network

Live Network settings required to communicate with the HP Live Network content server are configured in the Infrastructure Management area on the Configuration tab. See Configure the Connection to the HP Live Network Server on page 249.

Live Network updates are configured in the Infrastructure Management area on the Operations tab. See Live Network on page 183.

Configure the Connection to the HP Live Network Server

Use the Live Network settings to configure the connection used to automatically download the latest content from HP Live Network and to establish the RSS feed for the HP Live Network Patch Manager Announcements dashboard panes. This includes the following items:

- URL for the HP Live Network content server used to download the most recent scanners and data.

- Your HP Passport login credentials.

➤ For your security and convenience, the HP Live Network content server uses HP Passport authentication. HP Passport is a single sign-in service that enables you register with all HP Passport-enabled web sites using a single user ID and password. To set up your HP Passport profile, go to:

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

Make sure that your HP Passport profile includes the 12-digit service agreement identifier (SAID) associated with your HPCA support contract. This SAID must include entitlement to HP BSA Essentials so that you can access the HP Live Network content server. For assistance, contact your HP Software sales representative.

➤ Passwords entered on this page are encrypted.

You can test your configuration information before you save it. When you request a test, the HPCA Console attempts to connect to the HP Live Network content server. If the connection succeeds, you know that your configuration information is valid. See Test Your Live Network Settings on page 251 for details.

To specify the HP Live Network connection settings:

1   On the Configuration tab, expand the Infrastructure Management area, and click **Live Network**.

2   Specify the following information. All parameters marked with an asterisk (*) are required.

    — **HP Live Network User ID**—your HP Passport user ID.

    — **HP Live Network Password**—your HP Passport password.

    — **HP Live Network Content URL**—the location of the HP Live Network content server for vulnerability definitions and scanners (URL filled in by default).

    — **HP Live Network Connector**—the path to the Live Network Connector executable on the system hosting the HPCA Core (path filled in by default).

    For more information, see Download the HP Live Network Connector on page 85.

3   To test the settings that you have specified, click **Test**. See Test Your Live Network Settings on page 251 for more information.

4   Click **Save** to implement your changes.

▶   The HPCA Console does not automatically save your configuration settings after a successful test. You must click the **Save** button if you want to save your settings.

▶   If you leave this page, any information that you entered in the text boxes prior to clicking **Save** will be lost. Be sure to click **Save** if you want to keep this information.

▶   You can use the **Reset** button to restore the most recently saved settings.

Test Your Live Network Settings

When you are configuring your Live Network settings, you can test your settings to make sure that they work before you save them.

To run a test, click the **Test** button in the lower right corner of the page. The HPCA Console first confirms that all required settings are specified and that all settings have the proper format. It then takes the following actions:

The HPCA Console attempts to connect to the HP Live Network content server and log in using the user name and password specified. Any proxy information that appears on the Proxy Settings page in the Infrastructure Management configuration area is used.

Depending on network traffic and other parameters, this test can take up to three minutes. A dialog box asks you whether you want to continue with the test. If you want to continue, click **Yes**.

After the test is completed, the Test Results dialog box shows you the outcome of the test. The following table summarizes the possible outcomes and implications of each.

Table 30   Live Network Settings Test Results

Icon	Outcome	Explanation and Suggested Action
✅	Test was successful.	All settings are valid. Save your configuration.
❌	Test failed.	Here are some of the more common reasons that a test can fail: • A required setting is missing. • A setting is specified using an invalid format (for example, an invalid URL or path name). • A setting is spelled incorrectly. • The login credentials for the HP Live Network content server are not valid (for example, if your subscription has expired).

Table 30 Live Network Settings Test Results

Icon	Outcome	Explanation and Suggested Action
	Unknown	This outcome does not necessarily mean that your configuration information is invalid. It simply means that the test could not be completed.
		For example, if the HPCA Console is unable to connect to the HP Live Network content server within three minutes, the test times out. This can occur for the following reasons:
		• The server is unavailable.
		• Network traffic impedes the connection.
		• A firewall blocks the connection.
		This outcome can also occur if the connection goes through a proxy server, and either the proxy information specified is not correct or the proxy server blocks the connection.

To troubleshoot a failed or inconclusive test result, check the spelling and format of all the settings on the tab. Also check the vms-server.log file for errors.

▶ You must click the **Save** button to save your settings—even if the test is successful. The HPCA Console does not automatically save your settings.

Device Management

Use the Device Management section to configure alert options and Trusted Platform Module (TPM) settings.

The following sections describe the available device management options:

- Alerting on page 253
- Trusted Platform Module on page 257

Alerting

Use the Alerting section to configure CMI and S.M.A.R.T. alerts and reporting options.

- CMI on page 253
- S.M.A.R.T. on page 256

CMI

The CMI Softpaq is installed to each HP targeted device as part of the HPCA 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).

The following hardware related alerts are reported using the HP CMI and
S.M.A.R.T. Drive Alert Montoring:

Table 31   HP CMI and S.M.A.R.T. Runtime alerts

Runtime alerts	Desktop	Workstation	Notebook
BIOS configuration change	x	x	x
BIOS configuration security	x	x	x
Chassis intrusion	x	x	
Fan stall	x	x	
Fan normal*	x	x	
Thermal caution	x	x	
Thermal critical	x	x	
Thermal normal*	x	x	

* Can be indirectly detected by a management console through the absence of
a Fan Stall or Thermal Caution/Critical alert.

Table 32   HP CMI and S.M.A.R.T. Post error alerts

POST error alerts	Desktop	Workstation	Notebook
101-Option ROM Checksum Error	x	x	
163-Time & Date Not Set	x	x	
164-Memory Size Error	x	x	
214-DIMM Configuration Warning	x	x	
511-CPU fan not detected	x	x	

Table 32   HP CMI and S.M.A.R.T. Post error alerts

POST error alerts	Desktop	Workstation	Notebook
512-Rear Chassis fan not detected	x	x	
513-Front Chassis fan not detected	x	x	
515-Power Supply fan not detected	x	x	
912-The computer cover has been removed	x	x	
917-Front Audio not connected	x	x	
918-Front USB not connected	x	x	
1720-S.M.A.R.T. Hard Drive detects imminent failure	x	x	
1801-Microcode Update Error	x	x	

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 HPCA infrastructure.

▶ CMI is compatible with only specific HP device models. Refer to your device description for compatibility information.

To configure CMI

1   In the HPCA console click the **Configuration** tab, then select **Device Management**.

2   Click the **CMI** tab.

3   To report on captured client alerts from managed HP devices, select
    Enabled from the **Report Client Alerts** drop-down list. Alert reporting is
    disabled by default. The Minimum Severity to Report drop-down list will
    become available after you select Enabled.

4   Select the minimum alert severity to report.

5   To turn on client alerts for managed HP devices, select **Enabled** from the
    Show Client Alerts drop-down list. Alerts are disabled by default. The
    Minimum Severity to Display and Alert Window Timeout dialogs will
    become available after you select Enabled.

6   Select the minimum alert severity to display on the client device.

7   Type the number of seconds an alert should appear on the client device.
    By default, an alert is displayed for five seconds.

8   Click **Save**.

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 HPCA 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 HPCA 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.

Trusted Platform Module

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 Deploy Software on page 129 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 HPCA console click the **Configuration** tab, then select **Device Management**.

2   Select the **Trusted Platform Module** option. The Trusted Platform Module window is displayed.

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**.

Patch Management

Use the Patch Management link to enable patch management and define ODBC parameters for your patch database.

Starter and Standard users can also use this section to acquire Microsoft patches and HP Softpaqs, configure schedules for patch acquisition, and to define patch acquisition settings.

Refer to Patch Deployment Wizard on page 296 for details on how to deploy and entitle patches in your environment.

Patch Management options are explained in the following:

• Database Settings on page 258

• Agent Options on page 259

Database Settings

Patch must be enabled in order for the Patch Management areas of the Console and patch-acquisition facilities to be available.

Use the Database Settings area to enable this feature which will start the Patch Manager service (`HPCA Patch Manager`) and synchronize the information stored in the Patch Library with the patch information in the SQL database

Prerequisite

The Patch database must be created and an ODBC connection defined for it. For details, refer to the *Installing HPCA* chapter.

To configure Patch

1 In the Patch ODBC Settings area, set the following options.

   — **ODBC DSN**: Select the DSN for the Patch SQL database.

   — **ODBC User ID**: Specify the user ID for the DSN.

   — **ODBC Password**: Specify the password that is associated with the ODBC user ID.

2 Click **Save**.

3 If you modified Patch ODBC Settings, follow the prompts to restart the Patch Manager Service.

Agent Options

These Agent Options apply to patching Microsoft devices only.

Use the **Agent Options** available from the **Configuration** tab > **Patch Management** area to enable and configure these Patch Manager Agent options for patching Microsoft Devices.

The next time the Patch Agents connect to the HPCA servers they will receive any configuration changes that you set on these panels.

- Download Manager Options on page 260
- Agent Options on page 262

- **Enable Download Manager**: Select this box to download the required patch files onto the Agent machines using a background, asynchronous process. The Download Manager operates outside of the normal HPCA Agent Connect process. During a Patch Agent Connect, the following process runs in the background:

  a   Patch Agent Connect verifies if the patch is applicable and entitled to devices.

  b   Patch Agent Connect triggers the Download Manager and queues its download request to Download Manager if the patch is applicable and entitled to devices.

  c   Download Manager runs independently and downloads the binaries. If the user turns off the machine or is disconnected from the network during the download, on reboot, the timer ensures that the Download Manager resumes downloading the binary from the point where it stopped. If **Apply patches after download completion** is set to Yes, Download Manager automatically triggers a new Patch Agent Connect.

  d   After the binaries are downloaded from the Download Manager, they are installed in the next Patch Agent Connect.

  ⚠   Download Manager must be enabled to use Patch Distribution using Metadata.

When selected, several Download Manager options are displayed.

Complete the Download Manager Options using the following table:

Table 33　Download Manager Options for Patch Agents

Option and Valid Values	Description
Network Utilization Values = 0 to 100 % 　　　　0 is default	Specifies the maximum percentage of available network bandwidth to download the patch files when the device is active. A value of 0 means the download will use the available network bandwidth. Example: 25 specifies no more than 25% of the available bandwidth should be used for the patch download process.
Network Utilization in Screensaver Mode Values = 0 to 100 % 　　　　0 is default	This is a Screen Saver network utilization option. Network Utilization in Screensaver Mode specifies the maximum percentage of available network bandwidth to download the patch files when Screen Saver is on. This is typically a larger percent than when Screen Saver is off. A value of 0 means the download will use the available network bandwidth when Screen Saver is on. Example: 80 increases the bandwidth used to download the patch files by 80% when screen saver is on.
Delay initialization Values = 0 to 999 seconds 　　　　0 is default	After initialization, specifies the number of seconds to delay before starting or resuming the download of patches. This allows other processes to startup first, and then resume the patch download. Example: Set to 15 to delay initialization by 15 seconds. A value of 0 means there is no delay.
Apply patches after download completion Values = Yes (default) or No	After download completion, set to 'Yes' to trigger a Patch Agent Connect to apply the patches. HP recommends setting the value to Yes. Set to 'No' to have the patches applied when the next Patch Agent Connect is triggered.

Click **Save** to set these configuration options. The Patch Agents will receive the new configuration the next time they connect to the HPCA servers.

The following Agent Options are available for patching Microsoft devices.

- **Disable Automatic Updates**: Select Yes or No from the drop-down box. Use this option to address issues whereby the Patch Agent scan or deployment is getting interrupted because Automatic Updates is set to ON.

  — **Yes**: The Patch Agent will disable Microsoft Automatic Updates before each scan or deployment. Once Patch scan/deployment is done, it reverts the Automatic Updates to its original state.

  — **No**: (The default) The Patch Agent will not disable Automatic Updates before each scan or deployment.

- **Delete Software Distribution Folder**: Select Yes, Backup, or No from the drop-down box. This option is available to address the following issues:

  — Drastic growth in the size of the `SoftwareDistribution` folder

  — `SoftwareDistribution` folder corruption

  — Increased load on the Configuration Server during Patch connects

  > ⚠ Setting **Delete Software Distribution** folder to Yes or Backup automatically restarts the services for Microsoft Automatic Updates and BITS. HP warns against setting this option if the service restarts will cause issues in your environment, especially for those customers who are using both HPCA Patch Management and Automatic Updates as co-located patch solutions.

Set this option to Yes or Backup improves Patch Manager performance due to folder size, corruption, or infrastructure load issues.

— **Yes**: The Patch Agent deletes the contents of the `SoftwareDistribution` folder before every patch scan. Read the Caution (above) on service restarts.

— **Backup:** The Patch Agent first backs up and then deletes the contents of the `SoftwareDistribution` folder before every patch scan. Read the Caution (above) on service restarts.

— **No: (Default)** The Patch Agent will not do anything to the `SoftwareDistribution` folder.

- **Manage Installed Bulletins (-mib)**: Select None, No, or Yes from the drop-down box. This option controls how bulletins already installed on the target devices are handled.

    ⚠ If you do not supply a **-mib** option, the patch agent will behave as if you selected the **-mib Yes** option, which is resource intensive.

    — **None: (Recommended)** Manage all installed bulletins except for those that are detected as "no risk" bulletins. This is the recommended behavior since there is no impact on the client agent in terms of vulnerability or re-patching, and it offers greater performance.

    — **No:** Manage Patch Manager-installed bulletins only; do not manage bulletins installed by an external source.

    — **Yes**: Manage all installed bulletins, whether installed by Patch Manager or an external source. This option is resource intensive.

Click **Save** to set the configuration options. The Patch Agents will receive the new configuration the next time they connect to the HPCA servers.

Out of Band Management

Use the Configuration tab's Out of Band (OOB) Management area to configure OOB Management settings and preferences. For additional information on using Out of Band Management, refer to the *HP Client Automation Out of Band Management User Guide*. The following sections describe the available configuration options:

- Enablement on page 263
- Device Type Selection on page 264
- vPro System Defense Settings on page 266

Enablement

Use the Out of Band Management Enablement area to enable or disable the out of band management features supported by vPro or DASH devices.

Select the **Enable** checkbox to enable out of band management features.

Enabling Out of Band Management allows vPro or DASH devices to be contacted through the OOB Management remote operations capability in addition to the normal Wake on LAN capabilities of the HPCA console.

For additional information on using Out of Band Management, refer to the *HP Client Automation Out of Band Management User Guide*.

Device Type Selection

After enabling OOB Management, use the Device Type Selection area to select the type of OOB device you want to manage.

It is possible to make one of three choices for device type. These are explained in the following sections:

- DASH Devices on page 264
- vPro Devices on page 264
- Both on page 265

Depending on the device type that you chose, the HPCA Console displays an interface relevant to that selection as explained in Configuration and Operations Options Determined by Device Type Selection on page 265.

You can now go to the Operations tab and see the Out of Band Management section to view the OOB Management options.

For additional information on using Out of Band Management, refer to the *HP Client Automation Out of Band Management User Guide*.

DASH Devices

If you select DASH, you can enter the common credentials for the DASH devices if the DASH administrator has configured all of the devices to have the same username and password.

You can change the credentials the next time you visit this window if you have made a mistake entering them or if they have changed.

vPro Devices

If you select vPro devices, you must enter the SCS login credentials and the URLs for the SCS Service and Remote Configuration to access vPro devices.

You can change the credentials the next time you visit this window if you have made a mistake entering them or if they have changed.

Both

If you select both types of devices, you can enter the common credentials for the DASH devices and you must enter the SCS login credentials and the URLs for the SCS Service and Remote Configuration needed to access vPro devices.

Refer to Device Type Selection in the Administrative Tasks chapter of the *HP Client Automation Out of Band Management User Guide* for complete details.

Configuration and Operations Options Determined by Device Type Selection

After you make your device type selection, you will see options on the Configuration and Operations tab that reflect this selection. They are summarized in the following table.

Table 34   Configuration and Operations options

	DASH	vPro
Configuration	No additional options	vPro System Defense Settings
Operations	Device Management	Provisioning vPro Devices
		Group Management
		Alert Notification

▶ You must log out and log in again to the HPCA Console when you make or change your device type selection in order to see the device-type related options in the navigation panel on the Configuration and Operations tab.

vPro System Defense Settings

Before managing System Defense features on vPro devices and device groups you must define vPro System Defense Settings.

> This configuration option appears only if you have selected the vPro device type. System Defense settings do not apply to DASH devices.

- **Managing System Defense Filters**
  For vPro devices, you can create, modify, and delete System Defense filters. System Defense filters monitor the packet flow on the network and can drop or limit the rate of the packets depending if the filter condition is matched. Filters are assigned to System Defense Policies that can be enabled to protect the network.

- **Managing System Defense Policies**
  For vPro devices, you can create, modify, and delete System Defense policies and then deploy them to multiple vPro devices on the network. System Defense policies can selectively isolate the network to protect vPro devices from malware attacks.

- **Managing System Defense Heuristics Information**
  For vPro devices, you can create, modify, and delete heuristics specifications and then deploy them to multiple vPro devices on the network. These heuristics serve to protect the devices on the network by detecting conditions that indicate a worm infestation and then containing that device so that other devices are not contaminated.

- **Managing System Defense Watchdogs**
  For vPro devices, you can create, modify, and delete agent watchdogs and then deploy them to multiple vPro devices on the network. Agent watchdogs monitor the presence of local agents on the vPro device. You can specify the actions the agent watchdog must take if there is a change in state of the local agent.

For additional details, refer to vPro System Defense Settings in the Administrative Tasks chapter of the *HP Client Automation Out of Band Management User Guide* for complete details.

This is the last administrative task you have to perform on the Configuration tab to get the HPCA Console ready for you to manage System Defense features on vPro devices. Now, in the role of Operator or Administrator, you can go to the Operations tab and start to manage the OOB devices in your network as explained in the Operations chapter.

OS Management

Use the Operating System area to configure options pertaining to operating system deployment.

- Settings on page 268
- Deployment on page 268

Settings

The Operating Systems service allows Agents to connect to the HPCA server and retrieve their OS entitlements and provisioning information. The Operating System service setting is always enabled in the Starter and Standard editions of HPCA.During OS deployment, if you are planning to boot devices across the network, you must first enable the Boot Server (PXE/TFTP) installed with the Core. This will start two Windows services on the Core server: Boot Server (PXE) and Boot Server (TFTP).

- To enable the Boot Server (PXE/TFTP), select the **Enable Boot Server** box, and click **Save**.

You can host both the HPCA Boot Server (PXE) and a DHCP server on the same machine.

Deployment

Use the Deployment page to configure the global default settings for all operating system deployment operations. You can override these settings when you schedule a specific deployment using the OS Deployment Wizard.

▶ Changes made on this page affect all new and scheduled OS deployment jobs.

To configure the default settings for OS Deployment

1 On the Configuration tab, expand the OS Management section, and select the **Deployment** page.

2 On the Deployment Behavior tab:

   a Specify the Basic Deployment Behavior Properties.

b   Specify the Advanced Deployment Behavior Properties.

3   On the Partitioning Strategy tab:

a   Specify the Basic Partitioning Strategy Properties.

b   Specify the Advanced Partitioning Strategy Properties.

See OS Management on page 149 for more information about deploying operating systems.

Basic Deployment Behavior Properties

The Basic Properties area on the Deployment Behavior tab enables you to specify the default OS deployment mode and language settings. Note that these language settings apply only during the deployment process; they do not apply after the operating system is installed on the target device.

To specify the Basic OS Deployment Behavior Properties

1   Using the **When re-installing an OS** drop-down menu, specify the deployment mode:

— **Prompt User (Attended)** — A user must be present at the target device during operating system deployment to continue the deployment process.

— **Do not prompt user (Unattended)** — No dialogue windows are displayed on target 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.

2   Using the **Display Service OS messages in** menu, select the language that will be used to display messages on the target device while the Service OS is being installed.

3   Using the **Service OS keyboard layout** menu, select the keyboard layout that will be used if input is required on the target device during the installation of the OS.

4   Click **Save** to commit your changes.

Next Step: Specify the Advanced Deployment Behavior Properties.

Advanced Deployment Behavior Properties

The Advanced Properties area on the Deployment Behavior tab enables you to control the maximum OS image download speed and determine how various special cases should be handled during a deployment.

To specify the Advanced OS Deployment Behavior Properties

1   Specify the **Maximum OS Image download speed**. This is useful for managing network traffic—it enables you to set aside enough network bandwidth for business-critical applications while you are downloading the OS image to the target device. If you do not specify a value, HPCA will download the image as quickly as the network allows.

    If you specify a maximum download speed, be sure to also specify the **Units**.

2   Using the **Allow user to select which OS to install** menu, specify whether the user of the target device can choose which OS to install in the event that multiple OS are assigned to this device.

    When re-installing the exact same OS service on a device that is already managed by the HPCA OS Manager, selecting a value of **No** will disable an additional prompt during the maintenance OS installation phase

3   Using the **For a managed device, if the hard disk fails** menu, specify how HPCA should respond if the hard disk for a fully managed device fails:

    —   The administrator needs to take action (do nothing unless the administrator of the target device authorizes the OS re-installation)

    —   Automatically re-install the OS

4   Click **Save** to commit your changes.

Next Step: Specify the Basic Partitioning Strategy Properties.

Basic Partitioning Strategy Properties

The Basic Properties on the Partitioning Strategy tab of the Deployment page enable you to specify how HPCA should partition the hard disk when it installs the OS image on a target device. Different operating systems support different partitioning strategies.

⚠️ 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 are using Unattended deployment mode, be sure to back up existing data on the target devices before deploying a new operating system.

To specify the Basic Partitioning Strategy Properties for OS Deployment

1 In the Partitioning Strategy box, select the strategy that you want to use:

Strategy	Description
Remove existing partitions and install a single OS partition	Use this option when data on the target device does not need to be preserved. HPCA removes any existing partitions on the target device and creates a System Reserved partition (when supported) and an OS partition. IMPORTANT: All existing data on the target device will be lost.
Preserve existing data partitions and recreate a single OS partition	Use this option to replace (or update) the OS on a machine where existing data needs to be preserved. HPCA removes the existing OS partition (and the "System Reserved" partition, if it exists) and creates a System Reserved partition (when supported) and an OS partition. Any existing data partitions are not touched. • If the partitions to be installed are larger than the space already defined for these partitions, the installation will fail. • If the target drive does not contain existing partitions (bare metal, for example), then the result is the same as the Single OS partition option. NOTE: Use this option for migration purposes.

Strategy	Description
Remove existing partitions, install a single OS partition, and cache OS locally	Use this option to create a hidden back-up partition at the end of the target drive.
	The size of the partition will be dynamically determined by the size of the OS installation image. All files necessary to reinstall the OS will be saved (in compressed form) in this partition.
	IMPORTANT: All existing data on the target device will be lost.
Preserve existing data partitions and data restoration directory in the OS partition, and install OS	Use this option to preserve a set of files and folders on a target device during the installation of a new operating system and restore them after the OS installation. If you use this option, HPCA does not re-partition the disk.
	NOTE: This requires the ImageX method of OS deployment. Any attempt to use any other deployment method will result in an error.
	NOTE: You cannot use this option if your target device has a "System Reserved" partition in addition to the OS partition.

2   Click **Save** to commit your changes.

3   Specify the Advanced Partitioning Strategy Properties.

Advanced Partitioning Strategy Properties

The Advanced Properties on the Partitioning Strategy tab of the Deployment page enable you to specify the size of the System partition and any unpartitioned space on the hard disk of the target device prior to installing the operating system.

▶ These settings pertain only to Windows 7 and Windows Server 2008 R2 deployments.

To specify the Advanced Partitioning Strategy Properties for OS Deployment

1   In the **System partition size for Windows 7 / 2008 R2** box, specify the size (in MByte) of the System Reserve partition.

You can specify any non-negative five-digit value. If you specify a value that is too big, a warning appears in red. If you specify a value of 0 (zero), a System Reserve partition will not be created.

2 In the **Size of unpartitioned space at start of disk** box, specify the amount (in MByte) of unpartitioned space to leave at the beginning of the disk. This space can later be used, for example, to create a recovery partition.

If you specify a value of 0 (zero), a System Reserve partition will not be created.

3 Click **Save** to commit your changes.

To perform OS deployment operations, see OS Management on page 149.

Usage Management

Use the Usage Management section to configure usage database connection settings and usage data collection settings.

- Database Settings on page 274
- Settings on page 274

Database Settings

You can configure the usage database connection settings by using the Database Settings page.

To configure the usage database connection settings:

1 On the Configuration tab, click **Usage Management** and then **Database Settings**.

2 Specify the following Open Database Connection (ODBC) information:

    — **DSN** (data source name)

    — **User ID**

    — **Password**

    These settings must match the configured system ODBC DSNs on the Client Automation server. If the specified database has not yet been initialized, it will be initialized when these settings are saved.

3 Click **Save**.

Settings

Usage data is collected when the Usage Collection Agent is deployed. Usage settings are applied to existing client devices during their collection schedule. If required, usage data can be obfuscated to ensure privacy.

➤ Obfuscation should be enabled prior to deploying the Usage Collection Agent. If it is enabled after this agent is deployed, some reporting data will appear in both obfuscated and non-obfuscated forms.

1 Use the drop-down lists to select which usage data information should be hidden:

   — **Computer** – Hide computer-related information. The computer name is reported as a random set of alphanumeric values.

   — **User** – Hide user-specific information. The user name is reported as [AnyUser].

   — **Domain** – Hide domain information. The domain name is 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.

   Select **Enabled** next to the usage information that you want to obfuscate within the usage reports.

2 Click **Save** to commit the changes.

See the Application Usage Collection Wizard to deploy the Usage Collection Agent and define a collection schedule.

Dashboards

Use the Dashboards area on the Configuration tab to configure the dashboards:

The HPCA Operations dashboard provides information about the number of client connections and service events that have occurred over a given period of time.

The Patch Management dashboard provides data pertaining to patch policy compliance on the client devices in your enterprise.

By default, a subset of the dashboard panes are enabled. Provided that you have administrator privileges, you can enable or disable any of the panes.

HPCA Operations

The HPCA Operations dashboard shows you the work that HPCA is doing in your enterprise. The client connection and service event metrics are reported in two time frames. The Executive View shows the last 12 months. The Operational View shows the last 24 hours. Both views contain the following information panes:

Client Connections on page 67

Service Events on page 69

The Executive View also includes the following pane:

12 Month Service Events by Domain on page 71

All of these panes are visible by default. You can use the configuration settings to specify which panes appear in the dashboard. For detailed information about these panes, see the HPCA Operations Dashboard on page 66.

To configure the HPCA Operations dashboard:

1   From the Configuration tab, click **Dashboards**.

2   Under Dashboards, click **HPCA Operations**.

    This dashboard is enabled by default. To disable it, clear the **Enable HPCA Operations Dashboard** box, and click **Save**.

3   Under HPCA Operations, click either **Executive View** or **Operational View**.

4   Select the box for each pane that you want to show in the dashboard. Use the ⍰ icon to display information about any related HPCA configuration that is required for each pane.

5   Click **Save** to implement your changes.

Patch Management

The Patch Management dashboard provides information about any patch vulnerabilities that are detected on managed devices in your network. By default, the Patch Management dashboard is disabled.

The Executive View of the Patch Management dashboard includes two information panes:

- Device Compliance by Status (Executive View) on page 73
- Device Compliance by Bulletin on page 75

The Operational View includes the following information panes:

- Device Compliance by Status (Operational View) on page 79
- Microsoft Security Bulletins on page 80
- Most Vulnerable Products on page 81

You can use the configuration settings to specify which panes appear in the dashboard. For detailed information about these panes, see the Patch Management Dashboard on page 73.

To configure the Patch Management dashboard:

1 From the Configuration tab, click **Dashboards**.

2 Under Dashboards, click **Patch Management**.

By default, this dashboard is disabled. To enable it, select the **Enable Patch Dashboard** box, and click **Save**.

3 Under Patch Management, click either **Executive View** or **Operational View**.

4 Select the box for each pane that you want to show in the dashboard. Use the ? icon to display information about any related HPCA configuration that is required for each pane.

The following requires additional information:

— **The Microsoft Security Bulletins (Operational View)**

a Specify the URL for the Microsoft Security Bulletins RSS feed

Currently a valid default URL is provided. You may also need to enable a proxy server on the **Console Settings** page.

5 Click **Save** to implement your changes.

10 Wizards

While using the HPCA console, you will use many different wizards to perform various management functions. 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.

▶ The HPCA console may open additional browser instances when running wizards or displaying alerts. To access these wizards and alerts, you must include the console 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 on page 282.

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 Input** – Type or paste a list of device host names or IP addresses into the text box provided. You can also type a range of IP addresses separated by hyphen. For example, to import the devices in the range *xx.yy.zz.12* to *xx.yy.zz.19*, type *xx.yy.zz.12-xx.yy.zz.19*.

► If you use this option to manually import a device and later perform a domain scan (using the **Domain** option below), a duplicate device entry may be created. This is possible because the device that has been manually added may not have enough identifying attributes (such as MAC address, dnshostname, and so on) to uniquely identify it when a subsequent domain scan is triggered. As a result, a newly discovered device may not match the manually added one although it is the same device, creating a duplicate entry. To avoid this behavior, trigger device discovery using the **Domain** option instead of the **Manual Input** option.

— **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 on page 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 close 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.

▶ Using the agent removal wizard to remove a manually installed agent (an agent installed though the setup.standard.cmd command) causes the job to end in error. However, the agent is successfully removed despite the generated error condition.

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.

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 if you want to Power On 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.

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 to Power On 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.

Power Management Wizard

Use the Power Management wizard to turn on, turn off, or restart selected devices.

> Remotely powering on a device requires the Wake-On-LAN capability built into modern computers. Wake-On-LAN is a management tool that enables the HPCA 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 HPCA.

> When Out of Band Management is enabled, vPro or DASH devices can be contacted through the OOB Management remote operations capability in addition to the normal Wake on LAN capabilities of the HPCA console.

> 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.

1   Launch the wizard from the Device Management, Devices tab or from the

    Group Management, Groups tab by clicking the **Power Management** (icon)
    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, and 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   There are three ways to launch the wizard:

   — From the Software Management, General tab, click **Deploy.**

   — From the Software Management, Software Tab tab, select the
       software that you want to deploy, and click the **Deploy Software**
       button.

   — From the Software Details window (or the Group Details window),
       click the **Deploy Software** link on the General tab.

You can open the Software Details window from the Software tab on the Software Management page on the Management tab or the Software Library page on the Operations tab. Click the Service ID for any software service listed to open the Software Details window.

2   Click **Next** to launch the wizard.

3   If you launched the wizard from the Software Management, General tab:

   a   To select the software to entitle and deploy, check one or more boxes in the first column.

   b   Click **Next**.

4   To select the groups that will be entitled and targeted for deployment, check one or more boxes in the first column.

5   Click **Next**.

6   Configure the run schedule for the software deployment job:

   — Select **Run: Now** to deploy the software right away.

   — Select **Run: Later** to schedule a date and time for software deployment.

   — To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks**, and then select the **Interval** from the drop-down list.

   ▶   Recurring job schedule options (Every 'x' Days, for example) are available only when you are creating group-related jobs.

7   Specify any Additional Parameters listed. Hover your mouse over the tooltip ⁇ icon to learn more about a specific parameter.

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.

Settings Profile Deployment Wizard

Use the Settings Profile Deployment Wizard to deploy entitled settings profiles to or remove unentitled settings profiles from the managed devices in your environment.

To deploy or remove settings profiles using the Settings Profiles Deployment wizard

1   On the Management tab, click **Settings Management**. The Settings Management window opens.

    The Settings Profiles tab displays the settings profiles that are available in HPCA for deployment or removal. It shows the number of entitled groups and installed devices associated with each profile.

2   Check the box next to the Display Name of those profiles that you want to deploy. Selected profiles will be automatically entitled (if they are not entitled already) regardless of the deployment method you choose as described in step 4.

3   Click **Deploy Settings Profile** on the toolbar. The Settings Profile Deployment Wizard opens. This wizard allows you to deploy or remove profiles to/from device groups.

4   Click **Next** to begin the wizard. The Deployment Method window opens. There are two possible methods of deployment:

    — **Profile Enforcement** - This option determines which profiles are entitled and automatically manages (deploys or removes) profiles based on entitlement. As new profiles are entitled, the next time the deployment job runs, the newly entitled profiles will be deployed to the target devices. This is the recommended method of deployment.

    ▶ The only way to remove settings profiles is to unentitle the profile first and then select the Profile Enforcement method of deployment.

— **Manual Selection** - This option performs a one-time deployment of the selected profiles to the target devices. The Manual Selection option is an expedient way to immediately push out a profile for one time.

▶ To automatically manage (deploy or remove) profiles on the target devices, use the Profile Enforcement option. It is best to schedule a recurring job to manage the ongoing profile settings on target devices.

5 Click **Next**. The Groups window opens displaying the available groups.

6 Check the box next to the name of the group(s) to which you want the settings profile(s) to be entitled and deployed. This would be the group or groups that you specifically created for this entitlement.

7 Click **Next** to continue. The Schedule window opens.

8 Specify the job schedule information for the settings profile deployment.

9 Click **Next** to continue. The Summary window opens.

10 Review the information in the summary window.

11 Click **Submit** if it is accurate. The Complete window opens with a progress statement.

12 Click **Close** to exit the wizard.

13 Select the Current Jobs tab to view the status of the deployment job that you have scheduled. It should eventually report a successful status confirming the deployment job has been successfully scheduled.

14 Select the Settings Profiles tab to view the number of entitled groups and installed devices for the newly deployed settings profiles. These numbers should be updated accordingly to reflect your deployment choices.

15 Click on a **Display Name** for a newly deployed settings profile. The Settings Profile Details window opens.

— On the General tab, you can confirm that the summary information reflects the newly established group/device entitlement.

— On the Properties tab, you can view the properties for the settings profile.

— On the Groups tab, you can deploy or remove the settings profile, and you can add or remove entitlement.

— On the Devices tab, you can deploy or remove the settings profile.

— On the Reporting tab, you can view a contextual report based on the selected settings profile.

▶ If you deploy a profile and later change the settings to that profile, it must be redeployed. To facilitate redeployment, you can use a recurring profile deployment job, which will re-apply the settings on a periodic basis. To schedule a recurring profile deployment job, you must select the Profile Enforcement method of deployment.

▶ If you want to remove a profile from a device, you must:

• Unentitle the profile for that device

• Ensure that a deployment job (with the Profile Enforcement method specified) is scheduled which targets that device

When that job runs, the unentitled profile will be removed from the target device.

Service Import Wizard

Use the Service Import Wizard to import services from the ServiceDecks directory on the HPCA server into the Software, Patch, or OS library. By default, this directory is located here:

<InstallDir>\Data\ServiceDecks

To import a service using the Service Import wizard

1   On the **Operations** tab, click the **Import Service** toolbar button from any of the following pages:

   — **Software Management** > **Software Library**

   — **Patch Management** > **Patch Library**

   — **OS Management** > **OS Library**

   This launches the wizard.

2   Select the service to import. All service decks in the HPCA server's ServiceDecks directory whose names contain the following words appear in the list of available services:

Library	Service Deck Name Must Contain	HPCA Domain
Software	SOFTWARE	SOFTWARE
Patch	PATCH	PATCHMGR
OS	OS	OS

By default, the ServiceDecks directory is located here:

<InstallDir>\Data\ServiceDecks

The fourth section of each service's file name contains a descriptive name for that software service, patch, or OS. For example, the service deck for the Orca software application is:

PRIMARY.SOFTWARE.ZSERVICE.ORCA

3   Review the summary information, and click **Import**. The service is imported and will now be available in the pertinent (Software, Patch, or OS) HPCA library.

4   Click **Close** to exit the wizard.

Service Export Wizard

Use the Service Export Wizard to export services from the HPCA Software, Patch, or OS libraries to the `ServiceDecks` directory on the HPCA server machine.

To export a service using the Service Export wizard

1   On the **Operations** tab, click the **Export Service** toolbar button from any of the following pages:

   — **Software Management** > **Software Library**

   — **Patch Management** > **Patch Library**

   — **OS Management** > **OS Library**

   This launches the wizard.

2   Select the service to export.

3   Review the summary information and click **Export**. The service is exported to the HPCA server's `ServiceDecks` directory. By default, this directory is:

   `<InstallDir>\Data\ServiceDecks`

   A service deck consists of several files, all of which have the same file name prefix. For example, the service deck name for the Orca software application is:

   PRIMARY.SOFTWARE.ZSERVICE.ORCA

   The fourth section of each file name in the service deck contains the descriptive name for the software, patch, or OS that was exported.

4   Click **Close** to exit the wizard.

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 Power On drop-down list to enable Wake-on-LAN for devices in the group. This allows HPCA 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 click **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

1   On the Management tab, click the **Add Group Entitlement** 🔖 toolbar button from any of the following pages:

    —   Software Management > Software Tab

    —   Patch Management > Patches Tab

    —   OS Management > Operating Systems Tab

    This launches the wizard.

2   To select the groups that will receive entitlement to the service (or services), select 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. To view its status and progress, click the Current Jobs tab.

5   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.

OS Deployment Wizard

The OS Deployment wizard enables you to deploy operating systems to managed devices. Operating systems are deployed in either attended or unattended mode. For more information about deployment modes, see OS Management on page 268.

For an example, see How to Re-Install the Same OS Silently on page 307.

To deploy an operating system using the OS Deployment wizard

1   From the Management tab, OS Management section, click the **General** tab.

2   Under Common Tasks, click **Deploy Operating Systems**. The OS Deployment Wizard opens.

3   Follow the steps in the wizard to set up your OS deployment job.

Step 1– Introduction

If you are deploying Windows XPe, Windows CE, or Embedded Linux, select **Thin Client deployment**. Otherwise, make sure this box is not selected.

Click **Next** to proceed.

Step 2 – Operating Systems

From the OS Selection list, select the operating system that you want to deploy, and click **Next**.

All operating systems that have been published to the HPCA database are available in this list. See Publishing Operating System Images on page 352 for more information.

Step 3 – Groups

Select one or more groups of target device from the list, and click **Next**.

You can create static groups using the Groups page on the Configuration tab (see Group Management on page 114), or you can create dynamic groups on the Reporting tab (see Creating Dynamic Reporting Groups on page 179).

Groups created for OS deployment should have similar, compatible hardware.

On this page, you will specify settings that determine how the OS deployment is performed. These settings override the global default settings specified in the OS Management area on the Configuration tab.

OS Deployment Method Settings:

— **Deployment Method**

Select **Local Service Boot (LSB)** 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.

In a single-partition Windows 7 Local Service Boot (LSB) deployment, the Service OS (SOS) files are installed on both the System Reserved partition and the local disk partition. Do not delete these files from either partition.

Select **Local CD or PXE Server** if you will be using a PXE Server or Service CD to install the operating system on your devices.

— **Migrate User Data & Settings**

If you selected **Thin Client deployment** in Step 1, this option is not available.

Select **Yes** to backup user data and settings prior to the OS deployment and to restore them afterwards. During the operating system deployment, the HPCA Personality Backup service runs silently to back up user data.

After the new operating system is installed, there are three ways to restore the user data:

– The user of the managed device can run the HPCA Personality Backup and Restore Utility. The user must select the **Restore from operating system migration** option.

– You can run the pbr.exe command on the managed device.

– You can deploy the HPCA Personality Restore service from the Software Library to the managed device. The service will run once to restore the user data.

▶ Personality Backup is supported only on source computers that are running Windows XP, Vista, or Windows 7.

Personality Restore is supported only on destination computers that are running Windows XP, Vista, or Windows 7.

In addition, the current operating system and the operating system image being deployed must include an installation of USMT 3.0.1 or USMT 4.0 (see Personality Backup and Restore on page 387).

— **When re-installing an OS**

If you select **Prompt User (Attended)**, a user must be present at the managed device during operating system deployment to continue the deployment process.

If you select **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.

Additional OS Settings:

— **Maximum OS Image download speed**.

This is useful for managing network traffic—it enables you to set aside enough network bandwidth for business-critical applications while you are downloading the OS image to the target device. If you do not specify a value, HPCA will download the image as quickly as the network allows.

— **Units**

If you specify a maximum download speed, be sure to also specify the correct units.

— **Display Service OS messages in**

Select the language that will be used to display messages during OS deployment.

— **Service OS keyboard layout**

Select the keyboard layout that will be used if input is required during OS deployment.

Step 5 – Partitioning

On this page, you will specify how the hard disk on the target devices should be partitioned prior to the OS deployment.

▶ If you selected **Thin Client deployment** in Step 1, you cannot change the Partitioning settings. Proceed to Step 6.

Basic Properties:

— **Partitioning Strategy**

Strategy	Description
Remove existing partitions and install a single OS partition	Use this option when data on the target device does not need to be preserved.
	HPCA removes any existing partitions on the target device and creates a System Reserved (when supported) and an OS partition.
	IMPORTANT: All existing data on the target device will be lost.

Strategy	Description
Preserve existing data partitions, and recreate a single OS partition	Use this option to replace (or update) the OS on a machine where existing data needs to be preserved.
	HPCA removes the existing OS partition (and the "System Reserved" partition, if it exists) and creates a System Reserved (when supported) and an OS partition. Any existing data partitions are not touched.
	• If the partitions to be installed are larger than the space already defined for these partitions, the installation will fail.
	• If the target drive does not contain existing partitions (bare metal, for example), then the result is the same as the Single OS partition option.
	NOTE: Use this option for migration purposes.
Remove existing partitions, install a single OS partition, and cache the OS locally	Use this option to create a hidden back-up partition at the end of the target drive.
	The size of the partition will be dynamically determined by the size of the OS installation image. All files necessary to reinstall the OS will be saved (in compressed form) in this partition.
	IMPORTANT: All existing data on the target device will be lost.

Strategy	Description
Preserve existing data partitions and the data restoration directory in the OS partition, and install the OS	Use this option to preserve a set of files and folders on a target device during the installation of a new operating system and restore them after the OS installation. If you use this option, HPCA does not re-partition the disk.
	NOTE: This requires the ImageX method of OS deployment. Any attempt to use any other deployment method will result in an error.
	NOTE: You cannot use this option if your target device has a "System Reserved" partition in addition to the OS partition.
	NOTE: If you select this option, the two settings under Advanced Properties cannot be changed. Proceed to Step 6.

Advanced Properties:

— **System partition size for Windows 7 / 2008 R2**

Specify the size (in MByte) of the System Reserve partition.

You can specify any non-negative five-digit value. If you specify a value that is too big, a warning appears in red. If you specify a value of 0 (zero), a System Reserved partition will not be created.

— **Size of unpartitioned space at start of disk**

Specify the amount (in MByte) of unpartitioned space to leave at the beginning of the disk. This space can later be used, for example, to create a recovery partition.

If you specify a value of 0 (zero), no unpartitioned space will be reserved.

Step 6 – Schedule

On this page, you will specify when the HPCA job that performs this OS deployment will start. You can perform the deployment once or on a periodic basis.

— **Job Schedule**

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 are available only when you are creating group-related jobs.

— **Additional Parameters**

In the Power On menu, select **Yes** if you want HPCA to use the Out of Band Management feature (if it is enabled) to power on target devices. If you select **No**, Wake-On-LAN is used.

Step 7 – Summary

Review the settings for this OS deployment. To change a setting, click the **Previous** button until the appropriate wizard page appears. When you are ready to proceed, click **Submit**.

Step 8 – Complete

This page indicates whether the OS deployment job was successfully submitted to HPCA.

You can view the status of the job on the Current Jobs tab. Click the Refresh 🔄 button if the job is not immediately visible.

How to Re-Install the Same OS Silently

You can silently re-install an existing operating system provided that the following conditions are true:

- The target device is already managed by HPCA.
- The existing OS was installed by HPCA.
- You are installing exactly the same OS service that was previously installed.

If these conditions are true, and you set the deployment options as specified in the following procedure, you can control the re-installation of the OS from the HPCA console, and no user interaction on the target device will be required.

To silently re-install the same OS image

1 On the Configuration tab, go to the **OS Management** > **Deployment** page.

2 On the Deployment Behavior tab, specify the following:

   — For "When re-installing an OS" select **Do not prompt user (Unattended)**.

   — For "Allow user to select which OS to install" select **No**.

3 Click **Save**.

4 Launch the OS Deployment Wizard (see OS Deployment Wizard on page 300).

5 In the Deployment Behavior step, verify that "When re-installing an OS" is set to **Do not prompt user (Unattended)**.

6 Complete the remaining steps in the OS Deployment Wizard.

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 Usage Collection Agent on the targeted devices and then returns usage data based on filters that you create and enable (see Usage Collection Filter Creation Wizard on page 308).

1 On the Management tab, click **Devices** or **Groups**.

2 Click the **Inventory Collections** 🔍 toolbar button, and then select **Discover Application Usage**. The wizard opens.

3 Select one of the following options:

— Select **Run: Now** to schedule the job to run immediately after the wizard is complete.

— 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 only when you are creating group-related jobs.

Collecting application usage data on a weekly basis is recommended.

4 If you want to **Power On** the device, select **Yes** from the drop-down list. This allows HPCA to turn on the device, if necessary.

5 Review the summary information, and click **Submit**.

This creates a job that will install the Usage Collection Agent on the target devices and collect usage information from them. You can view all pending jobs by clicking **Current Jobs** in the Jobs area.

6 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 On the Operations tab, click **Usage Management**, and then click **Collection Filters**.

2   Click the **Create New Filter** ![icon] toolbar button. The wizard opens.

3   To configure the filter parameters, type the filter criteria into each text box.

     Only type values for those fields that you wish to filter usage data against. Empty text boxes are ignored and not used as part of the filter criteria.

     The values that you enter are compared to the file header in the software executable file to determine if the collected usage data meets the filter criteria.

     See Dashboards on page 275 to determine 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.

4   Click **Create.**

5   Click **Close** to exit the wizard.

     A new filter is added to the Collection Filters list.

Satellite Server Deployment Wizard

Use the Satellite Server Deployment Wizard to install the Satellite Server and enable remote services, such as data caching.

To deploy the Satellite Server

1   On the **Configuration** tab, goto the **Infrastructure Management** > **Satellite Management** area.

2   Click the **Servers** tab.

3   Select one or more devices in the Satellite Servers list.

     Any existing HPCA Satellite Servers or Legacy Proxy Servers selected will be automatically upgraded to the latest HPCA Satellite Server version.

4   Click the **Install the Satellite Server** ![icon] toolbar button to launch the wizard.

5   Enter the **User ID** and **Password** with administrator level access on the target device.

6   Click **Next**. The Properties window opens.

7   Select the **Installation Drive** and **Data Drive**.

> If you want to install the Satellite to a location other than the default location, you must follow these steps prior to the installation:
>
> a   Copy all of the HPCA installation files for Satellite from the HPCA media to the target machine.
>
> b   Edit the parameters INSTALLDIR and DATADIR in the setup.ini file.
>
> c   Run the setup.exe.

8   For HPCA Standard and Starter Editions, only Streamlined (Standard) deployment mode is available. Click **Next**. The Schedule window opens.

9   Specify the run schedule for the deployment job. Select **Run: Now** to deploy the Satellite Server right away, or select **Run: Later** to schedule a date and time for deployment.

10 Click **Next**. The Summary window opens.

11 Review the summary information.

12 Click **Submit**.

    A Satellite Server Deployment job is created.

    The Satellite Server download file is large. The deployment may take a long time if network traffic is heavy. You can check the status of the job in the Job Management area on the Management tab.

13 Click **Close** to exit the wizard.

Satellite Server Removal Wizard

Use the Satellite Server Removal Wizard to uninstall the Satellite Server from one or more devices in the HPCA Satellite Servers group.

1   On the Configuration tab, go to the Infrastructure Management, Satellite Management area.

2   Click the **Servers** tab.

3   Select one or more devices in the Satellite Servers list.

4   Click the **Uninstall the Satellite Server** 🖥 toolbar button. The Credentials window opens.

5   Enter the User ID and password with administrator level access on the Satellite server.

6   Click **Next**. The Schedule window opens.

7   Select **Run: Now** to uninstall the Satellite Server immediately after the wizard is complete, or select **Run: Later** and enter a date and time for the uninstall.

8   Click **Next**. The Summary window opens.

9   Review the summary information and click **Submit**.

    A Satellite Server Removal job is created. You can check the status of the job in the Job Management area of the Management tab.

10 Click **Close** to exit the wizard.

Server Pool Creation Wizard

Use the Server Pool Creation Wizard to create new Server Pools for Core and Satellite Servers. Server Pools enable software load balancing of client connections.

To add a new Server Pool

1   On the Configuration tab, go to the Infrastructure Management, Satellite Management area.

2   Click the **Server Pools** tab.

3   Click **Create a New Server Pool** 🖼 toolbar button to launch the Server Pool Creation Wizard. The properties page of the Server Pool Creation Wizard opens.

4   In the Properties area, specify the following:

 — **Name:** Enter a name for the new Server Pool.

 — **Description:** Enter a user-friendly description. This is optional.

 — **Enabled:** Indicates if this Server Pool should be enabled or not. A Server Pool must be enabled in order for client devices to contact the Server Pool and its Servers. A Server Pool can be disabled to prevent connections to the Server Pool during maintenance periods.

5   Click **Next**. The Server Selection window opens.

6   Select the Servers that will be members of this Server Pool. Members of this Server Pool will be randomly selected by each agent when resources are needed. A Server Pool can contain a maximum of 30 Servers.

7   Click **Create** to exit the wizard.

The new Server Pool is displayed on the Server Pools tab showing the number of Servers that are members in this pool.

Location Creation Wizard

Use the Location Creation Wizard to add new Locations. You can assign subnets and resources to these Locations and also set a priority order. Setting priority ensures that devices located in the subnets connect to resources in the indicated order.

To create a new location

1   On the Configuration tab, go to the Infrastructure Management, Satellite Management area.

2   Click the **Locations** tab.

3   Click the **Create a New Location** 🖼 toolbar button. The Location Creation Wizard opens.

4   In the Properties area, specify the properties for this Location. Name is the only required field, and it must be unique.

5   Click **Next**. The Subnet Selection window opens.

6   Select the Subnets to assign to this Location.

7   Click **Next**. The Connections window opens. You can either add a new connection or import an existing one.

To add a connection:

a   Click an **Add Connection** link to define a connection assignment for this Location. The Location Connection Selection window opens.

b   Select a resource from the available types to assign to this Location. Agent connections will attempt to use resources from the selected Server or Server Pool.

c   Click **Add Connection**.

To import a connection:

a   Click **Import Connections**. The Location Selection window opens.

b   Select a Location to import its connections.

➤   An existing connection is be lost if you import the connections of another Location.

c   Click **Import Connections**.

8   Change the order of the Connections as required. Use the up and down arrows in the Reorder column to establish the required order. The devices attempt to contact the Servers or Server Pools in this new order.

9   Click **Create**.

The new Location appears on the Location tab.

Subnet Creation Wizard

Use the Subnet Creation Wizard to add new Subnet addresses to which managed devices can be assigned. Managed devices will connect to Satellite Servers based on Subnet assignment to Locations.

1   On the Configuration tab, go to the Infrastructure Management, Satellite Management area.

2   Click the **Subnets** tab.

3   Click the **Create a New Subnet** toolbar button. The Subnet Creation Wizard opens.

4   In the Properties area, specify the following:

   — **IP Address**: Enter a valid IP address.

   — **Subnet Mask**: Enter a valid subnet mask.

   — **Subnet**: This field automatically generates the Classless Inter-Domain Routing (CIDR) address if you have entered a valid IP address and subnet mask.

   — **Name**: Enter a name for the new Subnet.

   — **Description**: Optionally enter a user-friendly description.

   — **Assigned Location**: Select a Location from the pull-down menu. The Locations available are the Default Location and Locations that you have added through the Location Creation Wizard.

5   Click **Create**.

The new Subnet IP address is displayed on the Subnets tab.

11 Patch Management Using Metadata

HPCA provides a lightweight model for acquiring and delivering patch updates to your Agent devices. Because the model only uses Metadata to perform the patch scans on your agents, it is called Patch Management using Metadata.

The chapter discusses the concepts, configuration and implementation details needed to take advantage of Patch Management using Metadata.

Patch Management using Metadata is only available for:

- Microsoft operating systems using a Microsoft Update Catalog data feed.
- HPCA Core and Satellite Enterprise-level and Standard-level environments.

Overview

The lightweight Patch Management using Metadata model is currently available for patching Microsoft devices and requires the use of a Microsoft Update Catalog feed.

It offers several advantages that are described below and illustrated in

The Metadata Patch Management model differs from the traditional HPCA patching model in that:

1 Only the bulletin Metadata information is stored in the Core server HPCA Database, and not the actual patch binaries.

This model makes patch acquisition run faster and also eases the load on the infrastructure traffic when running the Patch Discovery on an Agent and when synchronizing the HPCA servers.

2   The actual patch binaries are downloaded and cached on the Patch Gateway, a component of both the Core and Satellite server. The Gateway downloads the patch binaries upon the first request from an agent machine and caches them for other agent machines to use. Optionally, the Patch Gateway can have patch binaries preloaded onto it when you run an acquisition.

3   When using the Metadata model, the Agents must have the Download Manager enabled which allows them to contact the Patch Gateway at the end of the scanning phase with requests for applicable patch binaries.

The Download Manager handles the passive transfer of the patch files to the Agents. Once the file transfer is complete, an Agent connection is triggered to have the patches installed.

Figure 16 on page 317 illustrates the Patch Management using Metadata model.

For comparison, Figure 17 on page 318 illustrates the traditional Patch Management model.

Figure 16 Patch Management using Metadata Model
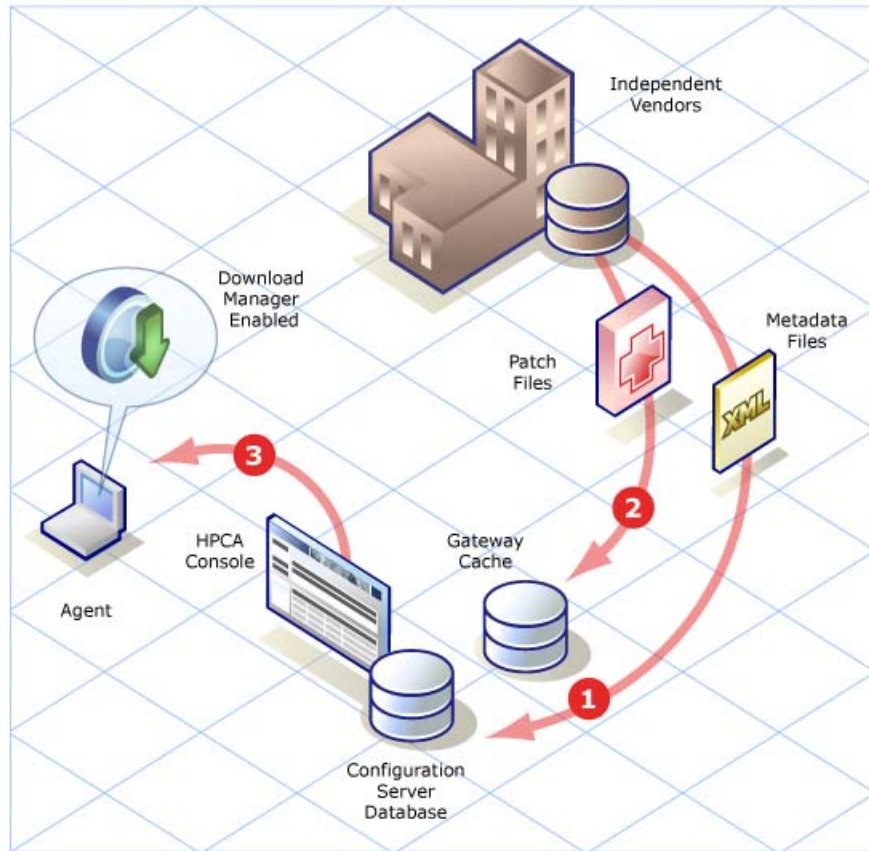
Legend:

1 A Patch Acquisition downloads only patch metadata files from the Vendor. The patch metadata is published to the Core HPCA database and used to discover the exact list of patch files required by the Agents being managed.

2 Upon request by an Agent (or optional preload), the Patch Gateway downloads the patch files from the Vendor and caches them for additional Agents to use. The patch files never need to be published to the HPCA database.

3　Patch Agents require the Download Manager to be enabled. The Download Manager uses a background process to handle the passive download of the required patch files onto the Agent.

Figure 17 Patch Management Model - traditional
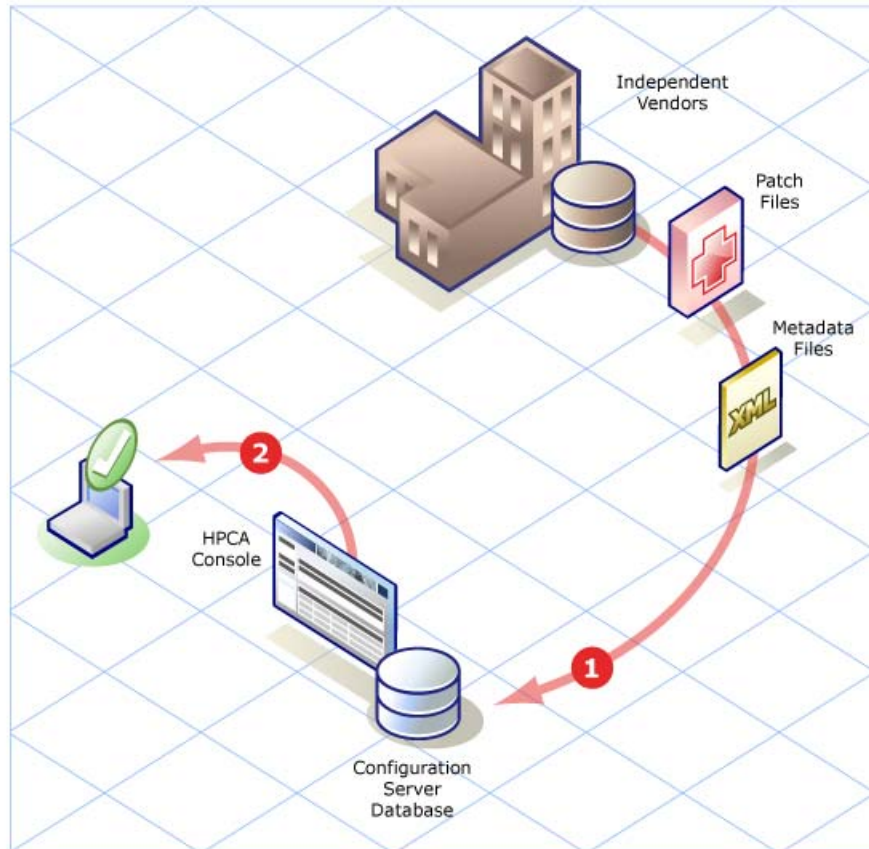
Legend:

1　A traditional Patch Acquisition downloads both metadata and all related patch files for bulletins from the Vendor. All of these files are published to the Core HPCA database, regardless of whether Agents in the enterprise require them or not.

2   Patch Agents can be patched with or without the use of the Download Manager option. Without it, the Agent connect handles the download of the required patch files in a foreground process. In contrast, the Download Manager uses a background process to handle the passive download of the required patch files onto the Agent.

Enabling on the Satellite

To enable the Patch Gateway on the Satellite server

1   From the Satellite Console, select the Configuration tab and click **Patch Management**. This option allows you to enable or disable the Patch Gateway.

When you disable the Patch Gateway, the Satellite server will forward the request for the patch binaries to the upstream server. This is the default setting for this option.

When you enable the Patch Gateway, the Satellite server will retrieve the patch binaries directly from the Internet. This is the recommended way for acquiring binaries.

2   If you enable the Patch Gateway, you will have to configure additional options.

3   Click **Save** to save your settings.

12 Preparing and Capturing OS Images

Introduction

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

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

To capture images of older operating systems, see Capturing Windows XP and Windows Server 2003 OS Images on page 469.

⚠ If you are prompted for the OS Manager Server's IP address and port number, you must specify the HPCA server port number (by default 3466).

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

Process Overview

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

Prepare the reference machine

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

See Preparing the Reference Machine on page 325.

Capture an OS image

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

See Capture the OS Image on page 328.

Publish the image

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

See Publishing Operating System Images on page 352.

Deploy the image

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

See OS Management on page 149.

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

Preparing and Capturing Desktop OS Images

The information in this section pertains to desktop, laptop, notebook, netbook, and workstation client devices. For information about Thin Client devices, see

Prerequisites

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

  Refer to the *Installing HPCA* chapter for more information.

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

  http://www.microsoft.com/downloads

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

  `%SYSTEMROOT%/Microsoft.NET/Framework`

- HPCA does not verify that enough free disk space exists on the Core server to successfully upload the OS image after it is captured. If sufficient free space is not available, the upload will fail.

  Make sure that enough free disk space exists on the Core server so that the OS image upload can be successfully completed.

- To capture Microsoft Windows Vista and above OS with a separate boot partition successfully, the size of the boot partition must be 300 MB at minimum. If it is less than 300 MB, increase the size to a minimum of 300 MB. The recommended boot partition size is one GB.

  If you have customized the `winpe.wim` image file, set the size of the boot partition to double of the size of your winpe.wim file. For example, if the size of the `winpe.wim` file is 200 MB, set the size of the boot partition to a minimum of 400 MB.

About the OS Image Capture Tool

The HPCA OS Image Capture tool performs the following tasks:

1   Collects and stores information (including hardware and OS information capabilities) about the reference machine.

2   Runs Microsoft Sysprep.

3   Restarts the reference machine into the Service OS (booted from the appropriate media). The Service OS runs to collect the image and its associated files.

4   Creates and copies files to the following directory on the HPCA server:

    `<InstallDir>\Data\OSManagerServer\upload`

    The files uploaded are:

    —   `ImageName.WIM`
        This file contains a set of files and file system information from the reference machine.

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

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

http://www.microsoft.com/downloads

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

`%SYSTEMROOT%/Microsoft.NET/Framework`

Preparing the Reference Machine

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

Windows 7 or Windows Server 2008 R2 x64

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

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

    — When you are prompted for the type of installation, select the **Custom (advanced)** option.

    — When you are prompted for where to install Windows 7, click **Drive Options (advanced)**.

2   Click **New** to create a new partition that will hold Windows 7.

3   In the **Size** box, select the maximum value.

4   Click **Apply**. A dialog box opens to warn you that Windows may create additional partitions. Click **OK** to close this dialog box and proceed.

5   To create a **single partition** installation, follow these steps:

    a   Select the small System Reserved partition, and click **Delete**. A dialog box opens to warn you that any data stored on this partition will be lost.

    b   Click **OK** to close the dialog box and proceed.

    c   Select the remaining partition, and click **Next**. The Windows 7 installation then proceeds.

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

a   Select the partition that you created in step 4, and click **Delete**. A dialog box opens to warn you that if you delete this partition, any data stored on it will be lost.

b   Click **OK** to close the dialog box and proceed.

c   Select the System Reserved partition, and click **Extend**.

d   In the **Size** box, specify 1024 MB.

e   Click **Apply**. Once again, a dialog box opens to warn you that extending a partition is not a reversible action.

f   Click **OK** to close this dialog box and proceed.

g   Select the partition that you created in step 4 again, and click **New**.

h   In the **Size** box, select the maximum value.

i   Click **Apply**. Once again, a dialog box opens to warn you that Windows may create additional partitions.

j   Click **OK** to close this dialog box and proceed.

k   Click **Next**. The Windows 7 installation then proceeds.

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

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

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

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

9   Using the Control Panel, set the User Access Control level to **Never notify**.

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

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

a Delete unnecessary files and directories from the files system.

b Turn off System Restore.

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

Windows Vista or Windows Server 2008

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

⚠️ Store the OS on the C: drive. It is the only drive that will be captured.

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

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

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

3 Turn off User Access Control.

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

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

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

   a   Delete unnecessary files and directories from the files system.

   b   Turn off System Restore.

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

Capture the OS Image

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

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

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

➤   The OS Image Capture tool supports Windows Preinstallation Environment (Windows PE) based captures only. To perform Thin Client captures, see Preparing and Capturing Thin Client OS Images on page 332. To capture older OS images, see Capturing Windows XP and Windows Server 2003 OS Images on page 469.

1   Log on to the reference machine using an account with administrator privileges.

2   Insert the ImageCapture media CD into the reference machine.

    See *Product Media* in the *HP Client Automation OS Management Reference Guide* if you need more information about where to get this media.

3   On the ImageCapture CD, browse to the following folder:

    image_preparation_wizard\win32

4   Run oscapture.exe.

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

▶   If the operating system on the reference machine is older than those listed above, the HPCA Image Preparation Wizard opens instead. See Capturing Windows XP and Windows Server 2003 OS Images on page 469 for more information.

5   Click **Next** to proceed. The Imaging Options page opens.

Imaging Options

Use the Imaging Options page to specify the following information:

- **Imaging Method** – Select ImageX or Windows Setup.

    — ImageX captures an image in .WIM format that will be deployed using Windows PE and the ImageX utility.

    — Windows Setup captures an image in .WIM format that will be deployed using Windows PE and Windows Setup.

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

    For more information about ImageX and Windows Setup, refer to the Windows documentation available at **http://technet.microsoft.com**.

- **Image Name** – A name that you choose for this image. The files that are uploaded to the HPCA server and used to deploy this image will use this name.

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

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

  The image description can be up to 80 characters long.

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

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

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

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

Summary

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

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

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

The following things happen...

1 This dialog box appears:
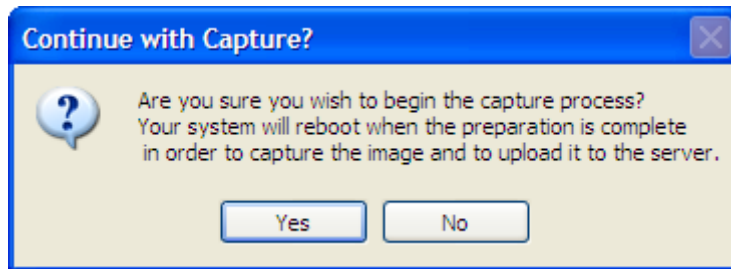
2 Click **Yes** to prepare the machine, reboot, and capture the image.

   The capture can take 15-20 minutes to complete, depending on the size of the image. During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 343 for more information.

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

   `<InstallDir>\Data\OSManagerServer\upload`

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

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

For more information about OS Management in HPCA, see Additional Resources on page 331.

Additional Resources

For more information about OS Management in HPCA, refer to the following:

• HPCA Console online help topics:

   — Preparing and Capturing OS Images

   — OS Management

- *HP Client Automation OS Management Reference Guide*

Preparing and Capturing Thin Client OS Images

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

- Windows XPe and WES OS Images on page 332
- Windows CE OS images on page 336
- ThinPro OS Images on page 339

⚠ Do not publish factory OS images for thin client devices. All thin client images must be captured before they are deployed to target devices.

During the OSM capture process additional information about the OS is retrieved and later used for image deployment. As a result, the administrator should not publish a factory image directly, as required information would be unavailable and the deployment would not succeed.

Windows XPe and WES OS Images

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

- Prepare the Windows XPe or WES Reference Machine on page 332
- Run the Image Preparation Wizard on page 333

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

Task 1: Prepare the Windows XPe or WES Reference Machine

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

- HPCA media

- Image Preparation CD-ROM

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

1 Log on to the Windows XPe or WES device as Administrator.

2 Install the HPCA agent on the Windows XPe or WES device.

   See Installing the HPCA Agent on HP Thin Clients on page 107 for details.

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 HPCA 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 Preparation CD you created). The Linux-based portion of the Image Preparation Wizard runs to collect the image and its associated files.

4 Creates and copies the following files to this directory on the HPCA server: `<InstallDir>\Data\OSManagerServer\upload`.

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

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

▶ While these files are transferred, network speed will be less than optimal.

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

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

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

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

4   Double-click **prepwiz.exe**. The 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 HPCA server. This must be specified in the following format:

    xxx.xxx.xxx.xxx:*port*

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

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

    —   Click **Yes** to continue anyway.

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

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

8   Click **Next**.

    The Image Name window opens.

9   Type a name for the image file. This is the image name that will be stored in the `\upload` directory on the HPCA 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 HPCA server after the OS is installed to verify that the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.

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

The Summary window opens.

15 Click **Start**.

16 Click **Finish.**

The wizard prepares the image.

17 Click **OK**.

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

⚠ If the device does not boot to the CD (boots to Windows XPe instead), you will need to restart the process from Prepare the Windows XPe or WES Reference Machine on page 332.

▶ The upload of the image may seem to take a long time. Transfer speeds will vary depending upon processor speeds and your network environment.

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

During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 343 for more information.

18 OS Image Preparation Wizard connects to the network, and stores the image on the HPCA server in the following directory:

<InstallDir>\Data\OSManagerServer\upload

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

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

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

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

Next, you will want to publish your image to the HPCA database. See Publishing on page 347.

Windows CE OS images

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

- Prepare the CE Reference Machine on page 336

- Run the Image Preparation Wizard on page 337

▶ Deploying an OS through LSB is not supported on Windows CE based HP thin client models t5550 and above.

Task 1:   Prepare the CE Reference Machine

- Product media
- Image Preparation CD-ROM

Before you capture the image, you must install the HPCA agent on the Windows CE device.

See Installing the HPCA Agent on HP Thin Clients on page 107 for details.

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

Follow these steps on the Windows CE device:

1 Click **Start**.

2 Select **Settings** > **Control Panel**.

3 Click the **System** icon.

4 Select the **Memory** tab.

5   Use the slider on the left to increase the **Storage Memory** to 10 MByte or
    more.

Task 2:   Run the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

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

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

3   Creates and copies the following files to
    `<InstallDir>\Data\OSManagerServer\upload` on the HPCA server.

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

▶   While these files are being transferred, network speed will be less
    than optimal.

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

To use the Image Preparation Wizard

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

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

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

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

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

    xxx.xxx.xxx.xxx:port

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

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

    —   Click **Yes** to continue anyway.

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

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

6   Click **OK**.

    The wizard prepares the image.

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

    ⚠️   If the device does not boot to the CD (boots to Windows CE instead)
         you will need to restart the process from Prepare the CE Reference
         Machine on page 336.

    ▶   The upload of the image may seem to take a long time. Transfer
         speeds will vary depending upon processor speeds and your
         network environment.

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

    During the capture, status information is displayed on the Service OS
    screen. See About the Windows PE Service OS Screen on page 343 for
    more information.

7   The Image Preparation Wizard connects to the network, and stores the
    image in the following directory on the HPCA server:

    <InstallDir>\Data\OSManagerServer\upload

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

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

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

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

Next, you will want to publish your image to the Configuration Server DB. See Publishing on page 347.

ThinPro OS Images

The following sections explain how to prepare and capture a ThinPro operating system image:

*   Prepare the ThinPro Reference Machine on page 339
*   Run the Image Preparation Wizard on page 340

Task 1:   Prepare the ThinPro Reference Machine

To prepare ThinPro client for image capture, you will need the following:

*   HPCA media
*   Image Preparation CD-ROM

Before you capture the image, you must install the HPCA agent on the ThinPro device.

See Installing the HPCA Agent on HP Thin Clients on page 107 for details.

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

To create a custom connection for xterm

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

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

Note: Control Center background will change from blue to red.

3   From the Control Center, click the **Add** drop down list and select the **custom** option.

4   Set Name to **xterm**.

5   Set Command to run to:

sudo xterm -e bash &.

6   Click **Finish**.

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

Task 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 HPCA agent is installed. If there is not enough free disk space, the Image Preparation Wizard displays a message and terminates.

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

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

3   Creates and copies the following files to `<InstallDir>`\Data\OSManagerServer\upload on the HPCA server.

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

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

▶ While these files are transferred, network speed will be less than optimal.

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

To use the Image Preparation Wizard

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

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

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

The Welcome window opens.

3 Click **Next**.

The End User Licensing Agreement window opens.

4 Click **Accept**.

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

`xxx.xxx.xxx.xxx:port`

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

If the Image Preparation Wizard cannot connect to the HPCA 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 HPCA 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 HPCA server after the OS is installed to verify the OS was installed properly. If this is not selected, the OS Connect will not occur automatically after the OS is installed.

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

The Summary window opens.

13   Click **Start**.

14   Click **Finish.**

The wizard prepares the image.

15   Click **OK**.

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

⚠   If the device does not boot to the CD (boots to Linux instead) you will need to restart the process from Prepare the ThinPro Reference Machine on page 339.

> The upload of the image may seem to take a long time. Transfer speeds will vary depending upon processor speeds and your network environment.

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

16 The Image Preparation Wizard connects to the network, and stores the image in the following directory on the HPCA server:

    `<InstallDir>\Data\OSManagerServer\upload`

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

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

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

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

Next, you will want to publish your image to the HPCA database for distribution to managed devices. See Publishing on page 347.

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the HPCA database. For instructions, see Publishing on page 347.

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

About the Windows PE Service OS Screen

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

1 Boots into the target hardware

2   Loads all the drivers that are needed in order for that hardware to function correctly

3   Downloads and runs HPCA programs which, in turn, download and install OS images

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

- Operations to hardware on a target device (for example, a BIOS update or hardware configuration)

- Provisioning target devices (for example, deploying an OS)

- Capturing an OS image

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

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

- A green checkmark icon indicates that a particular step either is in progress or has been successfully completed.

- A yellow triangle icon is a warning that something may be wrong.

- A red X icon indicates that this step in the capture or deployment has failed.

- A blue question mark (?) icon indicates that input is required.

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

If the operation is successful, a green check mark appears on the left side of the Service OS screen with further instructions.

At this point, you can take one of two actions:

- Click **Reboot** to reboot the device into the installed operating system.

- Click **Shutdown** to shut the device down.

After you click one of these buttons, a status message will appear briefly under the progress bar on the right side of the screen before the reboot or shutdown occurs.

If the operation is not successful, a red X appears on the left side of the Service OS screen with information about the nature of the failure. If the operation fails, you can use the scroll bar on the right side of the screen to view information about the hardware detected and determine where in the process the failure occurred. At this point, you can take one of three actions:

- Click **Reboot** to reboot the device into the installed operating system.

- Click **Shutdown** to shut the device down.

- Click **Exit to console** to close the Service OS screen and reveal the console window.

After you click one of these buttons, a status message will appear briefly under the progress bar on the right side of the screen before the action that you selected occurs.

13 Publishing

Use the HPCA Publisher to publish the following items to HP Client Automation (HPCA) database:

- Software
- BIOS configuration settings
- HP Softpaqs
- Operating system images

Published software is available in the Software Library on the Operations tab of the main HPCA console. Published operating systems are available in the OS Library on the Operating Systems tab.

➤ The Publisher is installed automatically during the installation of the HPCA Core. If the HPCA agent is already installed on the machine, the Publisher will be installed in the agent's folder. If you want to install it in a different location, you can use the HP Client Automation Administrator installation file on the product media or use the HPCA Administrator Publisher service in the Software Library. See *Manually Installing the HPCA Administrator* in the *Installing HPCA* chapter for more information.

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

After you publish one of the items listed above, it can be entitled and deployed to managed devices in your environment.

To start the Publisher

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

2 To log in to the Publisher use your HPCA Administrator user name and password. By default, the user name is **admin** and the password is **secret**.

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

shows which publishing options are available for each of the three license levels.

Table 35   Publishing Options Available with Each HPCA license

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

The following sections explain how to use the Publisher for the publishing options for your license. If you select a thin client publishing option, follow the instructions in the appropriate section below.

- Publishing Software on page 349

- Publishing Operating System Images on page 352

- Publishing OS Add-Ons and Extra Production OS (POS) Drivers on page 360

- Publishing HP Softpaqs on page 361

- Publishing BIOS Settings on page 363

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 on page 349
- Publishing Using Component Select on page 351

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 HPCA. When the software service is contained in HPCA, 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 347).

2   At the Logon window, type your administrator User ID and Password and click **OK**.

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

3   In the Publishing Options area, select **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 msiexec.**.

> ▶ 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 Window Installer file that you 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 347).

2   At the Logon window, type your administrator User ID and Password and click **OK**.

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

3   In the Publishing Options area:

—   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.
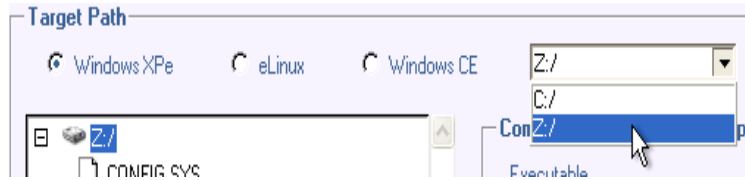
7   Enter the commands to run on application install and uninstall. For example, a command to run on install might be: `C:\temp\installs \install.exe /quietmode /automatic c:\mydestination`

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 HPCA server in the following directory:

`<InstallDir>\Data\OSManagerServer\upload`

You can use the Publisher to publish operating system image files for distribution to managed devices. The specific files that you will need depends on the deployment method that you intend to use (see Table 36 on page 353).

If you captured an OS image from a reference machine, you will need the files that resulted from that capture process. For more information, see Preparing and Capturing OS Images on page 321.

⚠️ Do not publish factory OS images for thin client devices. All thin client images must be captured before they are deployed to target devices.

See Preparing and Capturing Thin Client OS Images on page 332 for additional information.

▶ If you will be publishing .WIM images, see Prerequisites for Publishing .WIM images on page 355 before you begin the publishing process.

Table 36   Files Needed to Publish OS Images

Deployment Method	Files Required	Refer To
Directly from a DVD	DVD `WIM` file HPCA `unattend-dvd.xml`	Pre-requisites for Publishing Directly from a DVD on page 356

Microsoft ImageX	`ImageName.WIM`
	`ImageName.EDM`
	HPCA `unattend-capture.xml`
		Prerequisites for Publishing .WIM images on page 355

Table 36 Files Needed to Publish OS Images

Deployment Method	Files Required	Refer To

Windows Setup	`ImageName.WIM`
	`ImageName.EDM`
	HPCA
	`unattend-capture.xml`
		Prerequisites for Publishing .WIM images on page 355

Legacy	`ImageName.IMG`
	`ImageName.MBR`
	`ImageName.EDM`
	`ImageName.PAR`
	For WinXPe or Windows CE:
	`ImageName.IBR`
	`ImageName.EDM`
	For Linux:
	`ImageName.DD`
	`ImageName.EDM`
		Publish OS Images on page 358

▶ The names of the `unattend` files shown in Table 36 refer to the files provided in the Image Capture ISO. You can change the name of this file as you see fit.

For information about customizing the `unattend` file, see Customizing the Windows Answer File on page 455.

Prerequisites for Publishing .WIM images

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

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

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

- Have access to the `Media\client\default` folder on the HPCA media.

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

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

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

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

- The Windows Automated Installation Kit (AIK) for Windows 7 must be installed on the device where you are publishing the image. This is a Core installation prerequisite. Refer to "Using HPCA to Manage Windows Operating Systems" in the HPCA Installing chapter for more information.

- If you are using an existing *filename*.wim, copy the file to the device where you are publishing the image.

- If you prepared and captured a `.WIM` file using the Image Preparation Wizard, copy *filename*.wim and *filename*.edm from the HPCA server's `\upload` directory (`<InstallDir>\Data\OSManagerServer\upload`) to the device where you are publishing the image.

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

- HPCA provides a Windows Setup answer file that you can use for unattended installations. When you run the Publisher, you can choose to either use the answer file that HPCA provides (preferred method) or create your own. See Specifying the Windows Setup Answer File on page 357 for more information

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

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

  If you want to use the `unattend.xml` file that HP provides, you must modify it for your environment before you run the Publisher. At a minimum, you must specify the ProductKey for the image that you are publishing. You may also want to modify other settings in this file—for example, the TimeZone and the RegisteredOrganization. See Customizing the Windows Answer File on page 455 for details.

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

Pre-requisites for Publishing Directly from a DVD

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

To prepare to publish an OS image directly from a DVD

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

2 Mount the image capture ISO.

Specifying the Windows Setup Answer File

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

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

For backward compatibility, the old method is described in an appendix to this guide. See Customizing the Windows Answer File on page 455.

Publish OS Images

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

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

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

⚠️ Be sure to satisfy the Prerequisites for Publishing .WIM images or Pre-requisites for Publishing Directly from a DVD on page 356 before you start the Publisher.

To publish operating system images

1 Start the Publisher. See To start the Publisher on page 347.

2 In the Publishing Options area:

   — If you are publishing for thin clients, select **Thin Client Publishing**.

   — From the drop-down menu, select **OS Image**.

3 Click **OK**. The Select OS Image File page opens.

4 Select the OS image file that you want to publish.

   Images created using the Image Preparation Wizard are stored on the HPCA server in the following folder:

   `<InstallDir>\Data\OSManagerServer\upload`

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

6 Click **Next**.

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

8　If you manually created `*.subs` and `*.xml` files for this image, skip to step 10. This is not recommended. See Customizing the Windows Answer File on page 455 for more information.

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

See Prerequisites for Publishing .WIM images on page 355 for additional information.

10　Click **Next**.

11　Perform *either* Action 1 or Action 2:

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

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

b　Ignore the **Sources Directory** box.

or

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

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

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

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

12　Enter the appropriate Application Information in the fields provided.

13　Click **Next**. The Summary window opens.

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

15　Click **Finish** to exit the Publisher when the publishing process is complete.

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

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

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

▶ For a detailed discussion of this process, refer to "Customizing OS Deployment by Using Exit Points and Adding Device Drivers" in the *HP Client Automation OS Management Reference Guide*.

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

Prerequisites

- Publish your OS service. The Publisher automatically creates a connection, OS.ADDON.ServiceName_*, under this service.

- If you are publishing OS drivers:

    — Create the following directory:

      `C:\MyDrivers\osmgr.hlp\drivers`

    — Store the individual drivers that you want to publish in this directory.

To publish delta packages

1 Go to **Start→All Programs→HP Client Automation Administrator→HP Client Automation Administrator Publisher**. The Logon screen opens.

2 Type your HPCA Administrator user ID and Password (by default, **admin** and **secret**).

3 In the Publishing Options windows select **OS Add-ons/extra POS drivers** from the drop-down list.

4   Click **OK**.

5   Use the Select Drivers Directory window, specify the following:

   a   In the directory tree, select the C:\MyDrivers directory.

      Everything below this directory will be recursively scanned, included, and published.

   b   From the **Add-on type** drop-down list, select **OS Driver** file.

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

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

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

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

6   Click **Next**.

7   Review the summary screen and click **Publish**.

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 HPCA for distribution to managed devices.

▶   Publisher does not generate methods to uninstall HP Softpaqs. Therefore, HP Softpaqs cannot be uninstalled, once deployed.

To publish a Softpaq

1 Start the Publisher (see).

2 At the Logon window, type your administrator User ID and Password and click **OK**.

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

3 In the Publishing Options area, select **HP 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 HPCA and is available for distribution to managed devices. View the published Softpaq in the HPCA 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.

Two sample BIOS settings files (HP desktop sample BIOS settings.txt and HP notebook sample BIOS settings.txt) are included with the Publisher installation and located by default at: `<InstallDir>`\Agent\BIOS. Use one of these files to select BIOS settings to publish for deployment.

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 364.

To publish BIOS settings

1 Start the Publisher (see To start the Publisher on page 347).

2 At the Logon window, type your administrator User ID and Password and click **OK**.

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

3 In the Publishing Options area, select **HP BIOS Configuration** and click **OK**. The Select window opens.

4 Select a BIOS settings file from which to publish settings. Sample BIOS settings files are located by default in: `<InstallDir>`\Agent\BIOS.

5 In the **Current BIOS Admin Password** area, type and then confirm a BIOS password if required. This is required to change any settings if the target devices have a BIOS password.

6 If you want to change the current BIOS password, select **Change BIOS Password**, then type and confirm the new password. This is required only if you want to change the BIOS password on a client device.

7 Click **Next**. The BIOS Options window opens.

8 To select the BIOS settings to be publishes select the check box to the left of the BIOS setting names.

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. If it looks fine, click **Publish**.

14 When the publishing process is complete, click **Finish** to close the
     Publisher.

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

Creating a BIOS Settings File

If you would like to use a BIOS settings file other than the file included with
HPCA, you can use the HP System Software Manager (SSM) BIOS
Configuration Utility to generate your own settings file. SSM is installed with
the HPCA Agent (`<InstallDir>\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 (`<InstallDir>\SSM`, by default).

2   Type the following:

     **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`.

When you are ready to publish BIOS settings, select this file in step 4 of To
publish BIOS settings on page 363.

Viewing Published Services

View published software in the Management tab, Software Management area. Published operating systems are stored in the Operating System area.

HP Client Automation Administrator Agent Explorer

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

14 Using the Application Self-Service Manager

The HP Client Automation Application Self-Service Manager (Self-Service Manager) is the client-resident product with which users can install, remove, and update optional applications that have been made available to them. The applications have to be entitled to the users by an HPCA administrator. The Self-Service Manager presents users with a catalog of the applications to which they are entitled, and they can self-manage the installation, removal, and updating of the applications. The Self-service Manager gets installed on client devices when the Management Agent is deployed to those devices.

The following sections describe how to use the Self-service Manager user interface.

Accessing the Application Self-Service Manager

The Self-service Manager user interface can be accessed through either of the following methods.

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 Self-service Manager interface (see Figure 18 on page 369) has four main sections that allow users to manage available applications, view information and status for software in their catalog, and customize the user interface display.

Figure 18 Application Self-Service Manager user interface
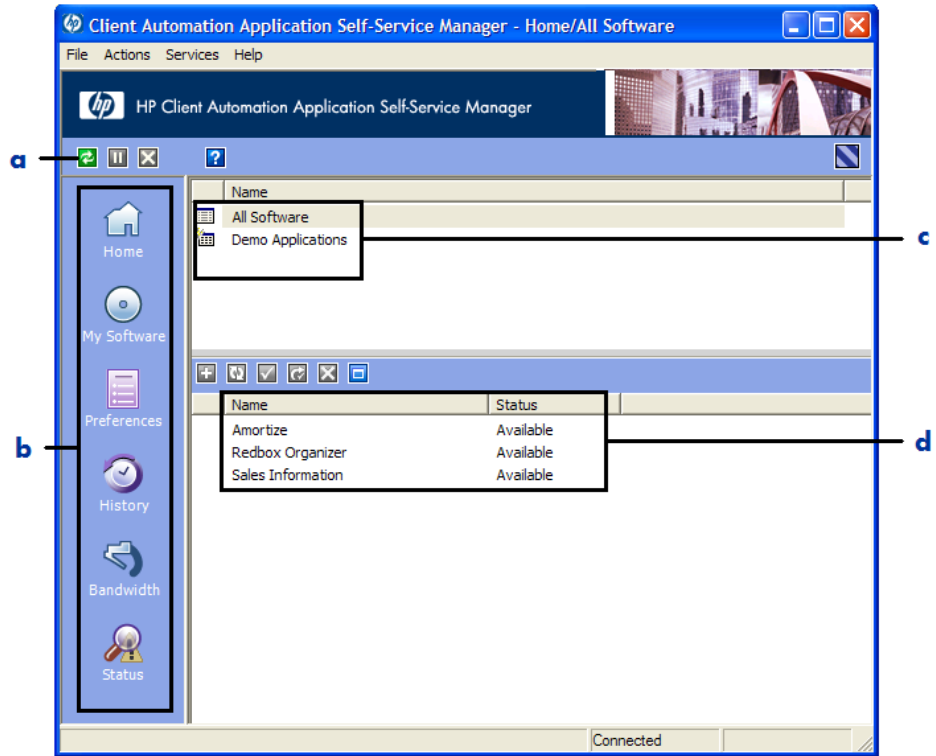
Legend

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 the user are entitled

The following sections describe the user interface sections in more detail.

- Global Toolbar on page 370
- Menu Bar on page 370
- Catalog List on page 371
- Service List on page 371

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**.

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 applications that you have installed.

Preferences: Click this button to access various display options, application list options, and connection options for the Self-service Manager.

At any point you can click **OK**, **Apply**, or **Cancel** in the top right corner of this 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 HPCA 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:
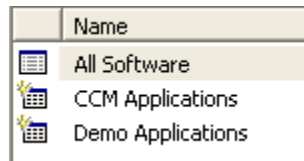
Service List

The Service List section lists the applications that are available to you. A check mark appears next to an application that is already installed. The column headings can be changed to suit your needs. For more information, see *Preferences* in the section, Menu Bar on page 370.

Table 37   Buttons in the Service List Section

Button	Action	Description
	Install	Installs the selected service on your machine.
	Verify	Verifies the files for the selected service.

Table 37   Buttons in the Service List Section

Button	Action	Description
	Repair	Repairs the selected service.
	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

Use the user interface to install and remove software, refresh the catalog of available applications, and view information about the applications. 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 373
- Refreshing the Catalog on page 373
- Viewing Information on page 374
- Removing Software on page 375
- Verifying Software on page 375
- Repairing Software on page 375
- Viewing History on page 376
- Adjusting Bandwidth on page 376
- Viewing Status on page 377

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 application 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 application 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 Self-Service Manager 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 update the 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

The Service List presents basic information, although additional information about an application (such as vendor, version, size, and installation date) can be retrieved by:

- Adding these columns to the Service List.

- Clicking **Show Extended Information** 🛈 in the expanded service box.
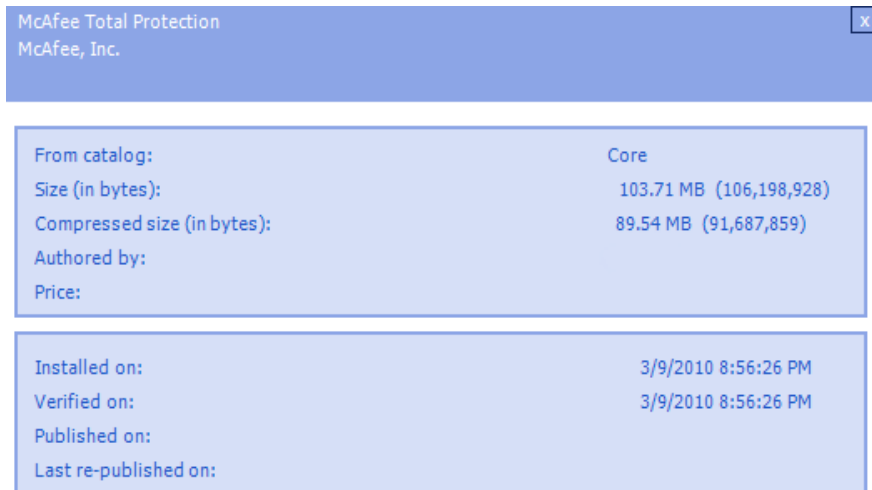
If you want more information from the manufacturer, click that vendor's link.

To view more information

1   In the Service List, select an application, and click **Show Extended Information** 🛈.

> You can also right-click the application, select **Properties**, then select **Information** from the shortcut menu that opens.

McAfee Total Protection McAfee, Inc.	x
From catalog:	Core
Size (in bytes):	103.71 MB (106,198,928)
Compressed size (in bytes):	89.54 MB (91,687,859)
Authored by:	
Price:	
Installed on:	3/9/2010 8:56:26 PM
Verified on:	3/9/2010 8:56:26 PM
Published on:	
Last re-published on:	

2   Click the corresponding **Cancel** button to return to the Service List.

Removing Software

Use the **Remove** button ❌ to remove an application from your computer.

To remove software

1 Select the application 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 application that you want to remove, then select **Remove** from the shortcut menu that opens.

Verifying Software

To check the installation of an application

1 In the Service List, select the installed service that you would like to verify.

2 Click **Verify**.

> ➤ You can also right-click the name of the software, then select **Verify** from the shortcut menu that opens.

— If the application passes verification, the date and time of verification will appear in the Verified Date column for the application.

— If the application fails verification, Broken will appear in the Status column.

3 To repair the software, click **Repair**.

Repairing Software

If there is something wrong with an application, click **Repair** to fix it.

1   Select an application that needs to be repaired. This is designated by an X
    in the first column, and Broken, in the Status column.

2   Click **Repair**. HPCA retrieves the files needed to fix the application.

Viewing History

1   In the Menu Bar, click **History** to display a history of the current session.

Figure 19 History window
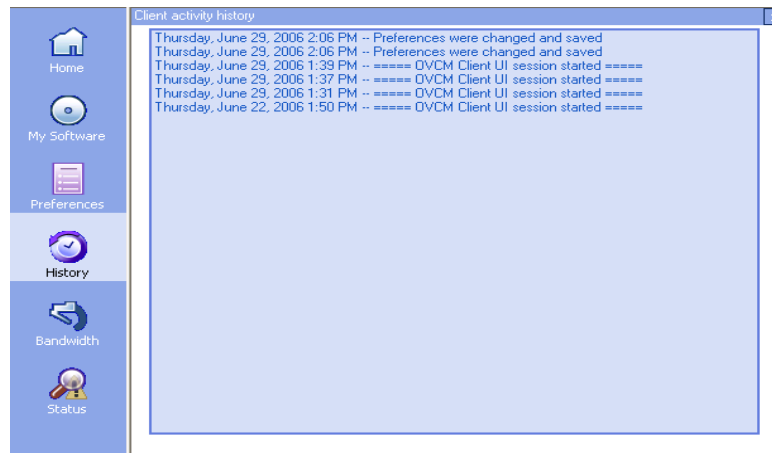
2   Close the history window to return to the service list.

Adjusting Bandwidth

In the Menu Bar, click **Bandwidth** to display the bandwidth slider. Changing
this value dynamically changes the throttling value.

•   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 20 Status display for selected application

The Status window can be docked or un-docked from the Application Self-Service Manager. This enables you to position it 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 Application Self-Service Manager interface, allowing you to position it anywhere on your screen.

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 interface.

Customizing the User Interface

Click the **Preferences** button in the Menu Bar to view the available
customization options. The following sections describe each customization
area.

- General Options on page 378
- Service List Options on page 380
- Connection Options on page 383

General Options

Use the General options window to modify the appearance of the Application
Self-Service Manager interface.

Figure 21 General options window
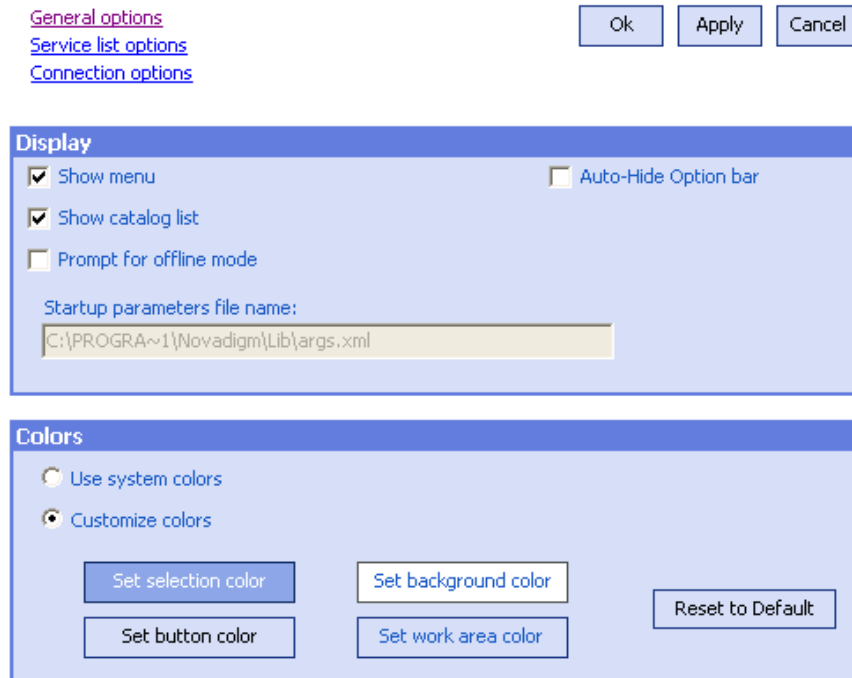
To modify the display

- If you want to display the menu, select **Show menu**.

- If you want to display the catalog list, select **Show catalog list**.

- If you want to be prompted to use the Application Self-Service Manager in offline mode at the beginning of each session, select **Prompt for offline mode**.

- If you want to have the Option bar automatically hidden, select **Auto-Hide Option bar**.

To modify the colors

- If you want to use the system colors, select **Use system colors**.

- If you want to customize the color scheme, select **Customize colors**.

  — 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 22 Service List options
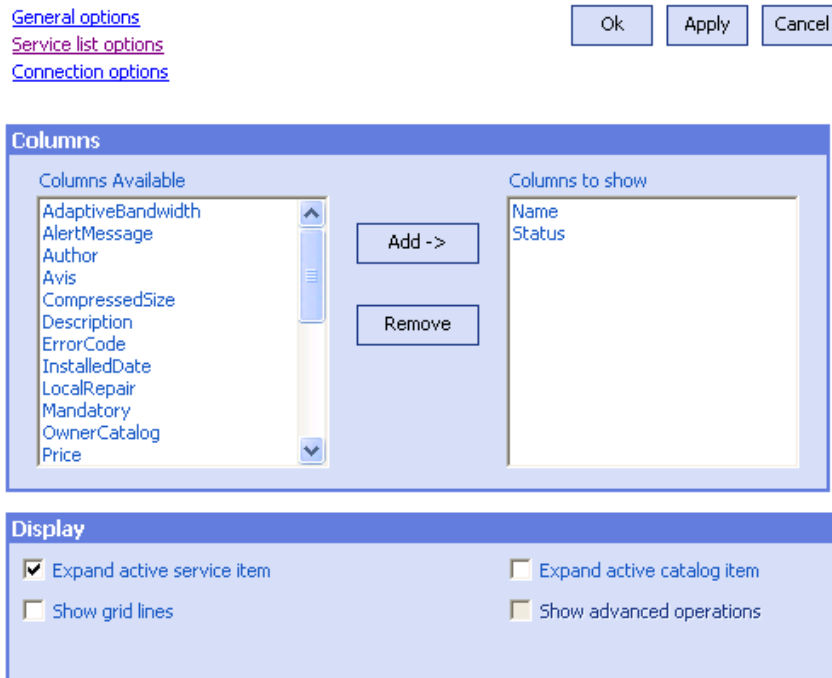
To customize the column names in the Service List

Use the Columns area to customize the columns that appear in your Service List. The right column lists the names of the column that are currently displayed in your Service List. For a description of each available column heading, see Customizing the Display on page 381.

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** keys 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 38 Column headings available for the Service List

Column Heading	Description
AdaptiveBandwidth	Adaptive minimum percentage of bandwidth used when using bandwidth throttling.
AlertMessage	Allows longer application 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).
Description	A short description of the application.
ErrorCode	Current Service status. Example: Initial = 999. Method Failure = 709.

Table 38   Column headings available for the Service List

Column Heading	Description
InstalledDate	The date on which the application was installed on your computer.
LocalRepair	If data is repairable locally (cached on your computer).
Mandatory	Mandatory/Optional files defined on application (for internal use).
Name	The name of the application.
OwnerCatalog	The originating application domain name.
Price	Price of the service.
PublishedDate	The date on which the application was published to the catalog.
Reboot	Service reboot settings (for internal use).
RePublishedDate	The date on which the application 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 application, locally.
Size	The size of the application (bytes). Note: You will need this amount of free space on your computer to successfully install the application.
Status	Current status of the application • Available • Installed • Update Available • Broken
SystemInstall	Displays if application will be installed using System account.
ThrottlingType	Type of Bandwidth throttling to use. Possible values: ADAPTIVE, RESERVED or NONE.
Option	Determines whether the status window is displayed.
UpgradedDate	The date on which the application was upgraded.

Table 38   Column headings available for the Service List

Column Heading	Description
Url	The software vendor's web address.
Vendor	The software vendor who supplied the application.
VerfiedDate	The date on which the application was last verified.
Version	The version of the application.

Connection Options

Use **Connection options**, see Figure 23 on page 383, to select the type of bandwidth throttling to use and to specify proxy server settings.

Figure 23 Connection Options
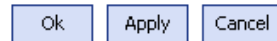
- **Throttling**

    — Select **None** for no throttling.

— Select **Reserve Bandwidth** to slide along the scale to indicate the maximum percentage of the network bandwidth to use. The reserve bandwidth can be changed in the interface by the user 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 be set only before a job is dispatched.

- **Proxy**

  — The Application Self-Service Manager can detect an internet proxy when one 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 *<InstallDir>*\Agent\Lib. The next time the HPCA agent computer connects to the HPCA server, the specified internet proxy will be used. To use this feature, you must enable your HPCA agent to use and discover an internet proxies.

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 user.

Figure 24 HPCA System Tray Icon

Move your cursor over the icon to see HPCA states:

- **Idle**: When no actions are in progress 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 Application Self-Service Manager 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 automatically pop up.

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 25 HPCA Status
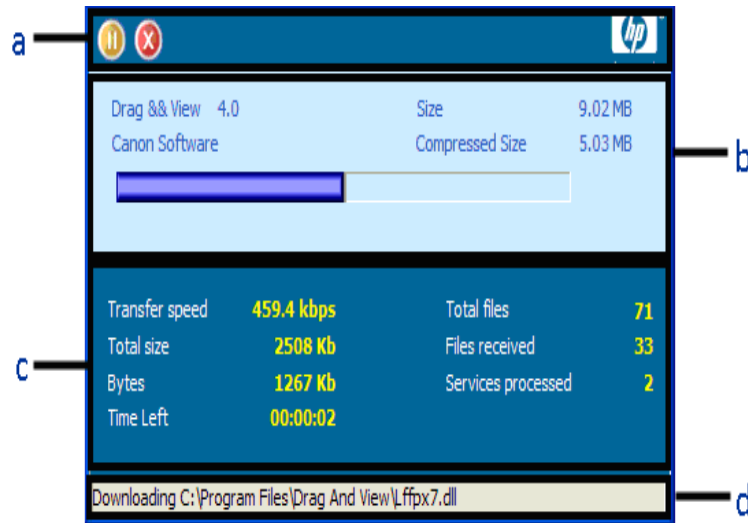
Legend

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 HPCA agent is actively working.

- **Information Panel**: This area contains information about the active application, and 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**: This area shows a message about the current process.

    — **Bandwidth Control**: If you set bandwidth throttling for the application on the HPCA 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.

15 Personality Backup and Restore

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

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

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

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

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

- Requirements on page 387
- About USMT on page 389
- Using Personality Backup and Restore on page 394
- Troubleshooting on page 403

Requirements

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

Operating System

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

- Windows XP
- Windows Vista
- Windows 7

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

- Windows XP
- Windows Vista
- Windows 7

> ➤ The /hardlink option can only be used for restore operations on Windows Vista and Windows 7 operating systems. It can be used for backup on Windows XP SP2 and later operating systems.

See Using the Command Line Interface on page 399 for more information.

Disk Space

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

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

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

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

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

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

Software

You need the following applications:

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

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

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

About USMT

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

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

This section describes Microsoft USMT; how to obtain it, install it, and how to use its migration files. For a description of the Hewlett-Packard user interface provided with the Personality Backup and Restore solution, which invokes USMT automatically during a backup and restore, see Using the HPCA Personality Backup and Restore Utility on page 395.

Supported Files, Applications, and Settings

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

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

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

http://technet.microsoft.com/en-us/library/dd560752.aspx

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

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

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

Obtaining and Installing Microsoft USMT 3.0.1 or 4.0

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

- As an administrator, you want to become familiar with the capabilities of USMT and to learn how to customize the migration rules for your personalized solution.

- As an end user, you want to be able to back up and restore files and settings on managed devices.

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

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

Obtaining Microsoft USMT 3.0.1

USMT 3.0.1 is available at the Microsoft Download Center:

http://www.microsoft.com/downloads

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

Obtaining Microsoft USMT 4.0

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

http://www.microsoft.com/downloads

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

▶ See Using the Command Line Interface on page 399 for information about how the /hardlink option can be used on the various supported operating systems.

Installing Microsoft USMT on Managed Devices

You can install USMT on managed devices in two ways. You can install it manually, or you can package it into a service using the HPCA Administrator Publisher (see Publishing on page 347) and then entitle or deploy it to managed devices. USMT must be installed in the default location on both the source and destination client devices:

Table 39   Default USMT Installation Locations

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

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

Migration Files

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

— `MigSys.xml` – migrates operating system settings

— `MigApp.xml` – migrates application settings

— `MigUser.xml` – migrates user folders and files

▶ In USMT 4.0, the `MigSys.xml` is renamed as `MigDocs.xml`.

Before you implement this solution in your environment you must obtain these files and store them on the HPCA Core Server (see Storing the Migration Rules on the Core Server on page 393).

To obtain these files you must install USMT on one of its supported platforms (see Obtaining and Installing Microsoft USMT 3.0.1 or 4.0 on page 390). The installation places these files in the directories shown in Installing Microsoft USMT on Managed Devices on page 392.

You can then edit these files (see Editing the Rules on page 393) or use them as is.

Editing the Rules

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

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

Storing the Migration Rules on the Core Server

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

DataDir\PersonalityBackupAndRestore\conf

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

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

ScanState and LoadState Command Lines

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

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

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

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

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

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

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

Using Personality Backup and Restore

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

All three methods invoke the same HPCA application, which is called pbr.exe. Each time that pbr.exe runs, it downloads the three migration XML files (see Migration Files on page 392) from the HPCA Core server to the managed device and uses these files to perform the backup or restore.

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

DataDir\PersonalityBackupAndRestore\backups

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

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

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

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

If you are using USMT version 4.0 (included in the Windows AIK for Windows 7), you can specify the `/hardlink` option to create a hard-link migration store instead of physically copying the files. This speeds up the backup and restore operations.

See for details.

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

Using the HPCA Personality Backup and Restore Utility

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

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

To start the Personality Backup and Restore Utility

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

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

The following sections explain how to use the Utility:

-
-

Personality Backup

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

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

To back up files and settings:

1   On the managed device, start the Personality Backup and Restore Utility (see To start the Personality Backup and Restore Utility on page 395).
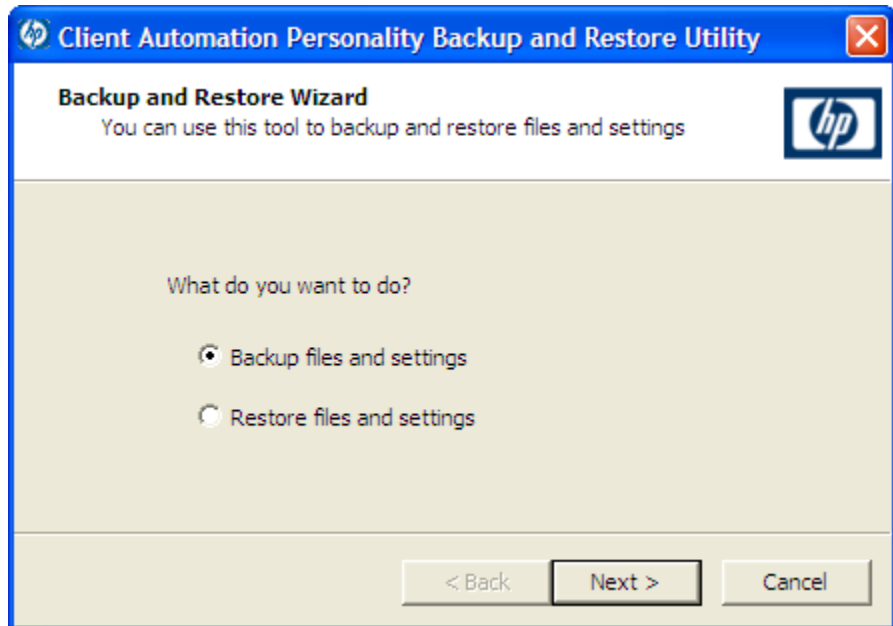
2   Select **Backup files and settings**, and click **Next**. The Backup dialog box opens.

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

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

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

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

Personality Restore

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

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

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

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

To restore files and settings

1   On the destination computer, start the Personality Backup and Restore Utility (see for instructions).

2   Select **Restore files and settings** and click **Next**. The Restore dialog box opens.
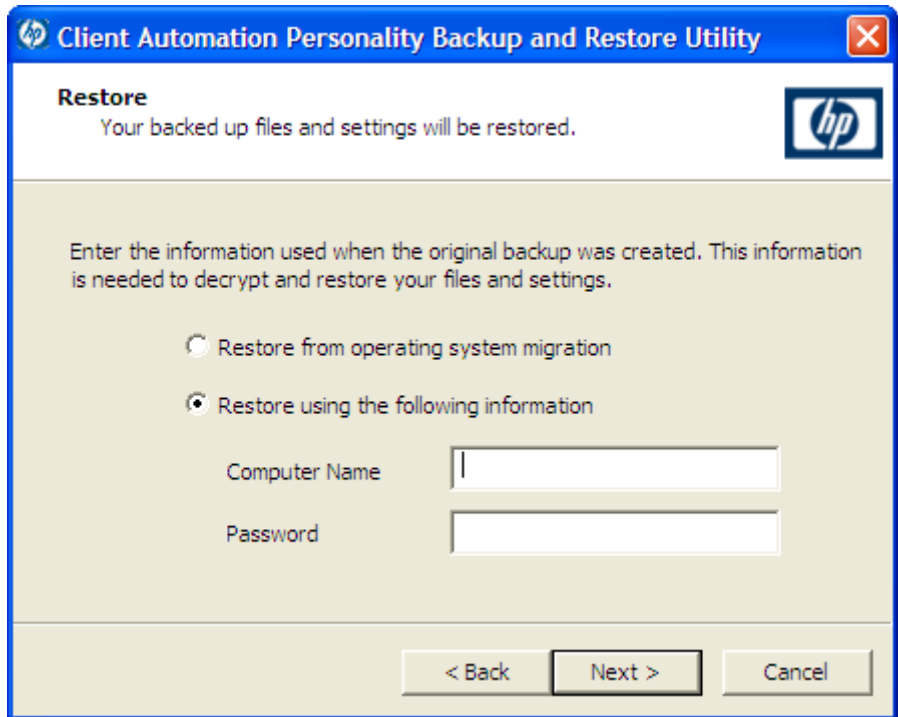
3   Perform one of the following actions:

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

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

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

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

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

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

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

Using the Command Line Interface

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

The syntax is as follows:

<InstallDir>\Agent\pbr.exe /B|/R [/localstore] [/hardlink]

Table 40   Command Line Options for pbr.exe

Option	Description
/B	Perform a backup.
/R	Perform a restore.
/localstore	Store the backup files on (or restore them from) the local hard drive of the managed device instead of the HPCA Core server.
/hardlink	For USMT 4.0 (included in the Windows 7 AIK), do not physically copy the backup files to the OSMGR.PRESERVE directory. Instead, create hard links to the files. This significantly saves backup space, because the backed up files are not duplicated. It also speeds up the backup and restore operations.
	If /hardlink is specified, /localstore is implied.
	When the /hardlink option is used, the target (restore) OS must be Windows Vista or Windows 7. The source (backup) OS, however, can be Windows XP SP2 or later.
	For USMT 3.0.1, this option is ignored. In this case, /hardlink is treated like /localstore.
/xml	Select xml files from HPCA Core Server using wildcards. This option can be used when you perform a backup.

Table 40   Command Line Options for pbr.exe

Option	Description
/--	Use this option to pass additional parameters for USMT utilities. The additional parameters are appended to the command line as set up by Personality Backup and Restore.

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

<InstallDir>\Agent\pbr.exe /B

Example 2: Restore from the HPCA Core server

<InstallDir>\Agent\pbr.exe /R

Example 3: Backup your files and settings locally

<InstallDir>\Agent\pbr.exe /B /localstore

Example 4: Restore after a local backup

<InstallDir>\Agent\pbr.exe /R /localstore

Example 5: Perform a local backup using hard links

<InstallDir>\Agent\pbr.exe /B /hardlink

This example is valid for the following operating systems: Windows XP SP2, Windows XP SP3, Windows Vista, and Windows 7.

Example 6: Perform a local restore using hard links

<InstallDir>\Agent\pbr.exe /R /hardlink

This example is valid for the following operating systems: Windows Vista and Windows 7.

Example 7: Select xml files from HPCA Core Server using wildcards

<InstallDir>\Agent\pbr.exe /B /xml myconfig*.xml

Example 8: Set log level for the USMT utilities ScanState and LoadState

<InstallDir>\Agent\pbr.exe /R /-- /v:4

Using the Personality Backup and Restore Services

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

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

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

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

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

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

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

2 Deploy the OS to the specified group of managed devices.

3 After the OS deployment is completed, make sure that USMT is installed in the default location on each managed device in the group (see Installing Microsoft USMT on Managed Devices on page 392).

4 Deploy the HPCA Personality Restore service (HPCA_RESTORE) in the Software Library to each managed device in the group.

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

An Alternate Method for Capturing and Restoring Data during OS Deployment

HP also provides a ROM Client method (`romclimth.tkd`) that you can use to capture and restore data during operating system deployment. This method is stored in `<InstallDir>\Agent`, and it has two exit points.

The exit points call two optional scripts:

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

These scripts must also be stored in `<InstallDir>\Agent`.

You can use these scripts to customize data capture, recovery, and restoration for any product that you would like to use.

How romclimth.tkd Works

Capturing, recovering and migrating data using `romclimth.tkd` relies on the OS Manager User Agent. This is because data can only be captured when the operating system is running. The process works like this:

1 The Application Manager senses the change to a target device's desired state and triggers the data capture if `Novapdc.cmd` is available in `<InstallDir>\Agent`.

2 The target device reboots, and the new operating system is installed.

3 If `Novapdr.cmd` is available, the ROM Client method begins the restore process after the operating system has been installed on the target device.

Return Codes for HP Exit Points

The following return codes are returned from the HP exit points `Novapdc.cmd` and `Novapdr.cmd`. The values may vary depending on the software that you are using with these exit points. If the return value of the

method is not equivalent to the following, use the standard batch error level conditional processing and the exit command to make them correspond to the following:

Table 41   HP Exit Point Return Codes

Code	Description
0	Successful
1	An error occurred and will be logged, but processing will continue. The log is located in: `<InstallDir>\Agent\Logs\romclimth.log.`
2	• For `Novapdc.cmd` (**capture**): A fatal error has occurred and will be logged here: `<InstallDir>\Agent\Log\romclimth.log.` Processing of the service has ended. • For `Novapdr.cmd` (**restore**): An error has occurred and will be logged here: `<InstallDir>\Agent\Log\romclimth.log.` The service is flagged, but at the next HPCA OS connect, the Application Manager will attempt to install the service again.

Troubleshooting

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

Backup or Restore Did Not Complete Successfully

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

`<InstallDir>\Agent\Log`

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

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

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

<InstallDir>\Agent\Lib

User Forgot Password and Cannot Restore Data

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

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

ComputerName_EncodedComputerNameAndPassword

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

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

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

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

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

16 Monitoring HP Client Automation

HP Client Automation (HPCA) is deployed in a distributed and tiered environment. Monitoring this infrastructure ensures the availability of the associated services and components. Though the monitoring mechanism is optional, HP recommends implementing this mechanism in your environment. The HP Client Automation performance and availability depends on several factors, wherein the following three critical aspects must be monitored:

- HPCA server availability
- HPCA service availability
- HPCA services responsiveness

HPCA is capable of monitoring software deployments, but does not function as a monitoring tool. A monitoring solution is required to ensure that the infrastructure meets the service level requirements. The HPCA log files and relational database tables provide information that monitoring tools can use to verify the infrastructure operations. You must ensure that the monitoring solution that you use in your environment is capable of performing the following tasks:

- Query HP Client Automation components for availability status and response time
- Report the status of the server components, key application processes, log files, and display the component status as per the thresholds that are defined for that component
- Raise alerts when the set thresholds are not met

A solution with proactive and periodic test should be deployed that ensures these critical aspects are functioning.

HPCA Infrastructure Components

Monitoring tools essentially monitor Windows system information, such as disk space usage, CPU utilization, and Windows service status. These tools can also monitor and extract log file contents to determine the success or failure of the task that the software performs. The HPCA infrastructure monitoring relies on such inherent capabilities of the monitoring tools.

The HPCA infrastructure monitoring solution is designed to ensure that the critical monitoring information is available to third-party external monitoring tools. In the Core-Satellite model, the individual infrastructure components are integrated into two major entities, a Core server and a Satellite server. For both these servers, most of the infrastructure components run as Windows Services. The key operational processes including DCS synchronization and Proxy server Preload are monitored by analyzing the corresponding log file content.

The following table lists the HPCA components and the parameters that you should monitor if you plan to integrate a monitoring solution in your HPCA environment.

Table 42   HPCA Infrastructure Components and Parameters to be Monitored

HPCA Component				Availability	
Monitoring Type	Component Name	Severity	Monitoring Parameter	Core	Satellite
Server Monitoring	HPCA Core/ Satellite	Critical	Ping the Core/Satellite server at *<IP address / fully qualified device name>*	✓	✓

Table 42   HPCA Infrastructure Components and Parameters to be Monitored

HPCA Component				Availability	
Monitoring Type	Component Name	Severity	Monitoring Parameter	Core	Satellite
Windows Service Monitoring	HPCA Configuration Server	Critical	Service Name: ZTOPTASK EXE: ZTOPTASK.exe	✓	✓
	HPCA Apache Server	Critical	Service Name: HPCA-Apache EXE: httpd.exe	✓	✓
	HPCA Tomcat Server	Major	EXE: tomcat.exe	✓	✗
	HPCA Boot Server (PXE)	Major	Service Name: HPCA-PXE EXE: cygrunsrv.exe	✓ Disabled by default	✓ Disabled by default
	HPCA Boot Server (TFTP)	Major	Service Name: HPCA-TFTP EXE: inetd.exe	✓ Disabled by default	✓ Disabled by default
	HPCA DB Server	Major	Service Name: HPCA-DB EXE: mysqld-nt.exe	✓	✗
	HPCA Directory Server	Major	Service Name: HPCA-DS EXE: slapd.exe	✓	✗
	HPCA Distributed Configuration Server	Major	Service Name: HPCA-DCS EXE: nvdkit-hpca-dcs.exe	✓ Disabled by default	✓

Table 42   HPCA Infrastructure Components and Parameters to be Monitored

HPCA Component				Availability	
Monitoring Type	**Component Name**	**Severity**	**Monitoring Parameter**	**Core**	**Satellite**
Windows Service Monitoring	HPCA Knowledge Base Server	Major	Service Name: `HPCA-KBM` EXE: `hpkbmanager.exe`	✓ Disabled by default	✗
	HPCA Management Portal Server	Major	Service Name: `HPCA-RMP` EXE: `nvdkit-hpca-rmp.exe`	✓	✗
	HPCA Messaging Server	Major	Service Name: `HPCA-MS` EXE: `nvdkit-hpca-ms.exe`	✓	✓
	HPCA Multicast Server	Major	Service Name: `HPCA-MCAST` EXE: `nvdkit-hpca-mcast.exe`	✓ Disabled by default	✓ Disabled by default
	HPCA OS Manager	Major	Service Name: `HPCA-OSM` EXE: `nvdkit-hpca-osm.exe`	✓ Disabled by default	✓ Disabled by default
	HPCA Patch Acquisition Server	Major	Service Name: `HPCA-PATCH` EXE: `nvdkit-hpca-patch.exe`	✓ Disabled by default	✓
	HPCA Policy Server	Major	Service Name: `HPCA-PM` EXE: `nvdkit-hpca-pm.exe`	✓	✓ Disabled by default

Table 42 **HPCA Infrastructure Components and Parameters to be Monitored**

HPCA Component				Availability	
Monitoring Type	**Component Name**	**Severity**	**Monitoring Parameter**	**Core**	**Satellite**
Service Response Monitoring	HPCA Apache Server Response	Major	URL: **http://< server>:<server_port>/ server-status**	✓	✓
	HPCA Apache Tomcat Server Response	Major	URL: **http://<core>:<core port>/console/flex/ console.jsp**	✓	✗
	HPCA Configuration Server Response	Critical	Run a batch script to internally execute the nvdkit.exe tpping. For example, nvdkit.exe tpping -host	✓	✓ Disabled by default
	HPCA Management Portal Server Response	Major	URL: **http://<core host>:<core port>/proc/ Radia/ ?WebService.Name=Aut henticateUser&Respons e.Format=Text&getauth ds=true**	✓	✗
	HPCA Messaging Server Response	Major	URL: **http:// <host>:<port>/proc/msg**	✓	✓
	HPCA Policy Server Response	Major	URL: **http://<server host>:<server port>/ policy/ ldap?dn=ldap%3a%2f%2f %2fcn%3ddevice%2ccn% 3dhp%2ccn%3dradia**	✓	✓ Disabled by default

17 FAQs

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

How do I access the HPCA Console?

Use a browser from any device in your environment to access the HPCA Console.

- Go to **http://*HPCAhost*:3466/** where *HPCAhost* is the name of the server where HPCA is installed.

How do I determine what version I am using?

- Use the Operations area, Infrastructure Management, Support page to view the HPCA 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 Access Control on page 217.

1 Click the User ID of the Console user to open the User Details window.

2 Click **Change Password**.

3 In the Password Change area, enter and confirm a new password by typing it into the text boxes provided.

4 Click **Commit** then click **Save**.

The new password has 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 HPCA.

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 280 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 on page 282.

- Follow the steps in the wizard on page 282 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, Groups section or the Group Management, Groups.

- 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 page 283 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 **Acquisition, Schedule** tab, 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 HPCA server.

2 When finished, click **Save** to commit your changes. The new schedule is displayed after Current Schedule.

3 In the **Acquisition, Settings** tab, enter the Bulletins to Acquire each discovery period. You can use wildcards (for example, MS05*) to designate a range of bulletins. Separate multiple bulletin searches with a comma (for example, MS05*, MS06*).

4 Go to the **Configuration** tab, **Infrastructure Management**, **Proxy Settings**.

5   Type a Proxy Server Address and Port from which to obtain bulletins. 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** 🖳 button, then select **Discover Patch Compliance** to launch the Patch Compliance Discovery Wizard.

- Follow the steps in the wizard on page 284 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 on the Configuration tab, Licensing page.

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   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 HPCA Agent without using the Console?

Use the HPCA Agent installation program included on the HPCA media to install the Agent to devices that may not be consistently connected to the network.

1   Use the standard-setup.cmd file located on the HPCA installation media in the Media\client\default\win32 directory.

2   From a command line, type **standard-setup.cmd** *HPCA_IP_Addr*, where *HPCA_IP_Addr* is the IP address of your HPCA 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 13, Publishing 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 13, Publishing 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 HPCA media in the \Media\iso\roms directory.

2 Follow the preparation steps in the Image Preparation Wizard online help or see Chapter 12, Preparing and Capturing OS Images 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 that any OEM drivers for all possible device hardware configurations are installed.

• The following Microsoft Knowledge Base article contains information for including OEM drivers for Windows OS installations, *How to Add OEM Plug and Play Drivers to Windows XP*.

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 *<InstallDir>*\OSManagerServer\upload directory on the HPCA server.

Refer to the Publisher online help or Chapter 13, Publishing 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.

3   Follow the steps in the wizard to select the newly created group and 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 Collection Filters on page 207 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 307 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. HP recommends 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.

18 Troubleshooting

Use the following sections to troubleshoot common problems you may encounter while using HPCA.

- Log Files on page 425
- Agent Deployment Issues on page 427
- OS Deployment Issues on page 429
- Application Self-Service Manager Issues on page 430
- Power Management Issues on page 430
- Patch Management Issues on page 431
- Troubleshooting the HPCA Server on page 431
- Dashboard Issues on page 436
- Other Issues on page 438

Log Files

HPCA log files are located in the following directories under `C:\Program Files\Hewlett-Packard\HPCA` on the server:

- `\Agent\Log`
- `\ApacheServer\logs`
- `\ApacheServer\apps\cas\logs`
- `\ApacheServer\apps\console\logs`
- `\BootServer\logs`
- `\ClientConfigurationManager\logs`

— \ConfigurationServer\log

— \dcs\log

— \DistributedCS\logs

— \Knowledge Base Server\logs

— \ManagementPortal\logs

— \MessagingServer\logs

— \MiniManagementServer\logs

— \MulticastServer\logs

— \OOBM\logs

— \OSManagerServer\logs

— \PatchManager\logs

— \PolicyServer\logs

— \ProxyServer\logs

— \ReportingServer\log

— \tomcat\logs

— \VulnerabilityServer\logs

Log file sizes will grow over time. Some logs will be in use while the HPCA services are running. These active log files should not be deleted. Historical log files can be archived or removed as necessary.

Log files can be downloaded using the Operations tab, Infrastructure Management area, Support page on the HPCA Core console.

Agent Deployment Issues

The following table shows common Agent Deployment Job error messages and the steps to take to resolve possible issues.

Table 43   Agent Deployment Job Messages and Troubleshooting

Message	Troubleshooting Steps
Failed to Install HPCA Management Agent - Reason: Failed to connect to *device* as user *user*. Code: No network provider accepted the given network path	The HPCA 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.
	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 though the HPCA console. If the devices are not part of a domain, additional steps are required to allow access for local administrators. Refer to the following Microsoft KnowledgeBase article for detailed steps.
	http://support.microsoft.com/kb/947232/en-us
	After making these changes, reboot the device.
Failed to Install HPCA Management Agent - Reason: Duplicate computer name.	Ensure that you do not have devices in your environment with duplicate computer names. It is possible to have duplicate computer names even if the IP addresses are all unique. Unique IP addresses produce unique DNS names – not unique computer names. Duplicate computer names will cause agent deployment to fail.
Failed to Install HPCA Management Agent - Reason: Failed to connect to *device* as user *user*. Code: Logon failure: unknown user name or bad password.	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.

Table 43   Agent Deployment Job Messages and Troubleshooting

Message	Troubleshooting Steps
Failed to Install HPCA Management Agent - Reason: Failed to connect to *device* as user *user*. Code: Logon failure: unknown user name or bad password.	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.
Connection timed out	After the HPCA 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 HPCA. 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 HPCA server using port 3466. If this port is blocked by a firewall on the HPCA server, the device cannot be managed by HPCA. Verify that port 3466 is added to the firewall exclusion list on the HPCA server.

OS Capturing Issues

This section includes common issues that are encountered during capturing an operating system image.

The capturing process fails due to the following error:

```
Capture Failed

Image preparation and capture failed:

1. Check the execution logs under:%Temp%/setup.

2. Consult the online help for further details.

Press OK to return to the OS capture wizard.
```

The `setup.log` and `prepwiz.log` under `%Temp%/setup` show an error similar to the following sample error:

```
There is not enough space on the boot volume so Prepwiz can
inject the Local Service Boot files.

    Required space: S:MB, available space: 185MB.
```

- Increase the boot partition size to a minimum of 300 MB or double the size of your `winpe.wim` file. The recommended boot partition size is one GB.

OS Deployment Issues

This section includes common issues that are 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.

OS Publishing Issues

This section includes common issues that are encountered during publishing an operating system image.

The publishing process fails due to the following error:

```
pub_file: File path
<InstallDir>\Data\OSManagerServer\capture-conf\x86\substitutes
specified does not exist.
```

- The error occurs when publishing an OS image that contains a corrupt or invalid install.wim file. Use an OS image that does not contain any corrupt files.

Application Self-Service Manager Issues

This section describes common HP Client Automation Application Self-Service Manager (ASSM) 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 HPCA power management feature.

Device does not respond to power commands from the HPCA server

If a managed device is not responding to a power on command from the HPCA server the problem may exist in the configuration of network devices such as routers and switches.

- Test the network path from the HPCA 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 when deploying patches to target devices (for example, you see the error message WUA Install Result Code 3 HRESULT $hresult), check to make sure the correct Windows Installer version is installed on the target devices that are receiving patch updates.

See Patch Management on page 140 for details regarding the supported minimum versions.

Troubleshooting the HPCA Server

The following section describes how to troubleshoot issues related to your HPCA server.

- Troubleshooting HPCA Core Components on page 431

Troubleshooting HPCA Core Components

The following sections describe how to troubleshoot issues related to the Core server components.

- HPCA Core Configuration Files on page 432
- HPCA Core Log Files on page 434

HPCA Core Configuration Files

The Core server installation sets default values for the various Core server components. These values should be left as-is, although some can be modified in the Core Console. The following table lists the locations and names of the configuration files in case they are needed for troubleshooting, or are requested by HP Technical Support.

The default path for the Core server's product configuration files is *<InstallDir>\xxxxxx*. If a different path was specified during the Core installation, be sure to follow that path. The value of *xxxxxx* will be replaced by the value in the Location column of the following table.

Table 44   HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (`C:\Program Files\Hewlett-Packard\ HPCA\...`)
HPCA Console	Apache Server	`ApacheServer\apps\console\etc\service.cfg`
	Apache Server	`ApacheServer\apps\console\etc\proxy.cfg`
	Sessionmanager	`tomcat\webapps\sessionmanager\WEB-INF\sessionmanager.properties`
	Sessionmanager	`tomcat\webapps\sessionmanager\WEB-INF\classes\log4j.properties`
Configuration Server		`ConfigurationServer\bin\edmprof.dat`
Distributed Configuration Server	Integration Server	`DistributedCS\etc\HPCA-DCS.rc`
	product	`DistributedCS\etc\dcs.cfg`
Messaging Server		`MessagingServer\etc\core.dda.cfg`
		`MessagingServer\etc\patch.dda.cfg`
		`MessagingServer\etc\rms.cfg`

Table 44   HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (`C:\Program Files\Hewlett-Packard\ HPCA\...`)
		`MessagingServer\etc\usage.dd.acfg`
OS Manager Server		`OSManagerServer\etc\HPCA-OSM.rc`
		`OSManagerServer\etc\roms.cfg`
		`OSManagerServer\etc\roms_upd.cfg`
Patch Manager		`PatchManager\etc\HPCA-PATCH.rc`
		`PatchManager\etc\patch.cfg`
Policy Server		`PolicyServer\etc\HPCA-PM.rc`
		`PolicyServer\etc\pm.cfg`
Portal	Integration Server	`ManagementPortal\etc\HPCA-RMP.rc`
	product	`ManagementPortal\etc\rmp.cfg`
		`ManagementPortal\etc\romad.cfg`
	OpenLDAP	`DirectoryService\openldap`
Reporting Server		`ReportingServer\etc\cba.cfg`
		`ReportingServer\etc\ccm.cfg`
		`ReportingServer \etc\ed.cfg`
		`ReportingServer\etc\rim.cfg`
		`ReportingServer\etc\rm.cfg`
		`ReportingServer\etc\rpm.cfg`
		`ReportingServer\etc\rrs.cfg`

Table 44 HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (`C:\Program Files\Hewlett-Packard\HPCA\...`)
		`ReportingServer\etc\rum.cfg`
		`ReportingServer\etc\scm.cfg`
		`ReportingServer\etc\vm.cfg`
Thin Client		`TC\etc\HPCA-TC.rc`
		`TC\etc\rmms.cfg`
Tomcat	HPCA Console	`tomcat\webapps\em\WEB-INF\Console.properties`
	HPCA Console	`tomcat\webapps\em\WEB-INF\classes\log4j.properties`
	OPE	`tomcat\webapps\ope\WEB-INF\classes\log4j.properties` (log levels)
	VMS	`tomcat\webapps\vms\WEB-INF\classes\log4j.properties` (log levels)

HPCA Core Log Files

If you are having issues with the Core server and need to access its log files for troubleshooting, the Core Console provides immediate access to the entire set of log files.

To generate the Core server log files

1   On the Core Console, go to the Operations tab and click **Support**.

2   In the Troubleshooting area, click **Download Current Server Log Files**.

3   When the WinZip file opens, extract and save the files.

You are not expected to understand the full contents of the files, but you should know how to access and view them in order to:

- Provide them to HP Support.

- Review them for entries that are labeled **severe**.

Browser Issues

The following troubleshooting tips pertain to issues that may arise with your browser:

-
-

Cannot Refresh Page Using F5

If you press the **F5** function key while using the HPCA Console, the splash screen will briefly appear, and then you will return to the last dashboard page that you viewed. You will not get a refreshed version of the page you are currently viewing.

Solution:

To refresh the page that you are currently viewing, use the built-in (Refresh) button on that page.

Cannot Enable HTTP 1.1 with Internet Explorer 6 and SSL

You cannot run the HPCA Console using Internet Explorer 6 with SSL if HTTP 1.1 is enabled. This is a limitation of Internet Explorer 6.

Solution:

Internet Explorer 6 is no longer supported. You must upgrade to Internet Explorer 7 or later.

Browser Error Occurs when Using Remote Control

The following message may appear when you attempt to launch either the VNC or the Remote Assistance remote control features from the HPCA Console:

```
Several Java Virtual Machines running in the same process caused
an error
```

This problem is likely due to a known defect in the Java browser plug-in. Refer to **http://bugs.sun.com/view_bug.do?bug_id=6516270** for more information.

Solution:

If this message appears, upgrade the Java Runtime Environment (JRE) used by your browser to JRE version 6 update 10 (or later).

Dashboard Issues

The following troubleshooting tips pertain to issues that may arise with the HPCA dashboards:

Delete Dashboard Layout Settings

The dashboard layout sessions are stored as a local shared object (like a browser cookie) on your computer. To delete the current settings, you must use the Adobe Website Storage Settings Panel to manage the local storage settings for Flash applications. Refer to the following web site for detailed instructions:

http://www.macromedia.com/support/documentation/en/flashplayer/ help/settings_manager07.html

Dashboard Panes in Perpetual Loading State

If the HPCA Consoleis hosted on a system where both of the following products are installed, some dashboard panes will remain in the Loading state forever while returning no results.

- Microsoft SQL Server with Service Pack 2
- Oracle ODBC Client Software

The following versions of the Microsoft SQL Server and Oracle client are known to cause a conflict with Reporting when installed on the same system:

Oracle ODBC Driver Version 10.2.0.1.0

Microsoft SQL Server 2005 Service Pack 2 (2005.90.3042)

To verify that this is the problem:

1 From the Control Panel, open the Event Viewer under Administrative Tools.

2 In the left navigation pane, select **System.**

3 Look for events with `Application Popup` in the Source column.

4 If you see an event with the following description, you are probably experiencing this error.

    Application popup: nvdkit.exe – Application Error: …

Solution:

Do not install both of these programs on the system hosting the HPCA Console.

RSS Query Failed

If an HPCA dashboard pane cannot connect to the RSS feed that provides its content, the following error message is displayed in the pane:

```
Connection to RSS feed {URL for RSS feed} has failed. Make sure
that the proxy server settings for HPCA Enterprise Manager have
been properly configured, you have subscribed to the RSS feed,
and that the RSS feed is accessible.
```

To determine the specific type of connection failure that has occurred, hover your mouse over the **RSS query failed** message in the lower left corner of the dashboard pane. One of the following messages will be displayed in a tool tip:

Table 45   Possible RSS Feed Failure Types

Failure Reason	Text Displayed
Proxy is not set	Error processing refresh: connection timed out: connect
Live Network password is invalid	Error processing refresh: Invalid Response: Login failed
You have not registered for the feed	Error processing refresh: Error on line -1: premature end of file

Solution:

Check the following things:

1   Make sure that the URL for the RSS feed is correct.

2   Paste the URL for the RSS feed site into a browser, and make sure that the site is accessible.

3   Make sure that your proxy settings for the HPCA Console are specified correctly.

4   Make sure that you have registered for the RSS feed, if necessary. To register for the feed, click the URL displayed in the error message.

Other Issues

The following troubleshooting tips pertain to issues not addressed in the previous topics:

Problems Configuring the SQL Server Database

When configuring a SQL Server database either in the first time setup wizard or from the configuration UI, you may experience problems with successfully completing the configuration. The configuration requires the specification of the reporting database DSN, user id, password, server, and port. There can be numerous reasons why the configuration is not able to be set.

The most likely causes are listed below.

- In SQL Server, the default static port is 1433. However, it is possible that the SQL Server installation is set up with a different static port or with a dynamic (non-specified port). For HPCA, you must use a static port. Verify your SQL Server port settings and update appropriately.

- The Server Host should be the hostname where the database resides. For example:

  `mydbserver.mycompany.com`

- If the SQL server setup is using something other than the default database instance, the instance needs to be appended to the server name. For example, if the named instance is HPCA, you would specify it as follows:

  `mydbserver.mycompany.com\HPCA`

- Check your authentication settings in SQL Server. If you are using Windows authentication, you need to use SQL Server authentication, and then update the Reporting Database Configuration appropriately.

Reporting Charts Display Problem in Non-English Environments

In non-English environments, the reporting charts display question mark (??) characters for certain strings. This erroneous display is caused by the fact that the JAVA JRE client installed on the client device is missing the non-English fonts file.

Solution:

This is a common Java issue regarding the `fonts.properties` file. The `font.properties` file in the JDK home directory has to be replaced with the one for the specific non-English environment to resolve this issue. For example in a Japanese environment, the `font.properties.ja` file should be used to replace the original fonts file.

Cannot Open a Report

This topic addresses the following problem:

1   You click the icon in a dashboard pane to open the pertinent report.

2   The report you requested does not open.

3   The Reporting home page opens instead.

This happens when a particular URL is blocked by the browser. If your browser security level is set to High, the URLs for the reports may be blocked. When the URL for a particular report is blocked, the default Reporting behavior is to display the home page.

This behavior is most prevalent with Internet Explorer 7 on the Windows 2003 Server platform. It can, however, happen on any supported platform.

Solution:

1   Open the list of blocked URLs.

2   In Internet Explorer 7, for example, click the eye-shaped icon with the red circle in the lower browser bar . The Privacy Report opens.
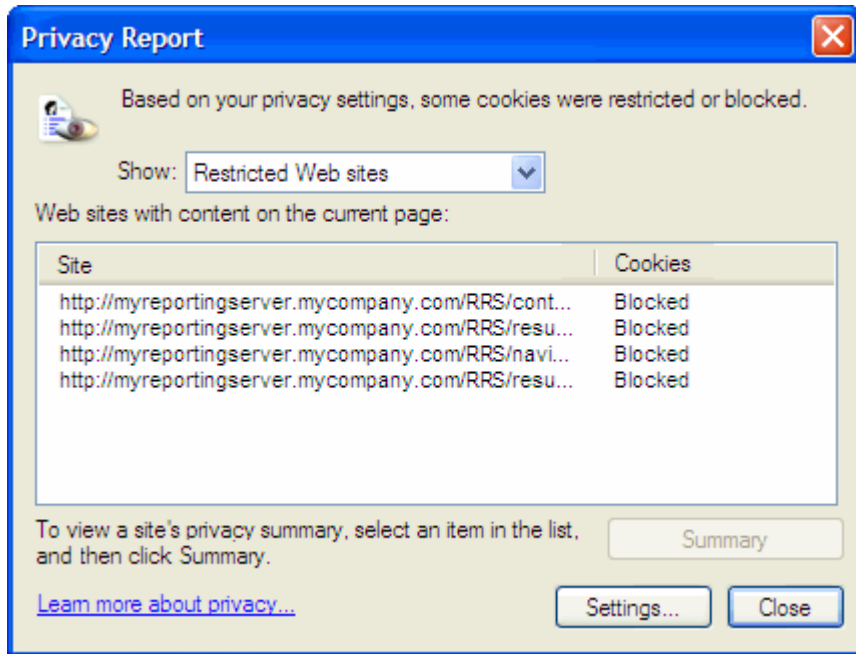
3   Using your browser privacy settings, add the URL for the report that you want to view to the **Allowed** cookies list.

Additional Parameters Disregarded by the HPCA Job Wizard

If you want to specify "additional parameters" when using the HPCA Job Creation Wizard, you must specify them in the following format:

```
option=value
```

If you do not use this format, the additional parameters are ignored. On the confirmation page (the last page of the wizard), be sure to verify that your additional parameters are included in the command line.

Virtual Machines Will Not Start

A licensing defect in ESX version 3.5 Update 2 (build number 103908) prevents Virtual Machines from being started after a certain date.

If you are running this ESX build, and you attempt to start a Virtual Machine from the HPCA Console, an error message similar to the following will appear in the console:

Result: "Start of Machine '*<machine name>*' failed"

Details: "Received Method Fault executing task
haTask-##-vim.VirtualMachine.powerOn-#####: A general system
error occurred: Internal error."

Solution:

Install ESX version 3.5 Update 2 build 110268 (or later).

For more information, refer to VMware *Release Notes* for this update:

**http://www.vmware.com/support/vi3//doc/
vi3_esx35u2_vc25u2_rel_notes.html**

Query Limit Reached

By default, only the first 1000 members of an Active Directory object are displayed in the HPCA Console. If you attempt to browse an Active Directory object that has more than 1000 members, a "Query Limit Reached" error message is displayed.

Recommended Solution:

Use the Search feature to fine tune the list of members displayed.

Alternate Solution:

Your HPCA administrator can specify the `directory_object_query_limit` in the `Console.properties` file for the HPCA Console. This file is located in the following directory:

`<tomcatDir>\webapps\em\web-inf\Console.properties`

By default, `<tomcatDir>` is as follows.

`<InstallDir>\tomcat`

After modifying the `Console.properties` file, be sure to restart the HPCA Tomcat service.

➤ Modifying the `directory_object_query_limit` property may negatively impact performance of the HPCA Console.

A SSL Settings on the HPCA Core and Satellite Servers

In order to fully understand how to use the SSL settings that are available on the HPCA Console, it is important to understand the various "parts" of SSL and their functions. This appendix offers a brief overview of SSL, including how it relates to an HPCA environment. See the following sections:

SSL Parts

SSL includes the following parts:

- Certificates

- Certificate Authorities (CA)

- Generating Certificates

- Private Key Files

- Public Key Files

In order to enable SSL, you will need the following:

- Public certificate and private key for each server that will have SSL enabled

- CA Certificates file if the servers' public certificates are signed by a CA not already included in the provided `ca-bundle.crt` file

SSL in an HPCA Environment

SSL uses **digital certificates** to establish proof of identity, and to establish shared **encryption ciphers** in order to provide secure communications. How you use SSL is dependent on how your infrastructure components are going to communicate. This section provides information on the two primary scenarios in which SSL should be enabled, and the role it plays in each.

Supporting SSL Communications to Remote Services

Assume that it is not necessary to secure the communications between the Core and Satellite servers; an SSL connection between them is not necessary. However, secure communications (LDAPS) are still required for the Core or Satellite server's communications with external servers (such as those hosting vendors' web sites), other HPCA servers, and Active Directory.

In order to trust that these other servers are "who" they claim to be, the Core or Satellite must obtain each server's **public certificate**, or the signature of the issuing **Certificate Authority** (CA). The Core or Satellite must also have a **CA Certificates file**, which it has obtained from a Certificate Authority, and which must be available to other servers so that they can decrypt messages from the Core or Satellite. (The Core and Satellite installations include a set of default trusted authorities, ca-bundle.crt, which is suitable for most environments.)

Providing Secure Communications Services to Consumers

Assume an environment in which the communications between the Core and Satellite servers needs to be secure. In this case, the Core will assume the role of server and, as such, will need a public certificate that it can share with the Satellites. The Core server's public certificate contains its public key, server name, and a signature from a Certificate Authority (attesting to the identity of the server).

- A public certificate (also known as a **server certificate**) can be given to anyone whom you want to trust you.

Further, each Satellite server, in the role of "client," will need its own set of certificates so that it can encrypt and decrypt messages between it and the Core. A certificate represents the Satellite, identifying it to the Core.

Each Core and Satellite also needs its own private key in order to decrypt messages.

- A **private certificate** (also known as a **private key**) should be kept private; it should never be shared.

The SSL Certificate Fields on the Consoles

The Infrastructure Management area of the Configuration tab of the HPCA Console contains two SSL Certificate areas: SSL Server and SSL Client. The differences between these areas and the necessity of each are explained in this section. To complete the SSL set up for the HPCA, review the information in this appendix, then see Infrastructure Management on page 225.

SSL Server

This area of the panel is used to enable SSL, and upload and save the private key file (server.key) and server certificate file (server.crt) for the HPCA servers. These files were either self-generated (within your organization) or obtained from a Certificate Authority. Check with your system administrator for access to these files.

- The private key file is needed in order to decrypt messages that were secured with the corresponding public key.

- The server certificate file is needed so that this host can identify itself to SSL-enabled servers.

After the files have been uploaded (located and **Save** clicked) these files are saved to:

<InstallDir>\ApacheServer\conf\ssl.

By default, these files will be saved with the names shown above, but the file names can be customized.

SSL Client

This area of the panel is used to upload and save the CA Certificates file (`ca-bundle.crt`) for the HPCA servers. This file contains a default set of trusted authorities that should be sufficient for most environments, and is needed only when an HPCA server communicates with another server over either LDAPS or HTTPS.

▶ It is possible to use an existing CA Certificates file that was obtained for your organization from a Certificate Authority. Check with your system administrator because you will need access to this file.

The CA Certificates file contains the signing certificates from trusted Certificate Authorities and is needed so that it can verify any incoming clients as "trusted."

After the file has been uploaded (located and **Save** clicked) it is saved to:

`<InstallDir>\ApacheServer\conf\ssl.crt.`

By default, the file will be saved with the name shown above, but the file name can be customized.

B About Double-Byte Character Support

This section covers the configuration changes that will set the locale for the service operating system (SOS). See the following sections:

▶ 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.

- Supported Languages on page 449
- Changing the Locale on page 450

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

Supported Languages

The following table presents the list of supported languages and their valid language codes.

Table 46 Supported Languages and Codes

Language	Language Code
Korean	ko_KR
English	en_US
Japanese	ja_JP
Simplified Chinese	zh_CN

Changing the Locale

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 specify a valid language code (see Table 46 on page 449).

The result will be the file resembling the following example in which the language was set to Japanese.

```
DEFAULT bzImage

APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1
ISVRPORT=3466 LANG=ja_JA
```

3   Save and close the default file.

To add support for a supported language when restoring from the Service CD-ROM

•   Specify **LANG=**xx_XX in the ServiceCD section of the `romsinfo.ini` file.

See Table 46 on page 449 for a list of supported languages and their valid codes.

•   The file `romsinfo.ini` is part of the Service CD iso.

Double-byte Support for Sysprep Files

If using double-byte character support in Sysprep, the file must be encoded in UTF-8 coding.

C Enhancing Reporting Performance

HPCA (Usage Manager) provides several scripts and materialized views that can be applied to the Microsoft SQL Server and Oracle databases to enhance the reporting performance.

The scripts and views are available at:

- `Media\Usage\Optional Features\SQL Server` for Microsoft SQL Server database
- `Media\Usage\Optional Features\Oracle` for Oracle database

Using Views

There are two types of views, Standard Materialized Views and Filter Materialized Views. Both views enhance reporting performance. Either one can be optionally applied to a database. Refer to the comments in the scripts for additional information about the functions of each view.

▶ The script names may abbreviate "Materialized" to "Mat", as in: `StepX_Define Filter Mat Tables` and `Indexes.sql`

Standard Materialized Views (SMV) - Converts all the views accessed by reports into tables. This view includes the index to enhance the query execution time. A feature where all the views (which is what the reports access) are converted into tables, and indexes are added to enhance the query speed.

Filtered Materialized Views (FMV) - Converts all the views accessed by reports into tables and requires filters to be applied before the views are converted into tables. The filters are stored in a separate table. For example, if a user selects `notepad.exe` as a filter, the FMV table is populated with the notepad details for all the devices. It is similar to SMV, but differs in that it requires filters to be applied at the time the views are converted into tables.

The filters are stored in a separate table. As an example, if a filter for Notepad.exe is selected, the FMV table will be populated with only notepad details for all the devices.

To apply the scripts for SMV or FMV

1 Stop the service for the **HPCA Knowledge Base Server**. The service may be stopped and started through the `Administrative Tools\Services` options of Windows Control Panel.

2 Use normal procedures to execute the database scripts, in the given order, provided in the following locations:

— For SQL Server:

    `\SQL Server\Optional Features\Filter Materialized Views`

    Or

    `\SQL Server\Optional Features\Standard Materialized Views`

— For Oracle:

    `\Oracle\Optional Features\Filtered Materialized Views`

    Or

    `\Oracle\Optional Features\Standard Materialized Views`

Each of the above locations also includes a corresponding script to remove the view from your database. For example, the script name for the Microsoft SQL Server and Filtered Materialized Views is:

    `SQLServer - Remove All Filter Mat Tables and Indexes.sql`

Utility Scripts

You as a database administrator can use the following scripts to enhance the reporting view performance:

• Purge_Computer_Data.sql: Deletes all data associated with the computer name. The computer name should be provided at the appropriate place in the script. The default value is MYCOMPUTER.

- Purge_User_Data.sql: Deletes all data associated with the computer name and the user name. The computer name and the user name should be provided at the appropriate place in the script. The default values are MYCOMPUTER and BOB.

- Delete All Windows OS Files from Database.sql: Deletes all Windows Operating System (OS) related files from the Usage Manager database.

Miscellaneous Scripts for Oracle

Miscellaneous scripts are additional scripts that can be applied along with the utility scripts to enhance the reporting view performance.

- Optional_Create_Public_Synonyms.sql: Creates public synonyms. The script may have to be edited for the Usage Manager's user names.

- Optional_Drop_Public_Synonyms.sql: Drops the public synonyms created by using the Optional_Create_Public_Synonyms script.

- Step99a_DropAll.sql: Drops all the tables present in the Usage Manager database.

D Customizing the Windows Answer File

This appendix contains the following topics:

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

Customizing the unattend.xml File

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

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

<InstallDir>\Data\OSManagerServer\capture-conf

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

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

- ProductKey on page 457
- TimeZone on page 459
- RegisteredOwner and RegisteredOrganization on page 460
- JoinDomain on page 460
- MetaData on page 462

⚠️ At a minimum, you must specify a valid product key (see ProductKey on page 457). Modifying the other settings discussed here is optional.

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

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

ProductKey

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

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

> For all DVD installations, be sure that /IMAGE/INDEX is pointing to the correct image on the DVD (see MetaData on page 462).

Retail Editions

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

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

```
<UserData>

    <AcceptEula>true</AcceptEula>

    <ProductKey>

        <Key>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</Key>

        <WillShowUI>OnError</WillShowUI>

    </ProductKey>

</UserData>
```

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

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

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

Business Editions

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

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

  `<Key></Key>`

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

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

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

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

64-Bit Platforms

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

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

  `<Key></Key>`

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

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

- Make sure that `/IMAGE/INDEX` points to the correct image on the media (see).

- Change `"amd64"` to `"x86"` in the following component specifications in the "WindowsPE" pass:

  ```
  <component name="Microsoft-Windows-International-Core-WinPE"
  processorArchitecture="amd64" ...
  ```

  ```
  <component name="Microsoft-Windows-Setup"
  processorArchitecture="amd64" ...
  ```

- During publishing, when you are prompted for the source directory, specify the one from the 32-bit media for the same operating system.

- Special instructions for Windows 2008 R2 x64:

  — Use the Windows 7 Enterprise Edition 32-bit installation media.

  — Before you publish the OS image, follow these steps:

    a From the Windows 7 32-bit installation media, copy the `mediaDrive:\sources` folder to `c:\temp`

    b Remove the Windows 7 media, and load the Windows 2008 R2 x64 media.

    c From the Windows 2008 R2 x64 installation media, copy the `mediaDrive:\sources\license` folder to `c:\temp\sources`

  If prompted to overwrite existing files, do so.

  This ensures that the Windows 2008 Server R2 EULAs are available from the Windows 7 installation folder.

► For more information, refer to the "ProductKey" topic in the `Unattend.chm` help file included in the Windows AIK.

⚠ HPCA does not currently support image capture for Windows Setup deployment on 64-bit platforms.

TimeZone

The `<TimeZone>` element appears in different places in the `unattend.xml` file depending on the specific OS image, architecture, and deployment method that you are using.

For example, in the `unattend.xml` file for a captured Windows 7 (x86) image, there are two places where the `<TimeZone>` element appears:

- In the `Microsoft-Windows-Shell-Setup` component under

  `<settings pass="oobeSystem">`

- In the `Microsoft-Windows-Shell-Setup` component under

  `<settings pass="specialize">`

Change the `<TimeZone>` to match the target devices to which the OS will be deployed. For example:

`<TimeZone>Eastern Standard Time</TimeZone>`

It is important that the spelling of the time zone exactly match the spelling used in the Windows Registry. For more information, refer to the "Language Pack Default Values" topic in the Unattend.chm help file included in the Windows AIK.

▶ Greenwich Mean Time is now known as Coordinated Universal Time.

▶ On a computer running Windows 7 you can use the tzutil command to list the time zone for that computer.

RegisteredOwner and RegisteredOrganization

These elements appear in different places in the unattend.xml file depending on the specific OS image, architecture, and deployment method that you are using.

For example, in the unattend.xml file for a captured Windows 7 (x86) image, there are two places where these two elements appear:

- In the Microsoft-Windows-Shell-Setup component under

    <settings pass="oobeSystem">

- In the Microsoft-Windows-Shell-Setup component under

    <settings pass="specialize">

Change these elements to the name of your company (or the entity to whom the operating system is registered). For example:

<RegisteredOrganization>Hewlett-Packard</RegisteredOrganization>

<RegisteredOwner>Hewlett-Packard</RegisteredOwner>

These strings can be up to 256 characters in length.

Refer to the "RegisteredOrganization" and "RegisteredOwner" topics in the Unattend.chm help file included in the Windows AIK for more information.

JoinDomain

You can instruct target devices to either join a domain or a workgroup after the OS is installed. Workgroup mode is the default. To instruct targets to join a domain, modify the following element:

```
<component name="Microsoft-Windows-UnattendedJoin" ... >
    <Identification>
        <Credentials>
            <Domain></Domain>
            <Password></Password>
            <Username></Username>
        </Credentials>
        <JoinDomain></JoinDomain>
    </Identification>
</component>
```

For example:

```
<component name="Microsoft-Windows-UnattendedJoin" ...>
    <Identification>
        <Credentials>
            <Domain>lan.mycompany.com.de</Domain>
            <Password>T3ch3d08</Password>
            <Username>administrator</Username>
        </Credentials>
        <JoinDomain>lan.mycompany.com.de</JoinDomain>
    </Identification>
</component>
```

▶ The user specified must have an access level sufficient to join the domain.

▶ If any of this information is missing or incorrect, the device will join a workgroup instead of a domain.

▶ If the target device was previously managed by HPCA, and the device was previously a member of a domain, the stored domain information will override the contents of the `<Domain>` and `<JoinDomain>` elements in the `unattend.xml` file.

▶ Any information that is set centrally—for example, by using an OS management script to set the domain—will override information in `unattend.xml`.

Refer to the "JoinDomain" topic in the `Unattend.chm` help file included in the Windows AIK for more information.

MetaData

If you are deploying an operating system image directly from a DVD, you must specify the location of that image within the WIM file on the DVD. In the WIM file, this information is organized like this:

```
<WIM>
    <IMAGE INDEX="2">
        <NAME>MyWIM</NAME>
        <DESCRIPTION>MyCustomWindowsImage</DESCRIPTION>
    </IMAGE>
</WIM>
```

In the `unattend.xml` file, the image information is specified in the `<MetaData>` element in the `Microsoft-Windows-Setup` component hierarchy under `<settings pass="WindowsPE">`. For example:

```
<MetaData>
    <Key>/IMAGE/INDEX</Key>
    <Value>2</Value>
</MetaData>
```

The `<Key>` element indicates which data item in the WIM file to match. It can be any of the following:

- `IMAGE/INDEX`

- `IMAGE/NAME`

- `IMAGE/DESCRIPTION`

The `<Value>` element indicates what the value of this data item should be. Here, the image to be deployed has an `IMAGE/INDEX` value of `2` in the WIM file.

You can extract a list of the images in a WIM file by using the following command:

```
imagex /info WIMFileName > c:\info.txt
```

Here, *WIMFileName* is the name of the WIM file (for example, `install.wim`). Be sure to redirect the output of the command to a text file (as shown here) so that you can easily search through the results.

For more information, refer to the *MetaData* topic in the `Unattend.chm` help file included in the Windows AIK.

XML File Processing in HPCA

The `unattend.xml` file that you publish is overlaid on top of any `unattend.xml` file that is present in the image that was published.

Before HPCA starts the image install, the published XML is combined with the `substitutes` file to generate the final `unattend.xml`.

This combining of files is done by HPCA before it starts the actual image installation. The previously exposed `substitutes` file is now used behind the scenes. Each operating system and architecture (for example, 32-bit or 64-bit) has its own file. The files are located in subdirectories of:

<InstallDir>\Data\OSManagerServer\capture-conf

The correct file is selected automatically depending on the processor architecture of the image being published.

Table 47 lists the settings in the `unattend.xml` file that are updated when the `substitutes` file is published.

⚠️ The settings in blue (`CommandLine`, `Path`, and both instances of `PartitionID`) are required for HPCA to work. They cannot be removed.

Table 47   Settings Updated Based on the `substitutes` **File**

Settings Pass	Component	Path	Setting	Override Value
windowsPE	Microsoft-Windows-Setup	DiskConfiguration/ Disk/ ModifyPartitions/ ModifyPartition	PartitionID	DISKPART volume ID to which HPCA will install the OS
windowsPE	Microsoft-Windows-Setup	ImageInstall/ OSImage/ InstallTo/	PartitionID	DISKPART volume ID to which HPCA will install the OS
windowsPE	Microsoft-Windows-Setup	ImageInstall/ OSImage/ InstallFrom/	Path	WIM file to use for installation

Table 47 Settings Updated Based on the `substitutes` **File**

Settings Pass	Component	Path	Setting	Override Value
oobeSystem	Microsoft-Windows-Shell-Setup	AutoLogon/	Domain	Computer name (for auto-logon)
specialize	Microsoft-Windows-Shell-Setup	AutoLogon/	Domain	Local computer name (for auto-logon)
specialize	Microsoft-Windows-UnattendedJoin	Identification/Credentials/	Domain	Centrally set domain via `getmachinename.tcl` or pre-existing device entry in the HPCA Core Console
specialize	Microsoft-Windows-UnattendedJoin	Identification/	JoinDomain	Centrally set domain via `getmachinename.tcl` or pre-existing device entry in the HPCA Enterprise console
specialize	Microsoft-Windows-Shell-Setup		Computer Name	Computer name
oobeSystem	Microsoft-Windows-Shell-Setup	FirstLogonCommands/SynchronousCommand	Command Line	Path to agent install media installer

You can, if required, customize the `substitutes` file to disable certain customizations or to add new ones. You cannot however remove or change the `PartitionID` or `CommandLine` settings.

About the .subs and .xml Files

⚠ HPCA now enables you to specify the source of this information when you run the Publisher. See Publishing Operating System Images on page 352 for more information.

▶ This topic does not apply to Windows XP or Windows 2003.

The HPCA Publisher is backward compatible. It supports publishing saved OS images that consist of a `.WIM` file, a `.EDM` file, a `.XML` file, and a `.SUBS` file.

If you choose to manually pre-create `*.SUBS` and `*.XML` files, they must have the same prefix as the `*.WIM` file. For example: `vista.WIM`, `vista.SUBS`, and `vista.XML`. All three files must be stored in the same directory.

▶ When you run the HPCA Publisher, if it finds a `*.SUBS` and `*.XML` file in the same directory as the `*.WIM` file, it will not prompt you for an `unattend.xml` file.

HPCA provides samples of these files on the Image Capture media in subdirectories of the following folder:

    \samples\unattend

If you choose to use the sample files, rename them and then modify them as needed—for example, setting the `<TimeZone>` and the `<ProductKey>`.

The `*.XML` file is an answer file that contains standard information as well as placeholders for information that will be included from `*.SUBS`. You can use the Microsoft Windows System Image Manager (SIM) tool to make additions to the `*.XML` file. If you do so, you must first open the corresponding `*.WIM` file before opening `*.XML`.

⚠ If you choose to use `*.XML` and `*.SUBS` files, you must specify your Windows installation product key in the `*.XML` file.

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

If you see errors in the Messages section in the SIM tool similar to "…`The value $$SUBSTR$$ is invalid`…" you can ignore them.

When you save the file, you may also see a message similar to "`There are validation errors in the answer file. Do you want to continue?`" Click **Yes** to continue.

The `*.SUBS` file is the "substitutes" file that lists each XML item to be modified in `*.XML` and what its value should be. The lines in the `*.SUBS` file are called XPATHs.

▶ Information entered in the `*.SUBS` file takes precedence over information in the `*.XML` file.

Example of Substitution

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

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

1 Locate the appropriate unattend*.xml and substitutes files for your operating system, target device architecture, and deployment method. These files are located under samples\ on the ImageCapture CD.

2 Make a copy of the unattend*.xml file, and name it *filename*.xml, where *filename* matches the name of your .WIM file. Store the copy in the same directory as your .WIM file.

3 Make a copy of the substitutes file, and name it *filename*.subs. Store the copy in the same directory as your .WIM file.

You should now have the following three files in one directory:

— *filename*.wim

— *filename*.xml

— *filename*.subs

4 Locate the XML element for JoinDomain in the *filename*.xml file. It should look similar to this example:

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

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

    <settings pass="specialize">
```

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

            <Identification>

                    <JoinDomain>anything</JoinDomain>

            </Identification>

        </component>

    </settings>

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

</unattend>
```

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

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

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

E Capturing Windows XP and Windows Server 2003 OS Images

▶ The information in this appendix pertains only to Windows XP and Windows Server 2003 OS image captures.

For information about capturing Windows Vista, Windows Server 2008, Windows 7, and all supported Thin Client operating systems—as well as important image capture process overview information—see Preparing and Capturing OS Images on page 321.

▶ HPCA only supports capturing unencrypted partitions.

⚠ The Legacy OS image capture method is not supported for devices where the hard drive is configured for RAID0 through a SATA drive controller. Use the Windows ImageX method instead.

This chapter includes the following topics:

About the HPCA Image Preparation Wizard

You can use the HPCA Image Preparation Wizard to capture Windows XP or Windows 2003 Server OS images for ImageX, Windows Setup, or Legacy deployment.

The Image Preparation Wizard performs the following tasks:

1 Collects and stores information (including hardware and OS information capabilities) about the reference machine.

2 Executes the exit points that are available for your use as needed. PRE.CMD is executed before the Image Preparation Wizard starts SysPrep to seal the image. POST.CMD is executed after Sysprep has sealed the image. See Image Preparation Wizard Exit Points on page 471 for details.

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

3 Runs Microsoft Sysprep (on supported operating systems).

4 Restarts the reference machine into the Service OS (booted from the appropriate media). The Service OS runs to collect the image and its associated files.

   During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 343 for more information.

5 Creates and copies files to the following directory on the HPCA server:

   <InstallDir>\Data\OSManagerServer\upload

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

   — ImageName.IMG
     This file contains the gold image. This is a compressed, sector-by-sector copy of the boot partition from the hard drive system that may be very large. The file contains an embedded file system that will be accessible when the image is installed.

   — ImageName.MBR
     This file contains the master boot record file from the reference machine.

   — ImageName.PAR
     The file contains the partition table file from the reference machine.

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

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

— `ImageName.WIM`
  This file contains a set of files and file system information from the reference machine.

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

Image Preparation Wizard Exit Points

You can use exit points for the Image Preparation Wizard as needed. For example, you may use them to clean up a device before performing a capture.

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

To use the exit points:

1 Create the files `PRE.CMD` and `POST.CMD`.

2 Save these files and any supporting files in `OSM\PREPWIZ\payload\default\pre` and `OSM\PREPWIZ\payload\default\post` respectively.

The Image Preparation Wizard copies these files to `%temp%\prepwiz\pre` and `%temp%\prepwiz\post` on the reference device and removes them before the capture begins. `PRE.CMD` is executed before the Image Preparation Wizard starts SysPrep to seal the image. `POST.CMD` is executed after Sysprep has sealed the image.

A non-zero return value from either `PRE.CMD` or `POST.CMD` will cause the Image Preparation Wizard to halt. In interactive mode, you can decide to Stop or Ignore the error and continue. In batch mode, the Image Preparation Wizard will halt.

Prerequisites for Capturing Images

The following steps must be completed prior to performing an OS image capture for ImageX, Windows Setup, or Legacy deployment:

Prepare the Reference Machine

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

> ⚠ Store the OS on the C: drive. It is the only drive that will be captured.

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

Article: 314479 - How to Add OEM Plug and Play Drivers to Windows XP

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

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

http://www.microsoft.com/downloads

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

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

4   If you plan to use the Legacy method to deploy this image, you must install the HPCA agent on the reference machine. This is not necessary for Windows Setup or ImageX deployments, because HPCA requires you to publish the agent along with the OS image for Windows Setup or ImageX.

For Legacy deployment only:

Install the agent from the HPCA installation media as per your requirements—at a minimum, you must install the Application Manager and OS Manager agents. These are required so that when the OS image is deployed, the device can connect to HPCA server. If you need to update the agents, you must use agent self-maintenance.

5   Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the HPCA server is finished.

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

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

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

The following steps help to minimize the size of the .WIM image file:

a   Create free space.

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

When ExtendOemPartition = 1, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The HPCA agent can then use the free space on the volume for application installations.

b   If you are using a laptop, disable hibernation.

c   If necessary, remove the recovery partition.

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

e   Turn off System Restore.

f   Turn off Indexing Service and Disk Compression.

g   Turn off On Resume Password Protect.

Install the Windows AIK

If you will use ImageX or Windows Setup for deployment, the Windows Automated Installation Kit (AIK) must be installed on the HPCA Core—where you will publish OS images to the HPCA database. This is a Core installation prerequisite.

Refer to "Using HPCA to Manage Windows Operating Systems" in the Installing HPCA chapter for more information.

Install and Configure Sysprep

Microsoft Sysprep is a program that enables you to distribute Microsoft operating systems using cloned images. The HPCA OS Image Preparation Wizard runs Microsoft Sysprep in order to strip out all of the security identifiers and reset the image.

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

To install Sysprep

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

> ▶ Review Microsoft's documentation for information about how to use Sysprep, how to create a Sysprep.inf file, and how to set the available parameters.

2   On the Microsoft operating system installation media, locate the
    DEPLOY.CAB file in the SUPPORT\TOOLS folder. See Microsoft's
    documentation for details.

3   Extract the Microsoft Sysprep files from the Deploy.cab file. Copy these
    files to C:\SysPrep on the reference machine and make sure the
    directory and files are not set to read-only.

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

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

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

        You must be an administrator to run this application.

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

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

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

To create Sysprep.inf

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

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

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

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

When creating the Sysprep.inf file:

- Adjust the `TimeZone` value for your enterprise.

- Set up the `AdminPassword`.

- Make sure to include a product key so that the user will not need to enter this at the target device.

- In order to have an unattended installation, you must include `UnattendMode = FullUnattended` in the `[Unattended]` section.

- Set `ExtendOemPartition` to 1, so that Microsoft Sysprep will extend the OS partition into any available non-partitioned space that physically follows on the disk.

- If `JoinDomain` is present in `Sysprep.inf`, then `Sysprep.inf` has to have the Admin User ID and Password of an account in the domain that has the rights to join the computer to the domain. Note that `JoinDomain` is case sensitive.

How Sysprep.inf Files are Prioritized

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

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

1 Sysprep embedded in the image (lowest priority). If there is no separately published `Sysprep.inf` (override Sysprep), just the `Sysprep.inf` in the image will be used.

2 Override Sysprep (a Sysprep file that is separate from the gold image. See "Using an Override Sysprep File" in the *HP Client Automation OS Management Reference Guide* for details).

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

3 Sysprep attached to policy criteria (highest priority).

Capturing OS Images

Refer to the instructions for the type of capture you want to perform:

Deployment Method	Instructions
ImageX, Windows Setup, Legacy	Capture Images Using the Image Capture Wizard on page 477 or Capture Images Using the Image Preparation Wizard in Unattended Mode on page 483

Capture Images Using the Image Capture Wizard

The following instructions pertain to OS image capture for ImageX, Windows Setup, or Legacy deployment.

To use the HPCA OS Image Preparation Wizard

▶ If you are capturing an image locally, before continuing, set the reference machine to boot from the CD-ROM/DVD drive. You must do this because the ImageCapture media is bootable. When you run the ImageCapture media, it reboots the device in order to upload the image.

1 Insert the ImageCapture media into the reference machine. See "Product Media" in the *HP Client Automation OS Management Reference Guide* if you need more information about where to get this media.

2 On the ImageCapture media, go to \image_preparation_wizard\win32, and run oscapture.exe.

 ▶ If the HPCA agent is not installed on the reference machine, you will see the following message.

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

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

> ▶ The `oscapture.exe` program requires the Microsoft .NET
> Framework version 2.0 (or later), which is available at the
> Microsoft download center:
>
> **http://www.microsoft.com/downloads**
>
> To determine which version of the .NET Framework is present on
> the reference machine, list the folders in the following directory:
>
> `%SYSTEMROOT%/Microsoft.NET/Framework`

— If you are capturing an image to be deployed using the Legacy method,
  the Image Preparation Wizard verifies that the `C:\Sysprep` folder
  exists and that the HPCA agent is installed before continuing.

— If you are capturing an image to be deployed using ImageX or
  Windows Setup, the Image Preparation Wizard will locate Sysprep in
  `C:\sysprep`.

> ▶ When using the Publisher, you will be given an option to select
> where to get the agent. This is advantageous, because you can
> package the agent independently and can update the agent as
> needed by publishing a new version to the HPCA database. After
> you do this, all new `.WIM` deployments will automatically use the
> latest agent.
>
> If you are using an HPCA Standard license, the agent must
> already be included on the image that was captured. However, you
> still must select where to publish the agent from when running
> the Publisher.

3 Click **Next**.

The End User License Agreement window opens.

4 Click **Accept**.

The deployment methods that may appear are:

— **Legacy** captures a raw disk image of the partition (`.IMG` format).

— **ImageX** captures an image in `.WIM` format that will be deployed using
  Windows PE and the ImageX utility.

— **Windows Setup** captures an image in `.WIM` format that will be deployed
  using Windows PE and Windows Setup.

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

5   Select the deployment method that you want to use, and click **Next**.

6   Type the IP address or host name and port for the HPCA server. This
    must be specified in the following format:

    xxx.xxx.xxx.xxx:port

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

7   Click **Next**.

8   Type a name for the image file. This is the image name that will be stored
    in the *<InstallDir>*\Data\OSManagerServer\upload directory.

9   Click **Next**.

    The Span Disk Image window opens.

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

    Use spanned images to break the image file into smaller segments. Each
    segment of a spanned image is restricted to 4000 MB. This is helpful so
    that you can comply with the restriction of whole images needing to be
    less than 4000 MB so that they can be stored in the HPCA database.

    If this value is set to 0 (zero), and the size of the image resource files
    exceeds 4000 MB, the image will be spanned automatically.

11 Click **Next**.

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

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

    ⚠   This is an advanced option. Any additional options that you add or
        changes that you make are not validated and may result in image
        capture or deployment failure. Use with caution or when instructed
        to do so by HP Software Support personnel.

    Review Microsoft's documentation for information about additional
    Sysprep options

12 Click **Next**.

13 If you chose ImageX for the deployment method, the Select Image
    Preparation Wizard payload window opens with the default option
    selected.

> The payload contains Local Service Boot (LSB) data to be delivered
> to target devices.

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

    The Select the Windows Edition window may open.

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

    The Options window may open.

> If you do not have the HPCA agent installed, you will not see the
> **Perform client connect after OS install** check box. It is important to
> have this agent installed only if you are using the Legacy method to
> capture an image.

16 Select the appropriate options.

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

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

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

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

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

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

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

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

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

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

17 Click **Next**.

The Summary window opens.

18 Click **Start**.

19 Click **Finish**.

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

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

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

21 Click **Next**.

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

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

23 Click **Finish** to run Sysprep.

The Image Preparation Wizard will start Sysprep; this can take 15-20 minutes to complete, depending on the size of the image.

> ▶ A message pops up if insufficient space is available on the System Reserve partition to hold the LSB injection files. You can either ignore this message or stop the Image Preparation Wizard. If you ignore the message (and have created enough space on this partition) the Image Preparation Wizard will continue. Otherwise, it will fail indicating that it cannot inject the LSB files.

During the capture, status information is displayed on the Service OS screen. See About the Windows PE Service OS Screen on page 343 for more information.

Sysprep will reboot the device when complete. You may need to click **OK** to restart the device.

> ▶ If you are using the audit mode (previously known as factory mode), the machine will reboot to the operating system with networking enabled. After your customizations are completed, you must put the Image Capture CD/DVD into the machine and then go to a command prompt and run
>
> **sysprep.exe –reseal –reboot**

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

— If the boot order is set to boot from CD-ROM first and the Image Capture media is loaded, the device will boot to the CD-ROM.

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

> ⚠ For Legacy capture mode, if the device does not boot to the CD (boots to operating system instead) you will need to restart the preparation process.

Then, the device will connect to the network, and store the image on the HPCA server.

➤ • The upload of the image may seem to take a long time. However, it is not the upload that is taking a long time, but rather the compression of the image and the optimization for compression of the unused disk space (especially if there is a lot of free disk space). This happens during the transfer of the image and therefore, the network pipe is not a bottleneck. Transfer speeds will be approximately 300 KByte/sec to 1MByte/sec or more but may vary depending on processor speeds and your network environment.

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

The Image Preparation Wizard connects to the network and stores the image on the HPCA Core in the following directory:

`<InstallDir>\Data\OSManagerServer\upload`

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

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

Next, you will want to publish your image to the HPCA database. See

Capture Images Using the Image Preparation Wizard in Unattended Mode

You may use a configuration file to run the Image Preparation Wizard in unattended mode.

To use the Image Preparation Wizard in Unattended Mode

1 Insert the ImageCapture media into the reference machine. See "Product Media" in the *HP Client Automation OS Management Reference Guide* if you need more information about where to get this media.

2 Go to \samples\prepwiz_unattend and copy the OS-specific configuration file (vista.cfg or xp.cfg) to your local machine or a network location.

3   Make the necessary modifications. Table 48 lists the values that you may need to change.

Table 48   Variables in the Configuration File to be Modified

Variable Name	Description	Sample Value
RISHOSTPORT	The HPCA server's IP address.	*xxx.xxx.x.x:port*
IMAGENAME	The prefix used to create the uploaded files. This is appended to `.WIM` to create the name of the uploaded image.	Vista
IMAGEDESC	Description of the image that is published to the Database.	"Windows Vista Unattended Test Image"
PREPWIZPAYLOAD (for future releases)	Payload that the administrator wants to use. The payload contains Local Service Boot (LSB) data to be delivered to target devices.	Use the default value "`/OSM/PREPWIZ/ payload/default/`"
OSEDITION (required for Vista)	Specifies the edition of Vista used.	"Enterprise"
set ::setup(DEPLOYOS,SELECTED)	Set to 1 or 0 to indicate whether you want to redeploy the OS after the image capture.	"0"
set ::setup(ClientConnect,SELECTED)	Set to 1 or 0 to indicate whether you want the target device to perform an OS a connect after the image is deployed.	"1"

4   On the reference machine, open a command window and change to the CD/DVD directory. Go to `Image_Preparation_Wizard\win32`. Then, run the following command:

```
prepwiz –mode silent -cfg <fully qualified
path>\<config_file>
```

Where <*config_file*> is the operating system-specific configuration file
(for example, `setup.cfg`).

The Image Preparation Wizard starts Sysprep; this can take 15-20
minutes to complete. Sysprep reboots the device when complete, connects
to the network and stores the image in the `/upload` directory on the
HPCA server.

Capture Images for Deployment using the Windows Native Install Packager

▶ Capture of Windows XP and Windows 2003 images for this deployment mode is only supported in HPCA Enterprise Edition.

This is the only case in which you will use the HPCA Windows Native Install Packager to prepare an image. The image is of the installation media for a pre-Windows Vista operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the HPCA agent. The image is sent to the `<InstallDir>\Data\OSManagerServer\upload` directory on the HPCA server, and then you use the Publisher to publish the image to the HPCA database.

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

Task 1: Prepare the Reference Machine

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

1 Connectivity to an HPCA server.

2 A target drive, recommended being on an extended partition, that:

— Will be used as if the target drive is currently formatted and empty (has no data). If the target drive is not formatted or it is formatted and contains data, the user will be prompted to format the drive.

— A user can pre-format the drive with FAT32 if they format the drive and ensure that there is no data on the drive.

> Note that FAT32 cannot be expanded after deployed. NTFS can be expanded and is the default.

— Is at least 1.5 GB. If the target drive is larger, it will take more processing time when the drive is imaged or the image may be larger than necessary depending on how the "Optimize Compression of Unused Disk Space" check box is set in the Image Preparation Wizard.

⚠ All data on the target drive will be lost.

3   A separate drive (to increase speed), such as the `C:` drive, with the HPCA Windows Native Install Packager software already installed. See Task 3: Install the HPCA Windows Native Install Package on page 489.

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

— The setup files for the HPCA agent.

— The `i386` directory from your operating system media.

You can slipstream any necessary service packs into this directory. See the `readme.txt` file associated with each service pack for more information about how to do this.

> Windows setup will not allow you to run the setup for an older version of Windows. For example:
>
>   • If your device is running Windows XP, you cannot use the `i386` directory for Windows 2000.
>
>   • If your device is running Windows 2003 Server, you cannot use the `i386` directory for Windows 2000 or Windows XP.

— `unattend.txt`

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

Task 2: Create unattend.txt

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

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

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

- The settings in the file should be as generic as possible so that the file can be used with any device in your environment.

- Include the statements `AutoLogon=YES` and `AutoLogonCount=1` in the `[GuiUnattended]` section of this file.

  You must use the `[GuiUnattended]` section, rather than `$OEM$\cmdlines.txt`, because the HPCA agent setup uses the Windows installer to install the agent on the target device, and `$OEM$\cmdlines.txt` cannot run the Windows Installer.

  The `AutoLogon` and `AutoLogonCount` statements ensure that the agent is installed during the first user logon after the operating system is installed.

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

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

- You can also create separate `unattend.txt` files for any necessary customizations. You can use the Publisher to publish these files to the SYSPREP class in the HPCA DB, and then you can connect them to the appropriate OS image. When the image is deployed, the customized `unattend.txt` will be merged with the original file.

  > See Publishing on page 347 for details about publishing files. When publishing `unattend.txt` files, follow the instructions as if you were publishing a `Sysprep.inf` file.

Task 3: Install the HPCA Windows Native Install Package

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

2 Click **Next**.

   The End User License Agreement window opens.

3 Review the terms and click **Accept**.

4 Select the directory to install the product in, and then click **Next**.

   The Summary window opens.

5 Click **Install**.

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

Task 4: Run the HPCA Windows Native Install Package

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

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

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

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

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

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

2 In the Client Automation Client Source Directory field, enter the path for the HPCA agent.

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

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

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

```
-trace_level 9
```

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

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

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

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

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

```
-trace_file filename.log
```

6 Click **Next**.

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

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

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

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

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

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

> ⚠ All existing data found on this drive will be lost.

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

11 Click **Next**.

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

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

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

15 In the **Client Automation OS Manager Port** text box, specify the port for the HPCA server.

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

17 Click **Next**.

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

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

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

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

> ▶ Remember the boot order must be set to boot from the CD-ROM/ DVD first.

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

21 Click **Finish**.

22 Reboot the device, and the image is uploaded the `<InstallDir>\Data\OSManagerServer\upload` directory.

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

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the HPCA database. For instructions, see Publishing on page 347.

When you have published the image, refresh the OS Library to view the list of available OS images. Use the HPCA Console toolbar to deploy the image to selected devices.

F   Building a Custom Windows PE Service OS

This chapter includes the following topics:

About the Custom Build Script

HP provides a script that enables you to:

- Add font support for Chinese and Japanese.

- Update the Windows Preinstallation Environment (PE) Service OS when a new `winpe.wim` file is made available through an updated Windows Automated Installation Kit (AIK).

- Add extra drivers or packages that do not exist in the Windows PE Service OS provided.

- Use the information in this chapter in conjunction with your knowledge of the Microsoft Windows AIK to rebuild the Windows PE Service OS with the drivers and packages necessary for your environment.

- Create a new `ImageCapture.iso` if you have updates that need to be applied, such as a change to the default Service OS or to the configuration of the boot menu.

- Create a new `ImageDeploy.iso` if you have updates that need to be applied such as a change to the default Service OS or to the configuration of the boot menu.

Prerequisites

Before you can use the script provided by HP to build a custom Windows PE Service OS, you must satisfy a number of prerequisites. See the following topics for details:

⚠ Do not attempt to run this script on a machine where incompatible software is installed. See the prerequisites for the Administrator Machine.

Process Knowledge

You will need a basic understanding of Microsoft's preinstallation customization process to add drivers and other information to the Windows PE Service OS.

Administrator Machine

To run the script, you will need an "administrator" machine with the 32-bit version of the Windows Automated Installation Kit (AIK) installed. This is the machine that you will use to build the customized Windows PE Service OS.

⚠ Do NOT use a machine where any of the following are installed:
- HPCA Boot Server
- HPCA Core or Satellite server
- Cygwin

Please note that with HPCA 8.1, we have updated Windows AIK to version 3.1. This is a supplement over Windows AIK 3.0 installation. The supported Operating Systems are:

- Windows 7 Service Pack 1
- Windows Server 2008 R2 SP1
- Windows Server 2003 with Service Pack 2
- Windows Vista SP1
- Windows Server 2008 family
- Windows 7 family
- Windows Server 2008 R2 family.

▶ Be sure to download and install the 32-bit version of the Windows AIK.

Media

You will need the following media (DVD or CD-ROM):

- HPCA product media
- HPCA Image Capture media
- HPCA Image Deploy media

Files and Directories

- You will need the build scripts bundle, build_scripts.zip, from the HPCA product media.
- If you are generating a new ImageCapture.iso or ImageDeploy.iso, you must do the following to include the updated files required.

    a Create a build items directory on the Administrator Machine, such as c:\build_items.

    b *Optional*: Copy any updated files that you have received from HP to this build items directory. Create subdirectories as needed, based on the structure of the Image Capture or Image Deploy media.

    If any of the required files are not in this directory, you will be prompted to insert the previous Image Capture or Image Deploy media so the files can be copied.

c   *Optional*: Include `romsinfo.ini` or `netinfo.ini` in the build items directory for use on the ImageDeploy CD.

d   *Optional:* Include `rombl_capture.cfg` and `rombl_deploy.cfg` in the build items directory for use on the appropriate ISO. These files contain information such as the menu timeout settings and the default Service OS.

To create these files, copy `rombl.cfg` from the previous `ImageCapture.iso` or `ImageDeploy.iso`, and modify and rename the files as necessary.

If you do not include these files in the build items directory, the script prompts you for the previous CD-ROM and retrieves the files from the media. If you choose not to insert a CD-ROM, a standard `rombl.cfg` file will be created automatically.

Support for Other Languages

If you want to add support for Chinese or Japanese without making additional changes to the ISO:

- Remove any existing `winpe.wim` files from the `build_items` directory.

- Copy `winpe_cjk.wim` from the `\custom_build\lang_support` directory on the product CD-ROM to the build_items directory.

- Rename `winpe_cjk.wim` to `winpe.wim`.

- See Building a Custom Windows PE Service OS on page 499 to run the script.

   ⚠ To use the Chinese or Japanese enabled `winpe.wim` file without rebuilding the `winpe.wim` file, be sure to type **N** when prompted to recreate the `winpe.wim` file.

- If you are using the ImageDeploy CD to install from CD—or you are installing from a cache and want messages to appear in your local language—copy the `\custom_build\lang_support\i18n` directory from the product media to the build items directory. You may remove the `.msg` files that are not needed for your local language.

Advanced Option

⚠ The following information is intended for experienced HPCA administrators only. Do not attempt to customize an existing `winpe.wim` file unless you have a strong understanding of both OS Management under HPCA and the Microsoft Windows AIK tools.

If you are using a pre-existing `winpe.wim` file:

- It is strongly recommended that the pre-existing `winpe.wim` was built using the same version of the Windows AIK that is installed on the machine where you are executing the build scripts.

- The `winpe.wim` file must have the following packages installed:
    - For Windows AIK version 1.1
        - `WinPE-HTA-Package`
        - `WinPE-Scripting-Package`
        - `WinPE-XML-Package`
        - `WinPE-WMI Package`
    - For Windows AIK version 2.0 and 3.1:
        - `WinPE-hta.cab`
        - `WinPE-scripting.cab`
        - `WinPE-wmi.cab`
        - `WinPE-setup.cab`
        - `WinPE-legacysetup.cab`
        - `WinPE-setup-client.cab`
        - `WinPE-setup-server.cab`

- If your `winpe.wim` file was prepared using the `peimg /prep` command, refer to the Microsoft documentation for the Windows AIK, peimg, and ImageX for restrictions (only applies to Windows AIK 1.1).

Adding Drivers to the Windows PE Service OS

You can add drivers to the Windows PE Service OS when you run the build scripts. For example, if you have a driver that requires a reboot, you must do it in "offline" mode. This means that the build script will pause, and you can make any necessary changes at that time. This is described in detail in the steps below.

► Additionally, you can add drivers to Windows PE while it is running ("online" mode). The drivers must be fully contained without need for a reboot, and the device must have connectivity to the HPCA server.

During the startup of the Windows PE Service OS, any drivers that exist in `<InstallDir>\OSManagerServer\SOS\WinPE\drivers` will be downloaded and installed using `drvload.exe`.

Building a Custom Windows PE Service OS

The following topics show you how to obtain and use the script that HPCA provides to build a custom Windows PE Service OS.

- To obtain the script and prepare to run it, see Get the Script on page 499.
- To launch the script and specify the information that it requires, see Run the Script on page 500.
- After you run the script, see Additional Information on page 504.

► Be sure to review and satisfy the Prerequisites on page 495 before you invoke the script.

Get the Script

The script that you will need to build a custom Windows PE Service OS is located on the HPCA installation media. Follow the procedure below to obtain the script and prepare to run it on your Administrator Machine.

1   Copy the following file from the installation media to a location on the
    Administrator Machine (where the Windows AIK is installed).:

    <InstallDir>\media\ISO\roms\build_scripts.zip

2   Unzip this file to a directory of your choice (such as C:\Build_scripts).

Run the Script

➤   This procedure assumes that you have satisfied the prerequisites (see
    Prerequisites on page 495) and obtained the script (see Get the Script on
    page 499).

For each question that the script asks, the default response is shown in
brackets on the far right side of the window. For example:

```
Type a number between 1 and 9                                    [1]:
```

In this example, the default response is 1. To accept the default, press **Enter**.

To build a custom Windows PE Service OS

1   Go to a Windows command prompt, and change to the *<version>* folder
    in the directory that you just created.

    Here, *<version>* is the SOS version number. For example:

    C:\ Build_scripts*<version>*

2   Type **run**

    In a few moments, a list of HPCA versions is displayed.

3   Type the number corresponding to the HPCA version that you want to
    use.

4   When asked whether you want to create a new WIM file, type **Y** or **N**.

    ➤   If the script that you are running was provided with an OS
        management service OS update (driver patch), you cannot create a
        WIM file. You can only create ISO files.

    If you typed **Y**, follow these steps to specify the WIM file options:

    a   You will be prompted to type the path to your Windows AIK tools
        directory. For example, C:\Program Files\Windows AIK\Tools

b When asked whether you want to use the `winpe.wim` file from the Microsoft Windows AIK, type **Y** or **N**.

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

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

c When asked whether you want to include font support for Chinese, and Japanese, type **Y** or **N**.

d When asked whether you want to pause the WIM creation process to add extra drivers or packages, type **Y** or **N**.

e When asked whether you want to provide a path to a directory containing additional drivers to be added during the WIM creation process, type **Y** or **N**.

f If you typed **Y**, you will be asked to enter the fully qualified path to the directory containing the drivers.

5 The next group of questions determines whether you want to create a new Image Capture ISO or Image Deploy ISO and which Service OS to include.

— You should create a new Image Capture ISO (type **Y**) if any of the following conditions are true:

– You have received updated files from HP Software Support.

– You have rebuilt `winpe.wim`, and you are using the ISO to perform the capture.

– You need to change the configuration (`rombl.cfg`, `netinfo.ini`, or `rominfo.ini`).

— You should create a new Image Deploy ISO (type **Y**) if any of the following conditions are true:

– You have received updated files from HP Software Support.

– You have rebuilt `winpe.wim`, and you are booting from the CD during deployment.

– You need to change the configuration (`rombl.cfg`, `netinfo.ini`, or `rominfo.ini`).

Follow these steps to specify the ISO options:

a   When asked whether you want to create a new Image Capture ISO, type **Y** or **N**.

b   When asked whether you want to create a new Image Deploy ISO, type **Y** or **N**.

c   If you answered **Y** to question (a) or (b), you will be asked which Service OSs to include on the ISO. Type the appropriate selection. Then, press **Enter**.

d   When asked if you want to create a new `rombl.cfg` or use a pre-existing `rombl.cfg` file, choose one of the following actions:

   –   To create a new `rombl.cfg` file, type **1**, and press **Enter**.

   –   To use a pre-existing `rombl.cfg` file, type **2**, press **Enter**, and skip to step (h on page 502).

e   When asked which Service OS you want to boot by default, type the appropriate selection. Then, press **Enter**.

f   Specify how the boot menu should be handled in each ISO that you are creating. There are three choices:

0	Hide the boot menu from the user of the target device. The default service OS that you specified in step (d and e) will be used.
-1	Show the boot menu, and wait for a user response. The response will override the default Service OS setting.
Number greater than zero	Show the boot menu, and wait this number of seconds for a user response before booting into the default service OS specified in step (e).

g   When asked if you want to change the port used to connect to the HPCA infrastructure, type **Y** or **N**. The default port is 3466.

h   When asked if want to specify the ISO boot load value that gets included in the ISO boot sector, type **Y** or **N**.

   ⚠   Use this option only if you experience problems using the default value and you have been instructed by HP Software Support to change it.

Certain hardware models require a boot load segment of 0x2000 due to a BIOS issue. Other models cannot boot from the CD when the boot load segment is something other than the default loader segment of the El Torito ISO format: 0x0000.

To specify the boot load segment setting, type **1**, **2** or **3**:

1 HPCA default (0x2000) – works with most BIOSs

2 ISO default (0x0000) – gets translated to 0x07c0 by most BIOSs

3 Manually enter a value

Then press **Enter**. If you typed **3**, specify the boot load segment setting as a hexadecimal string beginning with 0x.

i When prompted for the fully qualified path to the build items, type the directory name (such as C:\build_items), and press **Enter**.

This completes the questions pertaining to the Image Capture and Image Deploy ISOs.

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

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

7 When prompted for the fully qualified path for the output directory, type a directory name such as (C:\build_output).

> ▶ If you are prompted to create ISOs for CAS, type **N**.

The build process takes some time, as you will see from the on-screen messaging. When it is finished, you will see a message indicating that the Service OS creation process completed successfully and be returned to a command prompt.

After the build is completed, go to the directory where the `Windows PE.wim` was stored, such as `C:\WinPE_output`, and perform the following action:

Table 49

Boot Method for Target Devices	Action Required
PXE	Copy `winpe.wim` from the output directory to `<InstallDir>\BootServer\X86PC\UNDI\boot`
LSB	Use the CSDB Editor to replace `winpe.wim` in the LSB package.
CD	Create a new ISO using the Windows PE scripts.

If you chose to create `ImageCapture.iso` or `ImageDeploy.iso`, they will be stored in the same output directory.

Additional Information

After you provide all the information that the custom Windows PE service OS build script requires, the following things happen:

1 If files that are required to build the ISO are not in the build items directory, you must insert the CD/DVD, and the files will be copied. If you choose not to insert the CD/DVD, the build process will terminate.

2 The information that you entered is saved, and the Windows PE directory creation begins.

3 If you indicated that you wanted to pause the WIM creation process to add extra drivers or packages, the process will pause after the Windows PE directory is created and the contents of `winpe.wim` are extracted into the WIM directory (for example, `C:\build_work\WIM`). There are two ways to do this:

Method A: Use a Windows AIK tools to make your modifications.

If you are using Windows AIK version 1.1, use the `peimg.exe` command. The default location of this executable file is:

```
C:\Program Files\Windows AIK\Tools\PETools\peimg.exe
```

If you are using Windows AIK version 2.0 or 3.1, use the `dism.exe` command. The default location of this executable file is:

`C:\Program Files\Windows AIK\Tools\Servicing\dism.exe`

Refer to the Windows AIK documentation for information about how to use these commands (or use the **/help** command line option).

Method B: Add the drivers to a driver list.

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

For example:

```
declare DRIVERS = " cdrom.inf \

        e:\\tmp\\work\\WIM\\windows\\inf\\adp94xx.inf \

        e:\\tmp\\work\\WIM\\windows\\inf\\3com*.inf "
```

Because the back-slash (\) is a special character, you must "escape" it by using two back-slashes, as shown in this example.

Note that all lines except the last end with a back-slash. In this case, the back-slash indicates a continuation of the declaration.

If you do not specify a directory, the script will search for the driver in the *<work-dir>*\WIM\Windows\inf directory.

If you prefer, you can provide a fully qualified path that specifies the location and driver, such as `c:\\anydirectory\\mydrivers.inf`

You can also specify a path with a filename containing a wild card, such as `c:\\anydirectory\\md*.inf`, which will install all `md*.inf` files found in `c:\anydirectory`.

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

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

Using Customized build.config Files (Advanced Option)

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

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

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

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

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

Index

Status window
   Bandwidth Control, 386
   Button Bar, 385
   docking, 378
   Status Area, 385
   Status Message Area, 386
   undocking, 377

Stop Job(s), 162

support, 216

Synchronize Infrastructure Server, 237

Synchronize Software, 125

Sysprep.inf file
   creating, 476
   prioritizing, 476

SysprepMassStorage section, 480

SystemInstall column, 382

system requirements, 29
   HPCA Core
      communications ports, 31
      target devices, 88
   HPCA Satellite
      communications ports, 31
      target devices, 88

system tray
   active state, 384
   idle state, 384

T

TCP ports, 31

Thin client
   prepare and capture images, 332

thin client, 153
   deploying factory OS images to, 153

throttling, 383
   adapt to traffic, 384
   bandwidth, 384

ThrottlingType column, 382

TimeZone parameter, 476

TPM
   configuring, 257

TPM Enablement service, 130

transform file, 350

Transforms publishing option, 350

U

UDP ports, 31

UIOption column, 382

unattended mode
   Image Preparation Wizard, 483

UnattendMode parameter, 476

undocked Status window, 377

UpgradedDate column, 382

Url column, 383

Usage Collection, 207

Usage Collection Agent, 209

Usage Collection Filter
   creating, 208, 308
   enabling, 208
   modifying, 208

Usage Criteria, defining, 209

usage data, filtering, 210

usage data, obfuscating, 275

Usage Manager Reports, 175

Usage Settings page, 274

User Details window, 219

user interface for Application Self-service
   Manager, 367

Use system colors option, 379

We appreciate your feedback!

If an email client is configured on this system, click [Send Email]

If no email client is available, copy the following information to a new message in a web mail client and send the message to **docfeedback@hp.com**.

Product name and version: HP Client Automation 8.10

Document title:

Feedback: