HP Client Automation

Core

Starter Edition

for the Windows® operating systems

Software Version: 7.50

User Guide

Manufacturing Part Number: none
Document Release Date: May 2009
Software Release Date: May 2009

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

Trademark Notices

Documentation Updates

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

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

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

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

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

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

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

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

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

7 Configuration 147

1 Introduction

HP Client Automation Starter 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 *HP Client Automation Core and Satellites Getting Started and Concepts Guide.*

2 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 19
- Quick Start Tasks on page 20

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 139 and Configuration on page 147.

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 147 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 153 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 immediatley 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 22

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

Task 2: Deploy the HPCA Agent on page 23

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

Task 3: Configure Schedules on page 23

Configure schedules for inventory checking and patch management.

Task 4: Publish Software and Acquire Patches on page 24

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.

Task 5: Create Groups on page 25

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

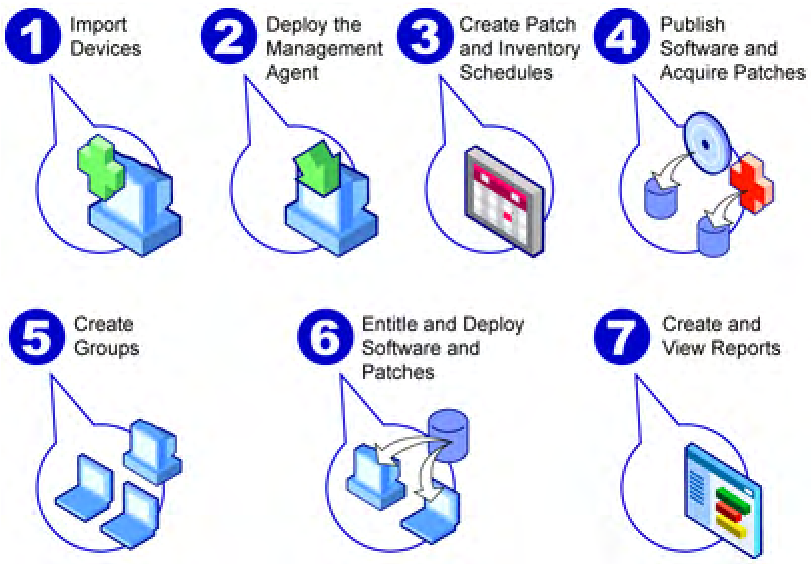
Task 6: Entitle and Deploy Software or Patches on page 26

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.

Task 7: Generate and View Reports on page 27

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


1 Import Devices
2 Deploy the Management Agent
3 Create Patch and Inventory Schedules
4 Publish Software and Acquire Patches
5 Create Groups
6 Entitle and Deploy Software and Patches
7 Create and View Reports

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.

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

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 KnowledgeBase 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 checkbox 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 185 to define software and hardware inventory collection for your devices and groups.

To configure patch acquisition schedule and settings

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

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.

> ➤ Microsoft Patch Management is available only with HPCA Standard edition.

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 Using the Publisher on page 213 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, Task 3: Configure Schedules on page 23.

  ➤ 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 Task 5: Create Groups to entitle software and patches for deployment.

Task 5: Create Groups

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

- 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 Group Management on page 72 for more information.

When the group has been created, go to Task 6: Entitle and Deploy Software or Patches 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.

3 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 30
- HPCA Operations Dashboard on page 34
- Patch Management Dashboard on page 40

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 34 shows you how much work is being done by the HPCA infrastructure.
- The Patch Management Dashboard on page 40 shows you information about any patch vulnerabilities that are detected on the devices in your network

Each dashboard includes two views:

Table 1 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 177 for more information.

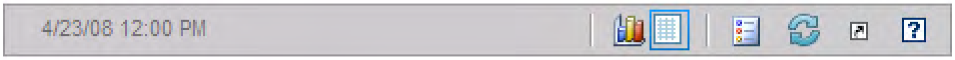
Each dashboard also includes a home page with summary statistics and links to related reports. When you click one of these links, a separate browser window opens, and displays the report.

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



4/23/08 12:00 PM

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 2 Dashboard Pane Actions

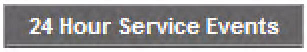
Icon	Description
📊	Display the information in chart format.
▦	Display the information in grid format.
☰	Display the legend for this chart.
🔄	Refreshes the data from its source. Click the refresh icon in an individual pane to refresh the data for that pane. Click the refresh icon in the upper right corner 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 2 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.
?	Open 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.
?	Open 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



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 282 for instructions.

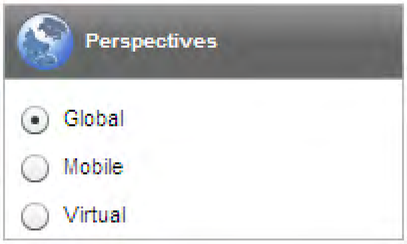
➤ If you press the **F5** function key while viewing one of the dashboards, you will return to that dashboard page after your browser reloads the HPCA Console.

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.

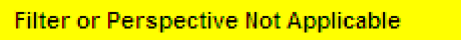
To apply a perspective, select it in the Perspectives box in the upper left corner of the console:



Perspectives

● Global
○ Mobile
○ Virtual

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 35

Service Events on page 36

The Executive View also includes the following pane:

12 Month Service Events by Domain on page 38

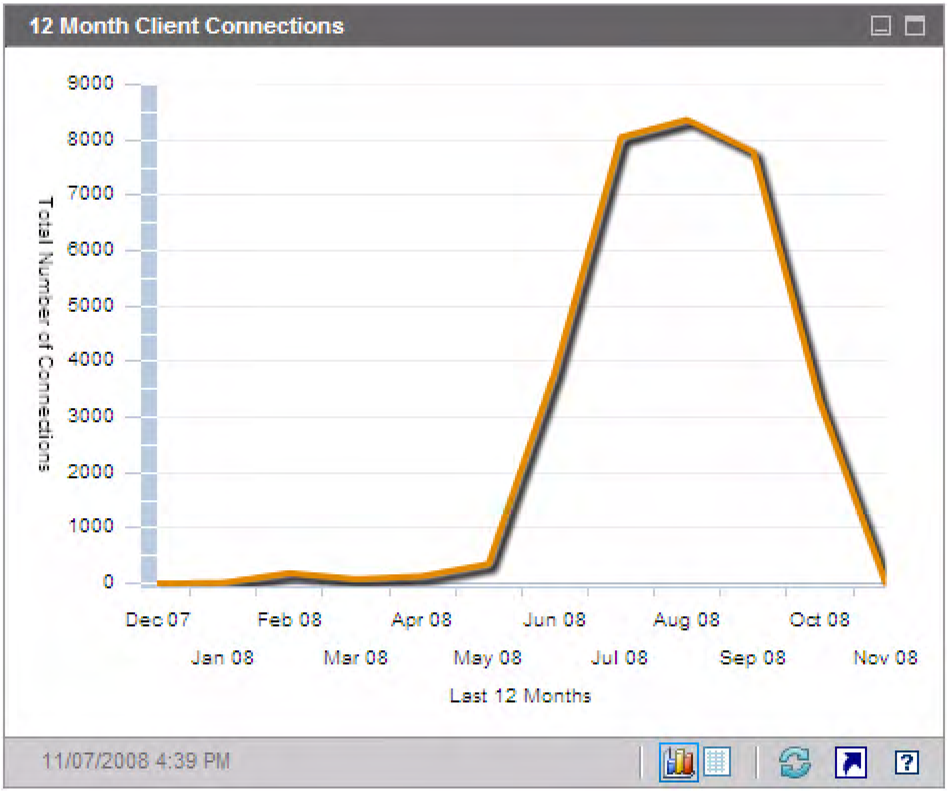
All of these panes are visible by default. You can configure the dashboard to show or hide any of these panes. See Dashboards on page 177.

➤ 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

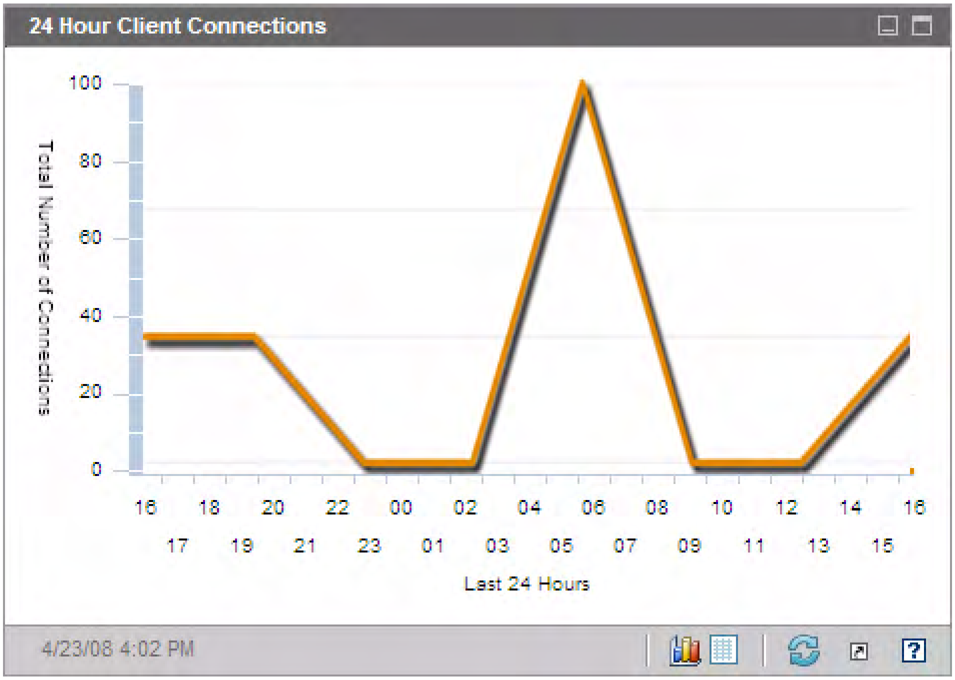
The chart view of this pane shows you the number of HPCA agent client connections that have occurred over the last twelve months (Executive View) or 24 hours (Operational View). When you rest the cursor on a data point, you can see the total number of connections for that month or hour.

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.

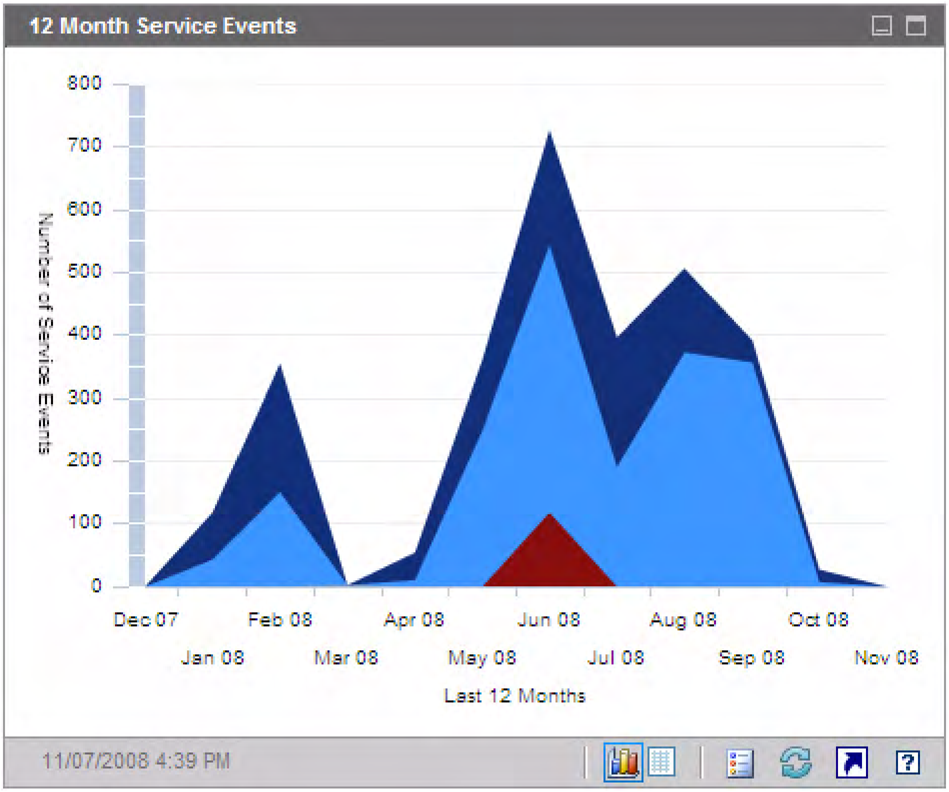
Service Events

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

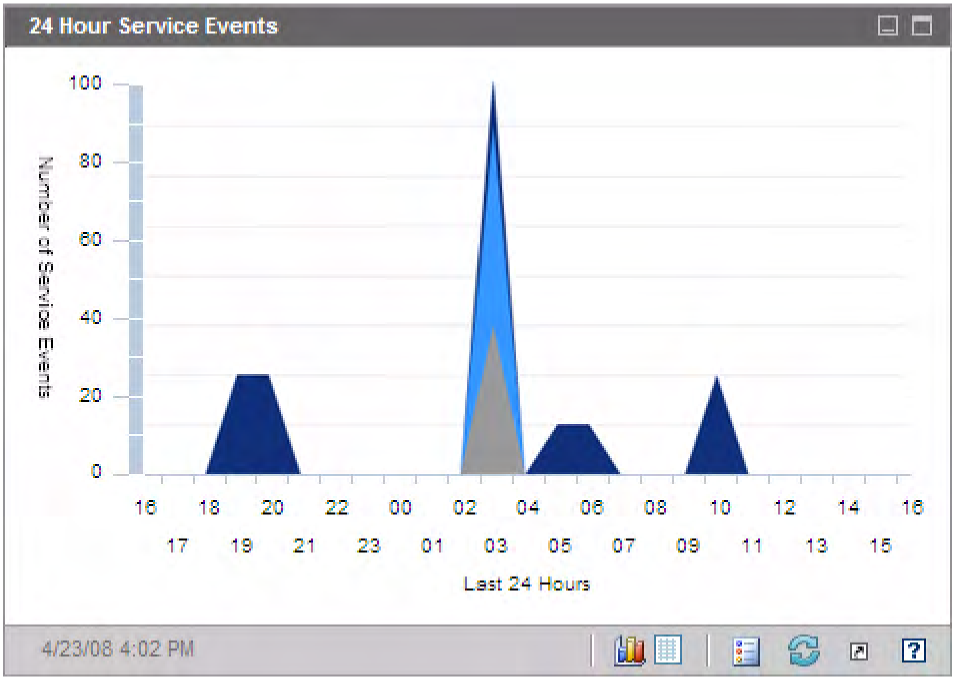
When you rest the cursor on a data point, you can see the number of service events that were completed during a particular month or hour.

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

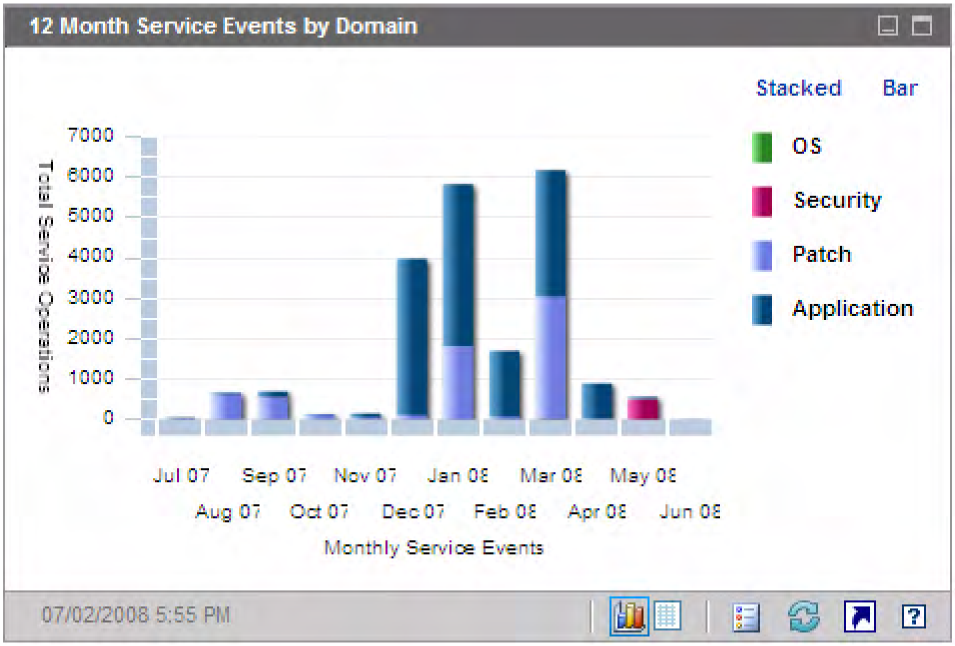
The chart view of this pane shows you how many of each of the following services that HPCA performed during each of the last 12 months:

- 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 two information panes:

- Device Compliance by Status (Executive View) on page 40
- Device Compliance by Bulletin on page 42

The Operational View includes three information panes:

- Device Compliance by Status (Operational View) on page 44
- Microsoft Security Bulletins on page 45
- Most Vulnerable Products on page 46

You can configure the dashboard to show or hide any of these panes. See Dashboards on page 177.

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:

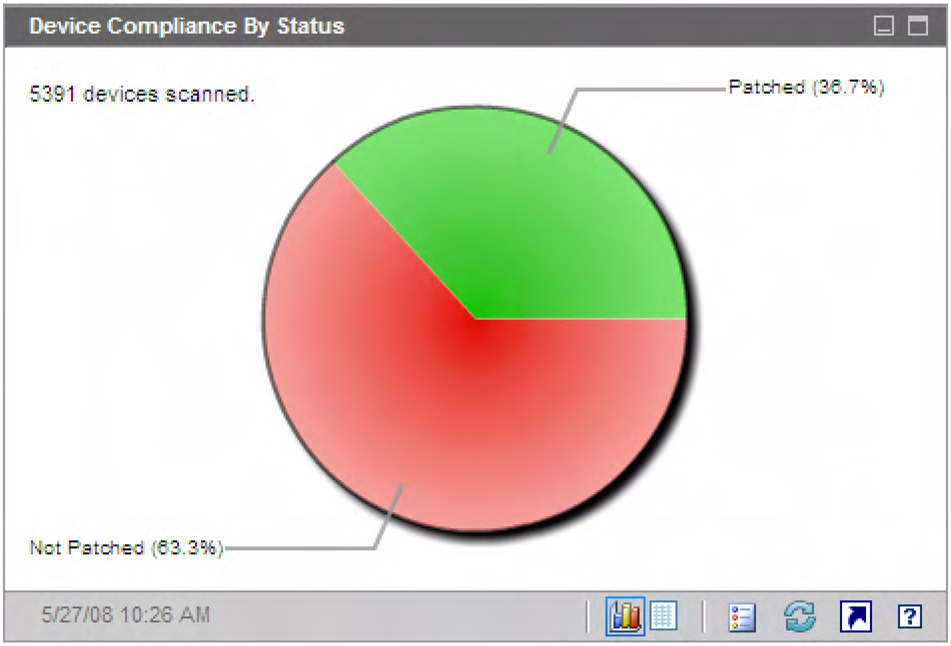
- Patched (green)
- Not patched (red)

The Device Compliance by Status (Operational View) on page 44 is similar but has finer-grained detail:

Table 3 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



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.

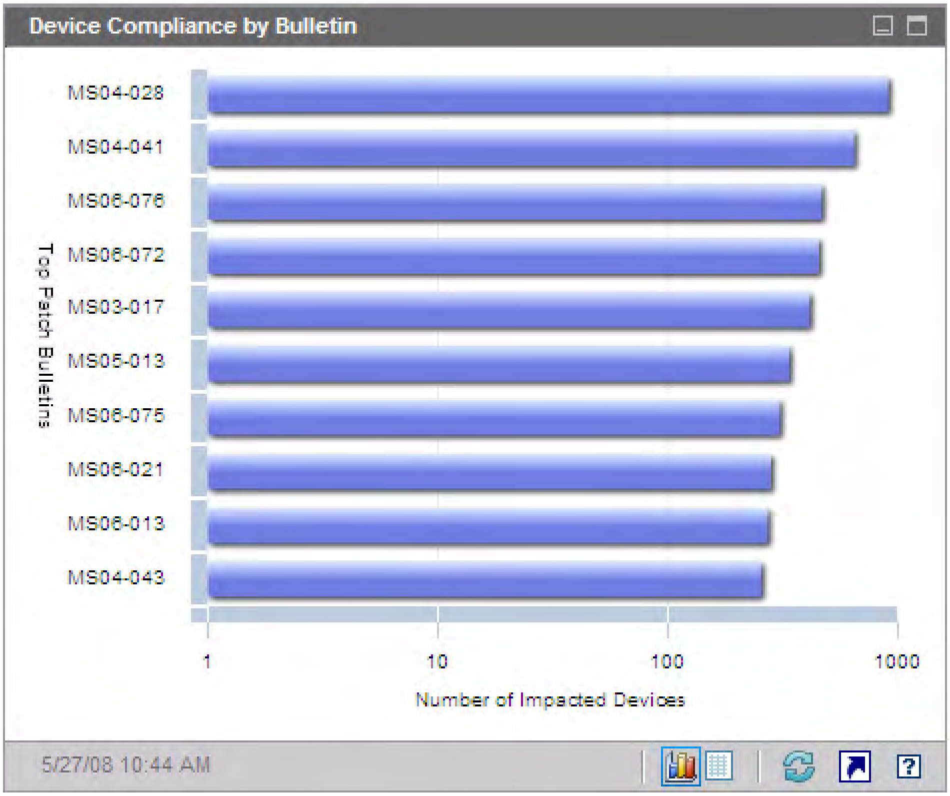
Device Compliance by Bulletin

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 affected 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.

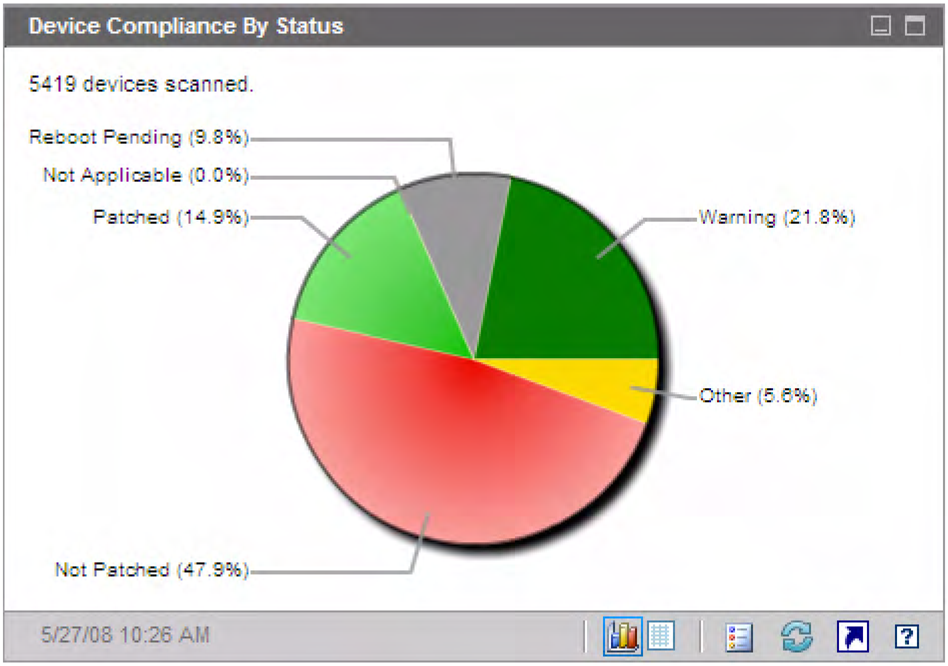
Device Compliance by Status (Operational View)

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. This pane shows finer 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 11 Device Compliance by Status (Operational View)



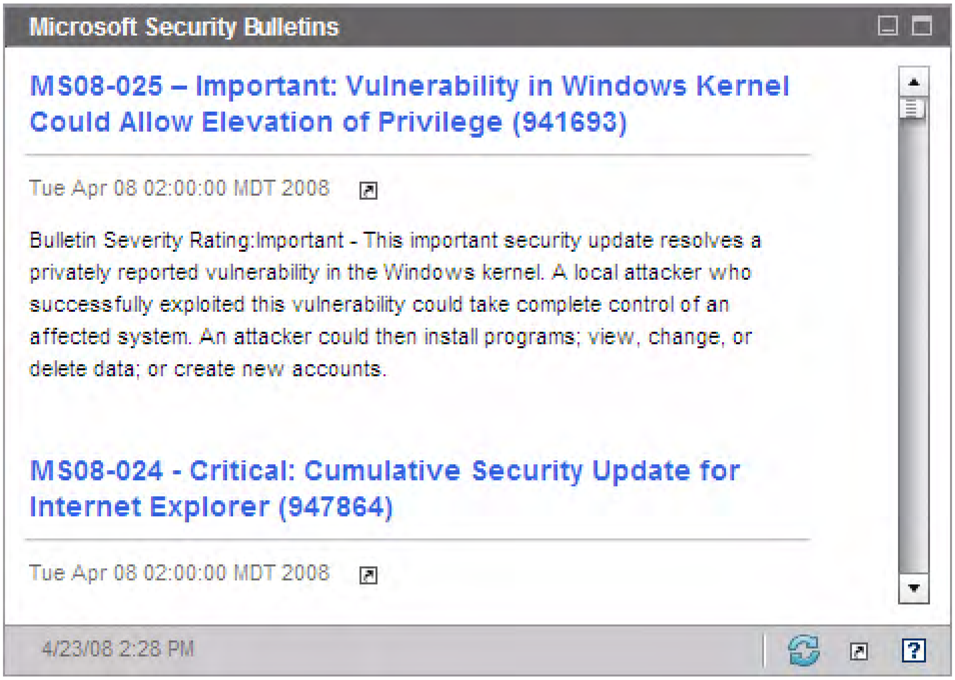
If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.

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 177).

Figure 12 Microsoft Security Bulletins



Microsoft Security Bulletins

MS08-025 – Important: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)

Tue Apr 08 02:00:00 MDT 2008

Bulletin Severity Rating:Important - This important security update resolves a privately reported vulnerability in the Windows kernel. A local attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

MS08-024 - Critical: Cumulative Security Update for Internet Explorer (947864)

Tue Apr 08 02:00:00 MDT 2008

4/23/08 2:28 PM

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 177.

The chart view of this pane shows you the software products in your network that have the largest number of patch vulnerabilities. The vertical axis lists the software products. The horizontal axis reflects the total number of patches pertaining to a particular product that have not yet been applied across the applicable managed devices in the enterprise. For example:

Say that product ABC has 6 bulletins that contain patches

— 10 managed devices require all 6 of these patches

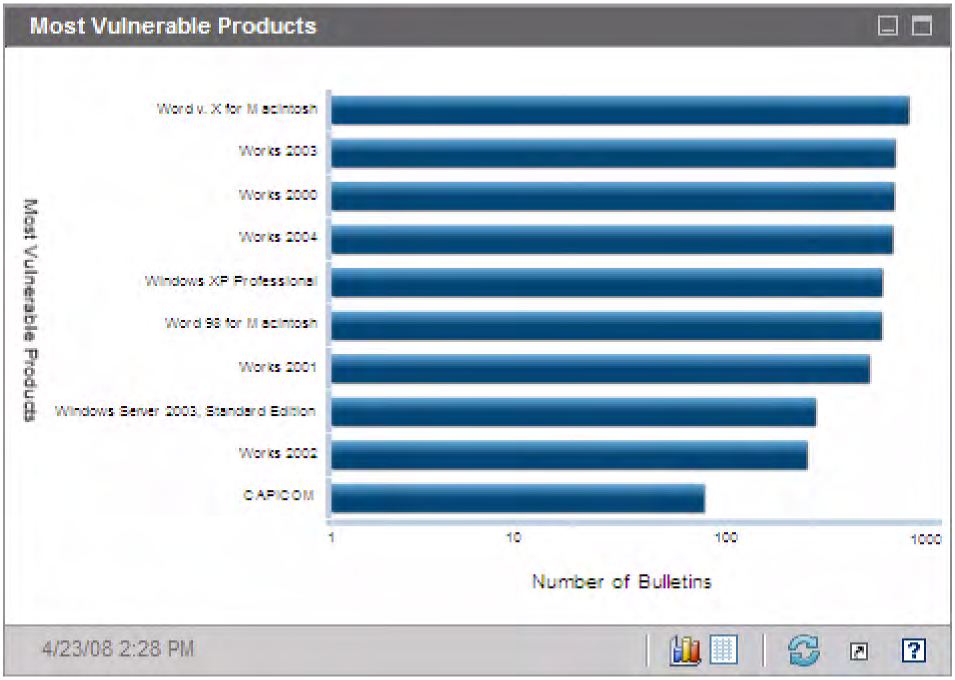
- 20 managed devices require 3 of these patches
- 50 managed devices only require 1 of the patches

Number of Bulletins for ABC = (10 x 6) + (20 x 3) + (50 x 1) = 170

Because this chart uses a logarithmic scale, if the Number of Bulletins 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. The data is visible in the grid view, however.

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 13 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 bulletins on all applicable devices for a particular product
- Applicable Devices – Number of devices on which this product is installed

- Applicable Bulletins – Number of Microsoft Security Bulletins that pertain to this product

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

4 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 50
- Group Management on page 72
- Software Management on page 85
- Patch Management on page 95
- OS Management on page 105
- Job Management on page 120

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:

- General on page 53
- Devices on page 54
- Current Jobs on page 64
- Past Jobs on page 64

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

- Target Device Prerequisites on page 50
- Manually Installing the HPCA Agent on page 64

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.

- Thin client devices that are to be managed by HPCA should have Windows CE, Windows XPE, or Embedded Linux installed.
- **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 `C:\Program Files\Hewlett-Packard\HPCA\Agent`:

  `RadUIShell.exe`

  `Radexecd.exe`

  `nvdkit.exe`

  `nvdtk.exe`

- And in `C:\Program Files\Hewlett-Packard\HPCA\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

Windows XPe thin client devices ship with the **Symantec Endpoint Protection** agent pre-installed. Therefore, two rules—one for the HPCA executables and one for the ports—must be created to allow HPCA to operate.

To create the HPCA executables rule

If you are running File-Based Write Filter, you must diable 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 `C:\Program Files\Hewlett-Packard\HPCA\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 64.

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 182 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 183 to deploy the HPCA agent to devices in your database.

HPCA Agent Notes

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

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 64.

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 KnowledgeBase 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 4 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 4 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.
⏻	**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 172 for enablement information. For more detailed information, refer to the *HP Client Automation Out of Band Management 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 141 for details.

The following tasks are available from the Devices tab.

- Importing Devices on page 57
- Deploying the HPCA Agent from the Devices Tab on page 57
- Removing the HPCA Agent on page 58
- Discovering Software/Hardware Inventory on page 58
- Discovering Patch Compliance on page 58
- Remote Control on page 59
- Power Management on page 60

- Out of Band Management on page 61
- Removing Devices on page 61
- Device Details on page 62

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 182 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 183 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 184 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.

Remote Control

Use the Remote Control interface to launch a remote session with any device. The interface allows you to connect to devices that have either RDP or VNC installed and enabled. HPCA will detect whether **Virtual Network Computing** (**VNC**) or **Remote Desktop Protocol** (**RDP**) is installed on the remote system by connecting to ports 5800 and 3389, respectively. If a connection is made on either port, HPCA will assume one of these programs 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.

  ➤ 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.

- **VNC Client** 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.

  > In order to use VNC, Sun Java Plugin for Internet Explorer must be installed. This plug-in can be downloaded from **http://java.com/en/index.jsp**.
  >
  > The VNC Server that is installed on the managed device must support the VNC Java applet running on port 5800. To verify this, open a browser to **http://hostname:5800**. If the applet is installed, the login page opens.

To launch a remote session

1. Select the device from the list, then click the **Remote Control** button to launch 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 C**lose** to exit the wizard.
6. When you are finished with the remote session, close the window to disconnect from the device.

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 172 for instructions. For more detailed information, refer to the *HP Client Automation Out of Band Management 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 141 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 via a Console login. If multiple users are logged on, only the lasto 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 121.

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.

To manually install the HPCA agent

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 Vista system with User Access 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 68) 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 57 or Deploying the HPCA Agent to a Group on page 76.

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 to HP Thin Client Devices on page 66
- HP Registration and Loading Facility on page 68

Manually Installing the Agent to HP Thin Client Devices

To manually install the HPCA agent on a Linux-based thin 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. If you are running ThinPro, you may have to create a custom connection for xterm (see note below).

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

3 Copy the installation media from the appropriate Linux thin 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 69.

To remove the HPCA agent from a Linux-based thin 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

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.

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 70.

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 is 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

RALF is shipped pre-installed on the latest HP thin client images (except those running ThinConnect). 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 `HPCARalf75.msi` file to install RALF to Windows XPE devices.

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

   ```
   msiexec /i HPCARalf75.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 5 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.

Option	Description
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 72
- Groups on page 74
- Current Jobs on page 84
- Past Jobs on page 84

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 6 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 6 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.
⏻	**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 141 for details.

The following tasks are available on the Groups tab.

- Creating a Group on page 76
- Deploying the HPCA Agent to a Group on page 76
- Removing the HPCA Agent from a Group on page 77
- Discovering Software/Hardware Inventory for a Group on page 77
- Discovering Patch Compliance for a Group on page 78
- Power Management on page 78
- Removing Groups on page 78
- Group Details on page 79
- Group Details Window Tasks on page 81
- Adding and Removing Devices from Static Groups on page 81
- Adding and Removing Software Entitlement from Groups on page 81
- Deploying, Removing, and Synchronizing Software from Groups on page 82
- Adding and Removing Patch Entitlement from Groups on page 83

- Deploying Patches to Groups on page 83

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.

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 Groups(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.

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 81
- Adding and Removing Software Entitlement from Groups on page 81
- Deploying, Removing, and Synchronizing Software from Groups on page 82
- Adding and Removing Patch Entitlement from Groups on page 83
- Deploying Patches to Groups on page 83

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 **Remove 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 Entitlement** . The Software Entitlement window opens.
3. Select the software to be entitled to the group and click **Add Entitlement**.

To remove software entitlement from a group

1. In the Group Details window, click the **Software** tab.
2. Select the software for which you want to remove entitlement, and click **Remove 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 191.

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 195.

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 Entitlement** 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 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 Entitlement** .

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** to launch the Patch Deployment Wizard.

3 Follow the steps in the wizard on page 194 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 121.

Past Jobs

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

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

Software Management

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

➤ HPCA Starter is limited to deploying only BIOS settings and HP Softpaqs. HPCA Standard is required in order to deploy software.

The Software Management tabs are:

- General on page 85
- Software on page 86
- Current Jobs on page 93
- Past Jobs on page 93

General

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

The Summary section displays how many software services are currently available in the HPCA database 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 on which you will be selecting and configuring software services. See Using the Publisher on page 213 for information about how to publish software into HPCA.

To entitle and deploy software

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

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

Software

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

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

HPCA contains the following default software services.

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

- **CCM_PUBLISHER** – HP Client Automation Administrator Publisher.

  An alternative installation method for the Publisher, use this service to deploy the Publisher to a device from which you will capture and publish software, and publish OS images, BIOS settings, and HP Softpaqs.

- **CCM_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 167 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.

Table 7 Software toolbar tasks

Button	Description
🔄	**Refresh Data** – Refreshes the Software Library.
	Export to CSV – Creates a comma-separated list that you can open, view, and save.
	Deploy Software – Launches the Software Deployment Wizard.
	Add Group Entitlement – Launches the Service Entitlement Wizard.
	Import Service – Launches the Service Import Wizard.
	Export Service – Launches the Service Export Wizard.
❌	**Delete Software** – Removes software from the library.

The following tasks are available from the Software tab.

- Deploying Software on page 88
- Adding Group Entitlement on page 88
- Importing a Service on page 89
- Exporting a Service on page 89

- Removing Software from HPCA on page 90
- Software Details on page 90

Deploying Software

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

To entitle and deploy software

1 Select the software for deployment and click **Deploy Software** to launch the Software Deployment Wizard.

2 Follow the steps in the wizard on page 191 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.

- In the Software Details window, open the Properties tab and 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.

Adding Group Entitlement

Software that is available in the Software Library can be entitled to groups of devices.

To add group entitlement

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

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

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

Importing a Service

HPCA can import software services to the Software Library. To import a service, the service import deck must be located within the `ServiceDecks` directory on your HPCA server.

(`C:\Program Files\Hewlett-Packard\HPCA\Data\ServiceDecks`, by default).

Importing a service is useful if you have created a testing environment. When you have approved a particular service in your test environment, export that service to the `ServiceDecks` directory on your production HPCA server. 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 to the Software Library.

Exporting a Service

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

To export a service

1 Select the check box in the first column to select the software to export as a service.

2 Click **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.

Removing Software from HPCA

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

To remove software from the Software Library

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

Software Details

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

General

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

Properties

Use the Properties tab to change the software details, including the software category and install/un-install command lines.

- **Description**
  Enter a detailed description of the software. 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**
  Select whether to display the software in the catalog on the managed device. Displaying software in the catalog allows the end user to install and remove the software.

- **Reboot Settings**
  Select whether to require a reboot of the managed 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 details.

Groups

The Groups tab displays all groups that have been entitled to the selected software. Use the toolbar buttons to manage group entitlements and the deployment and removal of the software to groups.

- To entitle a group, click the **Add Software Entitlement** button.
- To remove a group's entitlement, select the group and click **Remove Software Entitlement** .
- To deploy the selected software to a group, select the group and click the **Deploy Software** button.

  Follow the steps in the Software Deployment Wizard to deploy the selected software.

- To remove the software from a group, select the group and click the **Remove Software** button.

  Follow the steps in the Software Removal Wizard to remove the software from the managed devices in that group.

- To discover software and hardware inventory for a group, select the group and click the **Inventory Collections** 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, select the group 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 turn on, turn off, and reboot a group, select the group and click the **Power Management** button.

  Follow the steps in the Power Management Wizard to manage the devices.

Devices

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

- To deploy the software to a device, select the device and click the **Deploy Software** button.

  Follow the steps in the Software Deployment Wizard to deploy the software.

- To remove the software from a device, select the device and click the **Remove Software** button.

  Follow the steps in the Software Removal Wizard to remove the software.

- To discover software and hardware inventory on managed devices, select the devices and click the **Inventory Collections** button, then select **Discover Software/Hardware Inventory**.

  Follow the steps in the Software/Hardware Inventory Wizard to discover software and hardware inventory.

- To discover and enforce patch compliance for devices, select the devices and click the **Inventory Collections** button, then select **Discover & Enforce Patch Compliance**.

  Follow the steps in the Patch Compliance Discovery Wizard to discover and enforce patch compliance.

- 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' power.

Reporting

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

Current Jobs

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.

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 121.

Past Jobs

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.

Patch Management

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

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 168.

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 on page 98
- Patches on page 99
- Current Jobs on page 103
- Past Jobs on page 104

➤ HP Client Automation Standard is required for Microsoft Patch Management. With HP Client Automation Starter, you can manage HP Softpaqs.

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 following Microsoft Knowledge Base articles for more information about Automatic Updates.

- **How to configure and use Automatic Updates in Windows XP**.
- **How to configure and use Automatic Updates in Windows 2000**.

General

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 168 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

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 168 for more information.

Table 8 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.
⬆	**Import Service** – Launches the Service Import Wizard.
⬇	**Export Service** – Launches the Service Export Wizard.
✖	**Delete Software** – Removes the patch from the library. When a patch is removed, all entitlements to that patch are also removed, but the patch is not removed from the devices to which it has been deployed.

The following tasks are available on the Patches tab.

- Deploying Patches on page 100
- Adding Group Entitlement on page 100
- Importing a Service on page 100
- Exporting a Service on page 101
- Patch Details on page 101

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.

Importing a Service

HPCA can import patch services to the Patch Library. To import a service, the service import deck must be located in the `ServiceDecks` directory on the HPCA server.

(`C:\Program Files\Hewlett-Packard\HPCA\Data\ServiceDecks` by default).

Importing a service is useful if you have created a testing environment. After a service has been approved in your test environment, use the Service Export Wizard to export it to the `ServiceDecks` directory on the production HPCA server. Then use the Service Import Wizard to import the service to the production Patch Library and deploy the patch to managed devices.

To import a service

1. Click the **Import Service** button to launch the Service Import Wizard.
2. Follow the steps in the wizard to import the service to the Patch Library.

Exporting a Service

Published patch services can be exported to the `ServiceDecks` directory on an HPCA server. Exported services are available for import to any other HPCA Patch library (within a testing environment, for example).

To export a service

1. Use the check boxes in the first column to select a patch to export as a service.
2. Click the **Export Service** button to launch the Service Export Wizard
3. Follow the steps in the wizard to export the service to the `ServiceDecks` directory on an HPCA server.

Patch Details

Click any patch description to open the Patch Details window. Use the Patch Details window to view patch service properties, view and modify entitlements, 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.

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** .
- To remove entitlement from a group, select the group and click the **Remove Group Entitlement** button.
- To deploy the patch to a group, select the group and click **Deploy Patches** .

  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** 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** button, then select **Discover Patch Compliance**.

  Follow the steps in the Patch Compliance Discovery Wizard to discover patch compliance.
- To turn on, turn off, and reboot a group of devices, select the group and click the **Power Management** 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** 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 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

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 121.

Past Jobs

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

The following sections describe each OS Management tab:

- General on page 105
- Operating Systems on page 106
- Current Jobs on page 120
- Past Jobs on page 120

➤ HP Client Automation Starter allows Thin Client operating system management only. For expanded OS management, HP Client Automation Standard is required.

General

Use the General tab to find information about how to publish operating systems, entitle and deploy operating systems to managed devices, and view current and past OS Management jobs.

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

To capture and publish OS images

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

- Use the Image Preparation Wizard to prepare and capture OS images. See Chapter 9, Preparing and Capturing OS Images or the Image Preparation Wizard online help for image preparation and capture details.
- Use the Publisher to publish operating system images to HPCA. Published operating system services are displayed in the Operating System tab. See Using the Publisher on page 213 or the Publisher online help for information about publishing operating systems.

To deploy OS images

1. In the Common Tasks area, click **Deploy.** This launches the OS Deployment Wizard.
2. Follow the steps in the wizard to entitle and deploy an operating system to managed devices.

For additional information about deploying operating systems, including requirements for target devices and deployment scenarios, see Deploying Operating Systems on page 107.

Operating Systems

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

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

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

Table 9 OS Library toolbar tasks

Button	Description
⟳	**Refresh Data** – Refreshes the OS Library.
▦	**Export to CSV** – Creates a comma-separated list that you can open, view, and save.
◔	**Deploy Operating System** – Launches the OS Deployment Wizard.
✚	**Add Group Entitlement** – Launches the Service Entitlement Wizard.

Table 9 OS Library toolbar tasks

Button	Description
	Import Service – Launches the Service Import Wizard.
	Export Service – Launches the Service Export Wizard.
✖	**Delete Operating System** – Removes operating systems from the library.

The following tasks are available from the Operating System tab:

- Deploying Operating Systems on page 107
- Deploying an OS Image using Local Service Boot (LSB) on page 111
- Deploying an OS Image using PXE on page 112
- Deploying an OS Image using the Service CD on page 113
- Adding Group Entitlement on page 114
- Importing a Service on page 114
- Exporting a Service on page 115
- Removing Operating Systems from the Library on page 115
- Restoring Operating Systems on page 115
- OS Details on page 118

Deploying Operating Systems

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 175 to select the deployment mode.

See the sections 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 10 Deployment Scenarios

Device State	**Instructions for deployment**
Managed (agent installed)	If the device is already managed: • Add the device to a group. • Entitle an operating system to the group (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 10 **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 entitlement 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. • A device is added to HPCA using a variation on the MAC address as device name. • Add the new device to a group with OS entitlement. 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. • The device is rebooted and the Service CD or PXE will continue with the OS deployment. Note: LSB cannot be used for deploying an OS to a bare-metal device.

Requirements for Target Devices

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

- Must meet the minimum hardware and BIOS requirements published by Microsoft (for Windows operating systems) or the machine manufacturer for running the OS to be deployed by HPCA.
- Target devices must be able to contact a DHCP server and obtain an IP address.
- If you want to report on, or make use of the machine's make, manufacturer, and unique identifier for policy, the BIOS must support SMBIOS (for systems management) specification. If a target device lacks SMBIOS support, the only criterion available for specifying policy on that machine will be the MAC address.
- Have an English, French, or German keyboard.

- Have 128 MB of RAM or more.
- If you are using a network (PXE) boot, you must:
  - Be able to boot from the Boot Server. To do this, make sure that the BIOS is set to boot from the network before the hard drive.
  - Have a **Network Interface Card** (**NIC**) that supports PXE. Some network cards are PXE-capable, but only actually support PXE with the addition of a network boot ROM. These cards must have the network boot ROM installed. Some older 3Com cards require a firmware upgrade to MBA 4.3 and PXE stack version 2.2.
  - Be sure that the target devices have the same or a compatible **Hardware Abstraction Layer** (**HAL**) as the reference machine in order to use Microsoft Sysprep. Machines with the same version of `HAL.DLL` share the same Hardware Abstraction Layer. For more information on determining a machine's HAL, refer to the Microsoft Knowledge Base article, **How to Troubleshoot Windows 2000 Hardware Abstraction Layer Issues**.

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

- Embedded Linux images can be deployed only to target machines with flash drives of equal size. For example, an image that is 256 MB can be deployed only to target devices that have a flash drive of 256 MB.

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

1 HDD with 2 partitions:

- The boot partition is re-imaged; the second partition remains intact.

1 HDD with 1 partition:

- The hard drive is re-imaged; all existing data is overwritten.

2 HDDs with 1 partition each:

- The first hard drive is re-imaged; all existing data on first hard drive is overwritten. Second hard drive remains intact.

2 HDDs with 2 partitions each:

- The first hard drive boot partition is re-imaged; the second partition and second hard drive remain intact.

Deploying thin client factory images

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

- After the image is deployed to the device, you must install the HPCA agent to begin to manage the device. See Installing the HPCA Agent on HP Thin Clients on page 65 for installation instructions.

Deploying an OS Image using Local Service Boot (LSB)

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

When using Local Service Boot, existing machines do not need to be PXE-enabled and the boot order does not need to be configured locally in the BIOS for each target device.

See Deployment Scenarios on page 108 for prerequisite instructions for OS deployment.

To deploy an OS image using Local Service Boot

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

Deploying an OS Image using PXE

The PXE-based environment allows HPCA to assume management of the OS on target devices that are booted from the network. See Deployment Scenarios on page 108 for prerequisite instructions for OS deployment.

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

- A DHCP server and TFTP server must be configured prior to using PXE for OS deployment. Refer to the product documentation for configuration instructions.

When PXE is configured, make sure your target devices boot from the network or have PXE-enabled as the primary boot device. Make the necessary configuration adjustments to ensure this will happen (for example, with some BIOS versions, you can 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 you defined on your DHCP server.

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

Deploying an OS Image using the Service CD

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

Use `ImageDeploy.iso` to create the Service CD. This file is located on the 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 108 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 hostname and port number, then press **Enter** to continue. For example, `HPCA.acmecorp.com:3466` or `192.168.1.100:3469`. Port 3466 is reserved for OS imaging and deployment.

   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.

Adding Group Entitlement

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

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.

Importing a Service

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

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

To import a service

1. Click the **Import Service** button to launch the Service Import Wizard.
2. Follow the steps in the wizard to import the service to the OS Library.

Exporting a Service

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

To export a service

1. Select the check box in the first column to select the OS image to export as a service.
2. Click the **Export Service** button 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.

Removing Operating Systems from the Library

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

To remove an operating system service from the Operating System Library

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

Restoring Operating Systems

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

Prerequisites

- The ImageDeploy media.
- A working operating system stored on the network.

To recover your operating system

1 Insert the CD-ROM that you created from the `ImageDeploy.iso` in the `\Media\iso\roms` folder on the product HPCA media.

2 Boot the target device.

3 When asked which Service OS to use, select **_SVC_LINUX_** or **SVC_PEX86_**.

4 You will see several messages and then a menu opens with the following choices:

   1. Service OS networking (default selection if no option is chosen)

   2. Install OS from cache partition (Enterprise license only)

   3. Install OS from CD or DVD (Enterprise license only)

5 Type the number corresponding to the action you want. Options 2 and 3 require an Enterprise license. For Service OS networking, you must be connected to a network.

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

   or

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

   — IP address for the target device

   — Default gateway

   — Subnet

   — Subnet mask

   — DNS address

   — OS Manager Server IP address

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

— `romsinfo.ini`

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

  In the sample `romsinfo.ini` file below:

```
[ROMSInfo]

192.128.1.99=192.168.123.*,
192.168.124.*,192.128.125.*

osm.usa.hp.com=192.168.*

osm.hp.com=*
```

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

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

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

```
[ServiceCD]

source=net

netif=eth0
```

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

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

- `netinfo.ini`

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

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

  ```
  [SubnetDisplayname1]

  addr=192.168.123.50-192.168.123.69

  gateway=192.168.123.254

  subnet=192.168.1.0

  netmask=255.255.255.0

  dns=192.168.123.1
  ```

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

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

OS Details

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

General

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

Properties

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

- **Description**

The description displayed for the operating system service. This field is required.

- **Author**

  Optional field for OS service author.

- **Vendor**

  Optional field for the OS vendor.

- **Web Site**

  Optional field for a URL related to this service.

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

Groups

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

- To **entitle** additional groups, click the **Add Group Entitlement** button.
- To **remove entitlement** from a group, select the group then click the **Remove Group Entitlement** button.
- To **deploy** the operating system to a specific group, select the group and click the **Deploy Operating System** button. This launches the OS Deployment Wizard. Follow the steps in the wizard on page 196 to deploy the selected OS.

Devices

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

- To **deploy** the operating system to a specific device, select the device and click the **Deploy Operating System** button. This launches the OS Deployment Wizard. Follow the steps in the wizard on page 196 to deploy the selected OS.

Reporting

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

Current Jobs

Current Jobs shows all currently active or scheduled OS Management jobs. OS Management jobs are used to entitle and deploy operating systems services from managed devices in your 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 121.

Past Jobs

Past Jobs shows all completed OS Management jobs.

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

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

Job Management

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

The Job Management tabs are described in the following sections:

- General on page 121
- Current Jobs on page 121
- Past Jobs on page 125

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 on page 121
- Job Status on page 122
- Job Details on page 124

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 11 Job controls

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.

Table 11 Job controls

Icon	Description
⏹	**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 12 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 13 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 13 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 14, 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.

5 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 the Reporting tab in the HPCA Console, there are links to the following collections of reports:

- Inventory Management reports
- Patch Management reports

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:

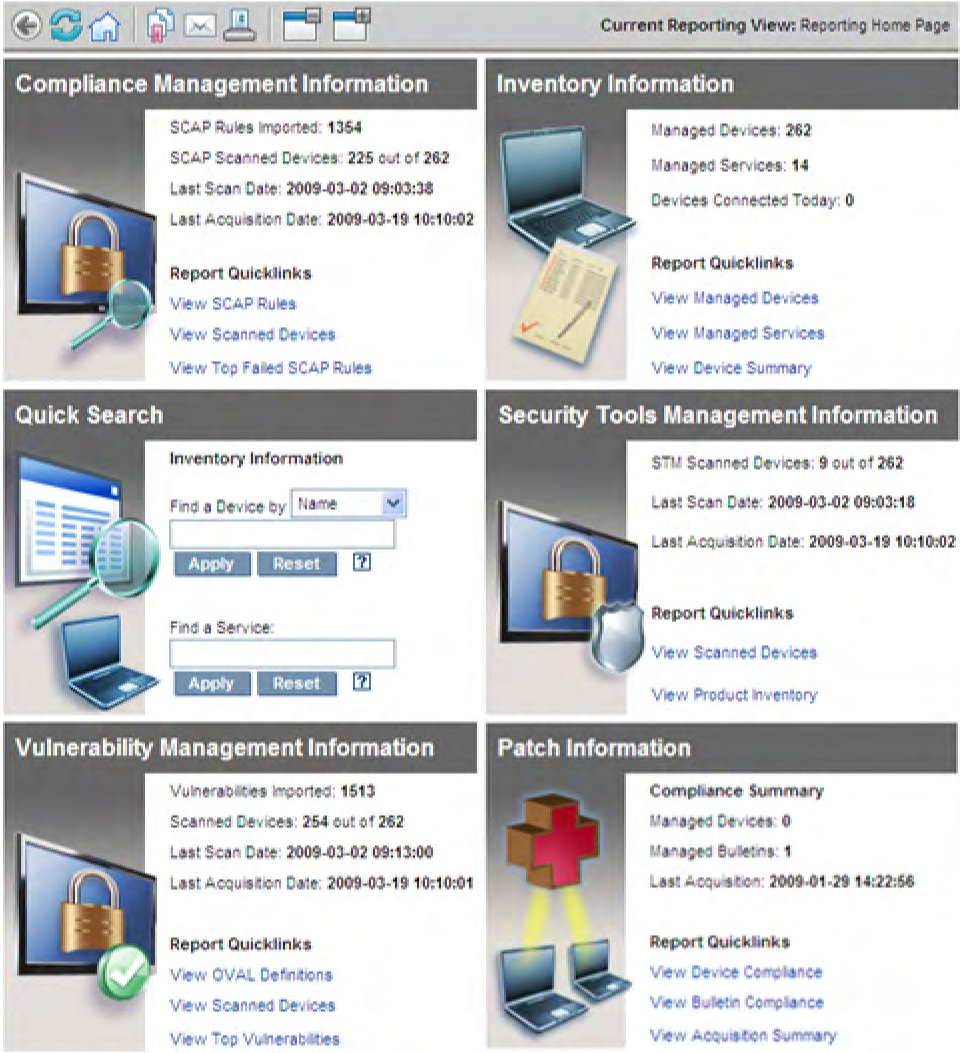
Report Pack	Report Type	Description
rpm.kit	Patch Management	Devices in and out of compliance with patch policy
rim.kit	Inventory	Devices currently managed by HPCA

➤ 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. As shown here, the home page provides a snapshot of the enterprise with respect toinventory management, patch management (if installed and enabled).



Current Reporting View: Reporting Home Page

Compliance Management Information

SCAP Rules Imported: 1354

SCAP Scanned Devices: 225 out of 262

Last Scan Date: 2009-03-02 09:03:38

Last Acquisition Date: 2009-03-19 10:10:02

Report Quicklinks

View SCAP Rules

View Scanned Devices

View Top Failed SCAP Rules

Inventory Information

Managed Devices: 262

Managed Services: 14

Devices Connected Today: 0

Report Quicklinks

View Managed Devices

View Managed Services

View Device Summary

Quick Search

Inventory Information

Find a Device by: Name

Find a Service:

Security Tools Management Information

STM Scanned Devices: 9 out of 262

Last Scan Date: 2009-03-02 09:03:18

Last Acquisition Date: 2009-03-19 10:10:02

Report Quicklinks

View Scanned Devices

View Product Inventory

Vulnerability Management Information

Vulnerabilities Imported: 1513

Scanned Devices: 254 out of 262

Last Scan Date: 2009-03-02 09:13:00

Last Acquisition Date: 2009-03-19 10:10:01

Report Quicklinks

View OVAL Definitions

View Scanned Devices

View Top Vulnerabilities

Patch Information

Compliance Summary

Managed Devices: 0

Managed Bulletins: 1

Last Acquisition: 2009-01-29 14:22:56

Report Quicklinks

View Device Compliance

View Bulletin Compliance

View Acquisition Summary

There are three ways to find more detailed information on the Reporting home page:

- Use 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 14 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.
✉	Email a link to this report.
?	Open a “quick help” box or tool tip. This applies only to filters.
🖶	Print this report.

Table 14 Report Actions

Icon	Description
⊟	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:

- Inventory Management Reports on page 132
- Patch Management Reports on page 133

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, detailed and summary device components, blade servers, TPM Chipset and SMBIOS information, and Self-Monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) Alerts.

Expand the Inventory Management Reports reporting view to see the report options. Note that certain data, like S.M.A.R.T. Alerts and HP Specific Reports, are only available after HPCA components are configured. Refer to Device Management on page 165 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 he device.
- **OS Level –** current operating system level (Service Pack 2, for example).

HP Hardware Reports

HP Hardware reports are a subset of the Inventory Reports that contain simple alert information captured by the HP Client Management Interface (CMI) on compatible, HP devices.

HP Hardware reports are located in the Hardware Reports view under Inventory Management Reports.

To search for a specific alert type or BIOS setting (based on the report view that you chose), use the additional data filter search box displayed at the top of the report window.

Patch Management Reports

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

- **Executive Summary Reports** – 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.
- **Compliance Reports** – 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.
- **Patch Acquisition Reports** – Acquisition-based reports show the success and failures of the patch acquisition process from the vendor's web site.
- **Research Reports** – Research-based reports display information about the patches acquired from the software vendor's web site. Research-based reports offer a Filter bar.

For details on using the Patch Management reports, refer to Patch Management on page 95.

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, Compliance Management filters apply only to Compliance 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.

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:

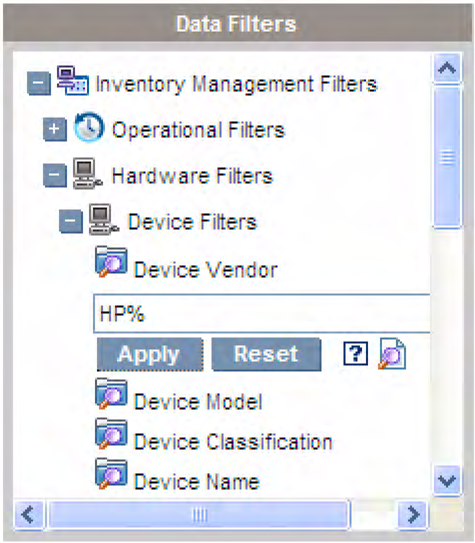
3 Specify the filter criteria in the text box, or click the (criteria) button to select the criteria from a list (if available—not all filters have lists).

You can use wildcard characters when creating filters. The following table describes the characters you can use to build search strings.

Table 15 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.



Data Filters

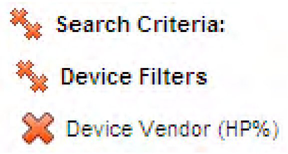
- Inventory Management Filters
  - Operational Filters
  - Hardware Filters
    - Device Filters
      - Device Vendor

        HP%

        Apply   Reset
      - Device Model
      - Device Classification
      - Device Name

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:



Search Criteria:

Device Filters

Device Vendor (HP%)

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 134 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.

6 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 on page 140
- Out of Band Management on page 141
- Patch Management on page 145

Infrastructure Management

Infrastructure Management operations are described in the following sections:

- Support on page 140
- Database Maintenance on page 141

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 140, 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.

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 are removed for a device, that data are no longer available when generating any reports.

➤ If you are deleting reporting data for an actively managed device, to avoid reporting data discrepancies, you should remove then re-deploy the Management Agent on that device.

Out of Band Management

Out of Band (OOB) Management is enabled using the Configuration tab. See Configuration on page 147 for OOB Management settings and Preferences.

For additional information on using OOB Management refer to the *HPCA Out of Band Management User Guide*.

The following sections describe the OOB Management tasks available in the console:

- Provisioning and Configuration Information on page 142
- Device Management on page 143
- Group Management on page 144

- Alert Notifications on page 145

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 Provisioning vPro Devices chapter of the *HPCA 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 Provisioning vPro Devices chapter of the *HPCA Out of Band Management User Guide* for complete details.

DASH Configuration Documentation

It is assumed that you have already provisioned DASH-enabled devices according to the documentation accompanying the device. DASH configuration information is documented in the "Broadcom NetXtreme Gigabit Ethernet Plus NIC" whitepaper. This can be found in the "Manuals (guides, supplements, addendums, etc)" section for each product that supports this NIC.

➤ This information pertains to DASH-enabled devices from Hewlett-Packard only.

To access this documentation

1 Go to www.hp.com.

2 Select Support and Drivers > See support and troubleshooting information.

3 Enter a product that supports this NIC, for example, the dc5850.

4 Select one of the dc5850 models.

5 Choose Manuals (guides, supplements, addendums, etc).

6. Choose the "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 > Download 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 NetXtreme Gigabit Ethernet Plus NIC driver.

Device Management

The Device Management area allows you to manage multiple and individual OOB devices.

On the Operations tab, under Out of Band Management, click Device Management. The Device Management window opens. From 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 *HPCA Out of Band Management User Guide* for complete details.

Group Management

The Group 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 *HPCA 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 Notification chapter of the *HPCA Out of Band Management User Guide* for complete details.

Patch Management

Patch Management Operations tasks are described in the following sections:

- Perform Synchronization on page 145
- View Acquisition History on page 146

Perform Synchronization

This operation synchronizes the patch information stored in the Patch Libary 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**.

View Acquisition History

Select a patch acquisition status page to view details from previous acquisitions.

7 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

- Licensing on page 147
- Core Console Access Control on page 148
- Infrastructure Management on page 152
- Device Management on page 165
- Patch Management on page 168
- Out of Band Management on page 172
- OS Management on page 175
- Dashboards on page 177

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**.

Access Control

This panel offers different administrative controls depending on whether you are in the Core or Satellite Console.

> ➤ HPCA Starter and Standard license editions do not offer a Satellite Console.

- Access Control on the Core Console allows HPCA administrators to configure and manage user access to the Console. See Core Console Access Control on page 148.

Core Console Access Control

Use the Access Control section to create instances of Console **users** (see Users Panel on page 149) with unique, custom IDs and passwords. Then, assign **roles** (see Roles Panel on page 151) to the users in order to manage the areas of that Console that they 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 will determine which areas of the Console each user can access. Users can also be deleted, and their roles modified.

> Management jobs contain a Creator field that displays the user ID under which the job was used created. It is the user IDs that are created in this area that will be displayed.

- By default, after installation, one default Console user, **`admin`**, exists with the default password of **`secret`**. This “failsafe” user account has full access to the Console and cannot be deleted.
- HPCA Console users can be either **internal** or **external**, as described below.
  - **Internal Users**
    All users that are created at the Users panel are created as “internal.” These users can be deleted and updated via the Core Console.
  - **External Users**
    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. These “external” users cannot be created, deleted, or updated at 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. That source will then appear in the Users panel and the Source column will reference the directory from which the user originated.
- The currently active user cannot be deleted. If you want to delete the currently active user, you must log out and log in as a different user. Then you will have the ability to remove the previously active user.

The following sections detail the administrative tasks that are available at the Users panel.

To create a Console user

1 Click the **Create New User** button to launch the User Creation Wizard .

2 Follow the steps in the wizard to add Console users.

User ID Considerations

User IDs cannot include spaces, slashes (/), or backslashes (\).

- If a space or backslash is included, an “unable to create” error message will result.
- If a slash is included, it will be automatically removed when the user ID is generated. For example, user ID **`jdoe/1`** would result in user ID `jdoe1`.

Password Considerations

- Use only ASCII characters when creating passwords.
- If you change the password for the *current user*, you will be automatically logged out. Log in as the user, but with the new password.

3 After creating a user, you can:

— Create another user (return to step 1 of this section).

— Click a user ID to view and change the user’s properties (as described in the next section).

— Assign a role to a user (as described in the section, Roles Panel on page 151).

To view and modify user properties

The steps in this section are specific to “internal” users; the properties of “external” users cannot be modified on the Core Console.

1 Click an internal user’s User 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.

4 You can now:

— Create another user (see step 1 in the previous section).

— Click a different user ID to view and change its properties (return to step 1 of this section).

— Assign a role to a user (as described in the section, Roles Panel on page 151).

To remove a Console user

The steps in this section are specific to “internal” users; the properties of “external” users cannot be modified on the Core Console.

- Select the user IDs from the list and click **Delete Users** ✖.

> The *current user* cannot be deleted.
>
> In order to delete this user 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 Console user roles 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’ permissions are restricted to viewing, compiling, and printing reporting data in the Core Console. Their access is limited to the Reporting and Dashboards tabs.

> More than one role can be assigned to a user.

Assigning Roles to Users

Roles can be assigned to users in either of two ways in the Console.

- In the Roles panel:

  a Click a role in the table to invoke the Role Properties window; this displays a list of the users that have been assigned that role.

  b Use the toolbar buttons to add/delete users to/from the role.

- In the Users panel:
  a. Click a user ID in the table to invoke the User Properties window.
  b. Click the Roles tab.
  c. Use the toolbar buttons to add/delete users to/from the role.

Infrastructure Management

The Infrastructure Management section allows you to configure various settings of your HPCA infrastructure. See the following sections for details.

- Proxy Settings on page 152
- SSL on page 153
- Database Settings on page 154
- Sites and Services on page 155

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.

6 Click **Close** to acknowledge the dialog.

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 153
- SSL Client on page 154

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 Select the check box after **Enable SSL**.

2 Select whether to **Use existing certificates** or **Upload new certificates**.

3 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. Click **Browse** to navigate to and select the CA Certificates file.
2. Select whether to append this certificates file to existing certificates, or to replace the existing certificate with this new file.
3. 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 intructions 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.
   - **ODBC DSN**: Select the DSN for the Core database.
   - **ODBC User ID**: Specify the user ID for the DSN.
   - **ODBC 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**.

Sites and Services

Implementing Infrastructure Servers allows you to optimize bandwidth and increase network performance by providing data caching services for managed devices. Infrastructure Servers can be deployed and managed using the Infrastructure Management, Sites and Services area of the Configuration tab.

To implement Infrastructure Servers:

1. Add devices to the Infrastructure Servers list.

   See To add an Infrastructure Server on page 158.

2. Deploy the Infrastructure Server Service.

   See To deploy the Infrastructure Service on page 158.

3. Create and assign Locations.

   See To create a New Location on page 163 and To assign a Location on page 164

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

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

- Servers on page 156
- Locations on page 162

Servers

Define Infrastructure Servers by adding devices to the Infrastructure Server group then by deploying the Infrastructure service. When you are finished adding servers, you will need to assign Infrastructure Locations for each server. See Locations on page 162 for additional information.

Infrastructure Servers automatically cache all requested data with the exception of operating system images. They can also be pre-populated with all data on the HPCA server using the synchronize feature. See Synchronizing Infrastructure Servers on page 159 for details.

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

Table 16 Infrastructure Servers toolbar buttons

Toolbar Button	Description
🔄	**Refresh Data** – Refresh the list data.
⬇	**Export to CSV** – creates a comma-separated list that you can open or save.
➕	**Add Infrastructure Server(s)** – Add devices to the Infrastructure Servers group.
➖	**Remove Infrastructure Server (s)** – Remove devices from the Infrastructure Servers group.
➜	**Deploy the Infrastructure Service** – Launches the Infrastructure Deployment Wizard.

Table 16 Infrastructure Servers toolbar buttons

Toolbar Button	Description
	Remove the Infrastructure Service – Launches the Infrastructure Removal Wizard.
	Synchronize the selected Infrastructure Servers service cache – Synchronizes the selected server's service cache with the HPCA Server.
✖	**Delete Device(s)** – Delete devices.

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

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

Managing Infrastructure Servers

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

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

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

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

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

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

To add an Infrastructure Server

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

Devices added appear in the Infrastructure Servers list.

To remove an Infrastructure Server

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

   The device is removed from the group.

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

When devices are added, you can begin deploying the Infrastructure service. This service is required to begin remote data caching on each server.

To deploy the Infrastructure Service

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

1. Select devices from the Infrastructure Servers list using the check boxes in the left column.
2. Click **Deploy the Infrastructure Service** toolbar button to launch the Infrastructure Deployment Wizard.
3. Follow the steps in the wizard to deploy the Infrastructure Service to the selected devices. The Infrastructure Service is installed to:

   ```
   System Drive:\Program Files\Hewlett-Packard\HPCA\ProxyServer
   ```

Each time devices request resources not available on theInfrastructure Server's local cache, the data is retrieved from the HPCA server, stored in the dynamic cache of the Infrastructure Server, and provided to the client devices. Services can be pre-loaded to Infrastructure Servers using the Synchronize feature. See Synchronizing Infrastructure Servers on page 159 for details.

To remove the Infrastructure Service

1. Select devices from the Infrastructure Servers list using the check boxes in the left column.
2. Click **Remove the Infrastructure Service** toolbar button to launch the Infrastructure Removal Wizard.
3. Follow the steps in the wizard to remove the Infrastructure Service from selected devices.

After you have created Infrastructure Servers, you need to define Locations to then assign those servers to specific subnets.

Synchronizing Infrastructure Servers

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

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

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

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

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

To select which data to preload

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

To synchronize Infrastructure Servers

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

1. To synchronize one or more servers, use the Infrastructure Servers list and select all of the servers for synchronization. Click the **Synchronize the selected Infrastructure Servers service cache** toolbar button to update all selected server's with the latest data from the HPCA Server. The services pre-loaded to each server depend on the settings configured in each server's Server Details window **Cache** tab.

   or

2 To synchronize a single server, select the server and use the toolbar button, or click the Server name to open the Server Details window and click **Synchronize** in the **Common Tasks** area. You can also use the Cache tab to determine which services to pre-load, and then click **Synchronize.**

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

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

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

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

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

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

Server Details Window

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

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

General
From the General tab you can view information about the server in the Common Tasks section and complete tasks like deploying the Infrastructure service and Synchronizing Infrastructure Servers service cache.

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

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

Cache
The Cache tab allows you to select the types of services stored in the Infrastructure Server's service cache. See Synchronizing Infrastructure Servers on page 159 for additional details.

Locations
The Locations tab defines which subnets are assigned to the server. For details on adding and assigning subnets see Locations on page 162.

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

Reporting
Use the Reporting tab to view the pre-load summary for services. Only pre-loaded services are displayed. Services cached automatically (after a device request) are not displayed. For details on each pre-load status, see Synchronizing Infrastructure Servers on page 159.

Locations

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

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

Table 17 Infrastructure Servers toolbar buttons

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

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

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

To create a New Location

1 Click **Create a New Location** 🏢 toolbar button to launch the Infrastructure Location Creation Wizard.

2 Follow the steps in the wizard to create a new Infrastructure Location.

To create new Locations based on Inventory Data

1 Click **Auto-create locations based on Inventory Data** 🏢.

2 Click **OK**.

3 Click **Close**.

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

After a Location is added, assign servers.

To assign a Location

1 Click the **Servers** tab.

2 Click the server to which you want to assign a Location. The Server Details window opens.

3 Click the **Locations** tab.

4 Click **Add Locations** toolbar button. The Server Locations window opens.

5 Select the Locations to assign to the Infrastructure Server and click **Add Locations.**

6 Click **Close**. If you are finished adding Locations, click **Close** again to close the Server Details window.

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

You can remove any Locations assigned to a server using the **Remove Locations** toolbar button.

To remove Locations from a server

1 Click the **Servers** tab.

2 Click the server for which you want to remove a Location. The Server Details window opens.

3 Click the **Locations** tab.

4 Select the Locations to remove from and click the **Remove Locations** toolbar button.

5 Click **Close**. If you are finished removing Locations, click **Close** again to close the Server Details window.

Location Details

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

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

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 165
- Trusted Platform Module on page 167

Alerting

Use the Alerting section to configure CMI and S.M.A.R.T. alerts and reporting options.

- CMI on page 165
- S.M.A.R.T. on page 166

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).

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 Deploying Software on page 88 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 **Hardware Management**.
2. Click the **TPM** tab.
3. Type the BIOS Admin and TPM Owner passwords.
4. Type the Emergency Recovery and Password Reset Tokens.
5. Select the Reboot Settings. After the TPM chip is enabled, the device is rebooted. This setting determines the level of interaction the end user will have.
   - **Accept Only** – After reboot, user must accept enablement
   - **Accept or Reject** – After reboot, user can accept or reject enablement
   - **Silent** – User is not prompted to confirm enablement after reboot
6. Type the file paths for Backup Archive, Emergency Recovery Archive, and TPM Password Reset Archives.
7. Click **Save**.

Patch Management

Use the Patch Management section to enable patch management and define ODBC parameters for your patch database. Starter and Standard users can also use this section to acquire patches and HP Softpaqs, configure schedules for patch acquisition, and to define patch acquisition settings.

Refer to Patch Deployment Wizard on page 194 for details on how to deploy and entitile patches in your environment.

Patch Management options are explained in the following:

- Database Settings on page 169

- Acquisition Jobs on page 169

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 *HPCA Core and Satellite Servers Getting Started and Concepts Guide*.

To enable and configure Patch

1. Select **Enable** (this will start the `HPCA Patch Manager` service).
2. 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.
3. Click **Save**.
4. If you modified Patch ODBC Settings, follow the prompts to restart the Patch Manager Service.

Acquisition Jobs

Use the Acquisition Jobs section to configure patch acquisition schedules and settings.

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

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

Current Schedule shows the currently configured patch acquisition schedule.

To acquire patches

- Click **Acquire Patches Now** to acquire patches based on the current Patch Acquisition settings. Patches are downloaded and stored in the Patch Library.
- View acquired patches in the Patch Management, Patches tab.

To configure the patch acquisition schedule

1 Use the tools provided to set the acquisition schedule.

  — **Run**: Select whether to discover patches based on an interval hours, days, or weeks.

  — **Interval**: Select the specific interval (hours, days, or weeks).

  — **Starting on**: Use the drop-down lists to select the date patch compliance should be discovered.

  — **Current Server Time** displays the current time of the 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 (*).

To configure patch acquisition settings

1 Complete the **Microsoft Bulletins** area.

  — In the **Enabled** drop-down list, select **Yes** to acquire Microsoft Bulletins.

- In the **Bulletins to Acquire** text box, type the Bulletins to download for each discovery period. Use wildcard characters to designate a range of bulletins (for example, MS05*). Separate multiple bulletin searches with a comma (for example, MS05*, MS06*).
- In the **Languages to Acquire** text box, type the language codes for each language version available for the patches you want to download. Use the following table to find the appropriate language codes. Separate multiple language codes with a comma and no space (for example: en,fr,ja). Codes are case-sensitive.

Table 18 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	

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 the the **Operations** tab, **Patch Management** area, **View Acquisition Jobs** page.

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 172
- Device Type Selection on page 173
- vPro System Defense Settings on page 174

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.

See the Operations tab, Out of Band Management section to view the OOB Management options.

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 173
- vPro Devices on page 173
- Both on page 174

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 174.

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 *HPCA 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 19 Confifguration 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 Opertions 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 mal-ware 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 *HPCA 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 Operating System service functions.

- Settings on page 176
- Deployment on page 176

Settings

The Operating Systems service allows Agents to connect to the HPCA server and retrieve their OS entitlements and provisioning information. When this service is disabled on a Core, this information will not be available for Satellites or Agents requesting this information.

- To enable Operating Systems service, select the check box and click **Save**.

During OS deployment, if you are planning to 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 check box and click **Save**.

Deployment

Use the OS Management section to configure settings for operating system deployment.

To configure the OS Deployment mode

1. In the Configuration tab, OS Management section, select the OS Deployment Mode:
   - **Prompt User (Attended) —** A user must be present at the managed device during operating system deployment to continue the deployment process.
   - **Do not prompt user (Unattended) —** No dialogue windows are displayed on managed devices during operating system deployment. No user interaction is required.

   ⚠ Deploying an operating system image will in some cases overwrite existing data depending on the number of hard drives and partitions on the target device. If you select **Do not prompt user (Unattended)**, be sure to back up existing data on target devices before deploying a new operating system.

2 Click **Save** to commit your changes.

➤ Changes to the OS Deployment Mode affects all new and scheduled OS deployment jobs.

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 35

Service Events on page 36

The Executive View also includes the following pane:

12 Month Service Events by Domain on page 38

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 34.

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 40
- Device Compliance by Bulletin on page 42

The Operational View includes three information panes:

- Device Compliance by Status (Operational View) on page 44
- Microsoft Security Bulletins on page 45
- Most Vulnerable Products on page 46

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 40.

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 Microsoft Security Bulletins (Operational View) pane requires additional information. Specify the URL for the Microsoft Security Bulletins RSS feed (a currently 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.

8 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.

- Infrastructure Location Creation Wizard on page 199

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 183.

To import devices using the Import Device wizard

1 To launch the wizard, click **Import** on the General tab in the Device Management section or click the **Import Devices to Manage** toolbar button on the Devices tab.

2 Select the Device Source from the drop-down list.

— **Manual Import** – Type or paste a list of device host names or IP addresses into the text box provided.

— **LDAP/Active Directory** – To import devices automatically from Active Directory or another LDAP-compliant Directory Service, type the LDAP Host, Port, User ID, password (if required) and the DN to Query.
Also select the scope, an advanced filter, or a device limit to apply to the query.

— **Domain** – To scan a network domain for devices to import, type the domain name (for example, type ABC for a full domain scan of the ABC domain) or part of the domain name and a wildcard character (ABC* returns all devices from domains beginning with ABC). To include specific devices from a domain, use the following syntax, domain\device. For example, `Sales\WS*` returns only devices beginning with `WS` from the `Sales` domain.
Use an exclamation mark ! to exclude specific devices from a domain. For example, `Sales,!Sales\WS*` will return all devices from the Sales domain with the exception of devices beginning with `WS`.

3 Click **Import**.

4 Click **Close** to exit the wizard.

Imported devices are displayed in the Devices tab.

Agent Deployment Wizard

Use the Agent Deployment wizard to deploy the Management Agent to devices in your HPCAS database.

➤ Prior to deploying the Management Agent to a device, review the Firewall Settings rules for 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 exit the wizard.

Agent Removal Wizard

Use the Agent Removal Wizard to remove the Management Agent from devices in your HPCAS database.

> Removing the Management Agent will disable the ability to deploy software and patches and to collect updated inventory information for that device. Unmanaged devices will remain within their respective groups until removed from the groups or deleted from HPCAS and will retain all deployed software.

To remove a Management Agent using the Agent Removal wizard

1. Launch the wizard from the Device Management, Devices tab or from the Group Management, Groups tab.
2. Select the devices or groups from which you want to remove the Management Agent and click the **Remove the Management Agent** toolbar button.
3. Click **Next** to begin the wizard.
4. Select **Run: Now** to remove the agent immediately after the wizard is complete, or select **Run: Later** and enter a date and time for Agent removal.
5. Click **Next**.

6 Review the summary information and click **Submit**. An Agent Deployment Job is created.

7 Click **Close** to exit the wizard.

Software/Hardware Inventory Wizard

Use the Software/Hardware Inventory Wizard to create inventory audit jobs that will discover software and hardware inventory for the selected devices.

To discover inventory using the Software/Hardware Inventory wizard

1 Launch the wizard from the Device Management, Devices tab or from the Group Management, Groups tab.

- Click the **Inventory Collections** toolbar button, then select **Discover Software/Hardware Inventory.**

2 Select **Run: Now** to discover inventory immediately after the wizard is complete, or select **Run: Later** and enter a date and time for inventory discovery. To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks** then select the **Interval** from the drop-down list.

> ➤ Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

3 Select 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.

To discover patch compliance

1 Launch the wizard from the Device Management, Devices tab or from the Group Management, Groups tab.

— Click the **Inventory Collections** toolbar button then select **Discover Patch Compliance**.

2 Select **Run: Now** to schedule the job to run immediately after the wizard is complete, or select **Run: Later** and enter a date and time for the job to begin. To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks**, then select the **Interval** from the drop-down list.

> Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

3 Select whether 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.

To remotely turn on, turn off, or restart a device

1. Launch the wizard from the Device Management, Devices tab or from the Group Management, Groups tab by clicking the **Power Management** ⏻ toolbar button.
2. Select the Power Management function from the drop-down list. You can choose to turn on, turn off, or restart the selected device.
   - **Power On** – turn on the selected device
   - **Power Off** – turn off the selected device
   - **Reboot** – restart the selected device
3. Configure the run schedule for the job. Select **Run: Now** to schedule the job to run immediately, or select **Run: Later** to schedule a date and time for the job to begin. To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks** then select the **Interval** from the drop-down list.

   ➤ Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

4 Review the summary information and click **Submit**.

5 The job is successfully created. Click **Close** to exit the wizard.

Use the Current Jobs tab to view all pending Management Jobs.

Group Creation Wizard

Software or patches must be deployed to groups of managed devices in your database. Use the Group Creation Wizard to define device groups based on devices you specify, discovered devices, or on the devices returned as part of a reporting query.

The Group Creation Wizard steps vary depending on the type of group you are creating.

To create a static group

1 Do one of the following to launch the wizard

— From Group Management, General tab click **Create a new Static Group**.

— From the Groups tab click the **Create a New Static Group** toolbar button .

2 Click **Next** to begin creating the group.

3 Enter a name and description for the group.

4 Click **Next**.

5 Select the devices you want to include in the group by checking the box in the first column for each device to include. You can use the Search function to narrow the list of devices, if necessary.

6 Click **Next**.

7 Review the summary information. Make sure the number of devices you selected matches the **# Devices** summary. Click **Previous** if you need to modify the group.

8 Click **Create**. The group is successfully created.

9 Click **Close** to exit the wizard.

To create a Dynamic Discovery Group

Discovery group membership is based on the devices found during an LDAP query or domain scan.

1. To launch the wizard:
   - From Group Management, General tab, click **Create a new Discovery Group**
   - From the Groups tab, click the **Create a New Group** toolbar button then select **Create a new Dynamic Discovery Group**.
2. Click **Next** to begin creating the group.
3. Enter a name and description for the group.
4. Click **Next**.
5. Select the discovery source.
   - **LDAP/Active Directory –** Type the LDAP Host and Port number, User ID, password (if required) and the DN to query.

     Also, select the scope, advanced filter or a device limit to apply to the query.
   - **Domain –** to scan a network domain for devices to import, type the domain name (for example, type ABC for a full domain scan of the ABC domain) or part of the domain name and a wildcard character (ABC* returns all devices from domains beginning with ABC). To include specific devices from a domain, use the following syntax, domain\device. For example, `Sales\WS*` returns only devices beginning with `WS` from the `Sales` domain.
     Use an exclamation mark ! to exclude specific devices from a domain. For example, `Sales,!Sales\WS*` will return all devices from the Sales domain with the exception of devices beginning with `WS`.
6. Click **Next**.
7. Configure the refresh schedule for the dynamic group.
   - **Run:** Select whether to update dynamic group membership based on an interval of hours, days, or weeks.
   - **Interval:** Select the specific interval (hours, days, or weeks).
   - **Starting on:** Use the drop-down lists to select the date the group should be refreshed.

- **Current Server Time** displays the current time of the HPCAS server.

8. Click **Next**.
9. Review the summary information and click **Create**.
10. Click **Close** to exit the wizard.

A Discovery Group is created containing the devices found during the LDAP query or domain scan. If discovered devices were not already a part of HPCAS, they are automatically added to the device list. The device membership of this group will update based on the refresh schedule you configured.

To create a Dynamic Reporting Group

Reporting groups are created using the devices returned in a report query.

1. To launch the wizard from the Reporting area, Action Bar click **Create a new Dynamic Reporting Group** .
2. Click **Next** to begin the wizard.
3. Enter a name and description for the group.
4. Click **Next**.
5. Configure the refresh schedule for the dynamic group.
   - **Run:** Select whether to update dynamic group membership based on an interval hours, days, or weeks.
   - **Interval:** Select the specific interval (hours, days, or weeks).
   - **Starting on:** Use the drop-down lists to select the date the group should be refreshed.
   - **Current Server Time** displays the current time of the HPCAS server.
6. Click **Next**.
7. Review the summary information and click **Create**.
8. A Reporting Group is created containing the current devices in the report query. The device membership of this group will be updated based on the refresh schedule you configured.
9. Click **Close** to exit the wizard.

Software Deployment Wizard

Use the Software Deployment Wizard to entitle and deploy software to managed devices in your environment.

To entitle and deploy software using the Software Deployment wizard

1 To launch the wizard:

- From the Software Management, General tab, click **Deploy.**
- From the Software tab, Software Details window, or Group Details window, click the **Deploy Software** toolbar button.

2 Click **Next** to begin the wizard.

3 To select the software to entitle and deploy check the box in the first column.

4 Click **Next**.

5 To select the groups that will be entitled and targeted for deployment check the box in the first column.

6 Click **Next**.

7 Configure the run schedule for the software deployment job. Select **Run: Now** to deploy the software right away, or select **Run: Later** to schedule a date and time for software deployment. To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks** then select the **Interval** from the drop-down list.

> Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

8 Click **Next**.

9 Review the summary information and click **Submit**. The job is successfully created and added to Current Jobs.

10 To view the current software deployment jobs click the Current Jobs tab.

11 Click **Close** to exit the wizard.

Service Import Wizard

Use the Service Import Wizard to import services from the ServiceDecks directory on the HPCAS server machine into a Software, Patch, or OS library.

To import a service using the Service Import wizard

1 Launch the wizard from the Software Management, Software tab, Patch Management, Patches tab or the OS Management, Operating Systems tab by clicking the **Import Service** toolbar button.

2 Select the service to import. All service decks available within the HPCAS server's ServiceDecks directory appear in the list.

The fourth section of each service's file name contains a descriptive name for that software, patch, or OS. For example, PRIMARY.SOFTWARE .ZSERVICE.ORCA is the service deck for the Orca software application.

3 Review the summary information and click **Import**. The service is imported and will be available in the HPCAS library.

4 Click **Close** to exit the wizard.

Service Export Wizard

Use the Service Export Wizard to export services from the HPCAS Software, Patch, or OS libraries to the ServiceDecks directory on the HPCAS server machine.

To export a service using the Service Export wizard

1 Select a service to export (Software, Patch, or OS).

2 Launch the wizard from the Software Management, Software tab, Patch Management, Patches tab or the OS Management, Operating Systems tab by clicking the **Export Service** toolbar button.

3 Review the summary information and click **Export**. The service is exported to the HPCAS server's ServiceDecks directory.

4 Click **Close** to exit the wizard.

The fourth section of each service's file name contains a descriptive name for that software, patch, or OS. For example, PRIMARY.SOFTWARE .ZSERVICE.ORCA is the service deck for the Orca software application.

Software Synchronization Wizard

Use the Software Synchronization Wizard to create a Software Synchronization Job that will automatically deploy all entitled software to group members that do not have the software installed. Also, Software Synchronization Jobs ensure all new group members automatically receive all entitled software.

To create a Software Synchronization Job

1 On the Group Details window, Software tab, click the Synchronize Software toolbar button to launch the wizard.

2 Configure the run schedule for the software synchronization job. Select **Run: Now** to schedule the job to run right away, or select **Run: Later** to schedule a date and time for the job. To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks** then select the **Interval** from the drop-down list.

> ➤ Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

3 Use the 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 by clicking **Deploy**

— from the Patch Library area, Patch Details, or Group Details windows click the **Deploy Patch** toolbar button.

2 Click **Next** to begin the wizard.

3 Select a deployment method.

Compliance Enforcement – Select this method to determine which patches are applicable to the target devices. Only applicable patches will be installed. As new patches are entitled to the devices, they will be installed the next time this job runs. You must create a recurring schedule in order to enforce patch compliance on an ongoing basis.

Manual Selection – Select this method to deploy the patches to the target devices. If the patches are not applicable to the devices, the job may end in error. Use this method to deploy the patches to target devices one time without creating a recurring compliance schedule.

4 To select the patches to entitle and deploy check the box in the first column.

5 Click **Next**.

6 To select the groups that will be entitled and targeted for deployment check the box in the first column.

7 Click **Next**.

8 Configure the run schedule for the job. Select **Run: Now** to schedule the job to run right away, or select **Run: Later** to schedule a date and time for the job. To configure a recurring schedule, select **Every 'x' Hours, Days,** or **Weeks** then select the **Interval** from the drop-down list.

> ➤ A recurring schedule is only available when you select the **Compliance Enforcement** deployment method.

9. Click **Next**.
10. Review the summary information and click **Submit**. The job is successfully created and added to Current Jobs.
11. To view the current patch deployment jobs click the Current Jobs tab.
12. Click **Close** to exit the wizard.

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

Service Entitlement Wizard

The Service Entitlement Wizard entitles groups of devices to software, operating system images, and patch services.

To add group entitlement using the Service Entitlement wizard

Launch the wizard from the Patch Management, Patches tab or from the OS Management, Operating Systems tab.

1. Select the patches to entitle to a group then click the **Add Group Entitlement** toolbar button.
2. To select the groups that will receive entitlement to the service click the check box in the left column.
3. Click **Next**.
4. Review the summary information and click **Submit**. The job is successfully created and added to the current jobs.
5. To view the current software removal jobs click the Current Jobs tab.
6. Click **Close** to exit the wizard.

Software Removal Wizard

The Software Removal wizard uninstalls software from selected devices or groups.

To remove software using the Software Removal wizard

1. From the Software Details window or the Group Details window, select the software to remove.
2. Click the **Remove Software** toolbar button to launch the wizard.
3. Click **Next** to begin the wizard.
4. Configure the run schedule for the software removal job. Select **Run: Now** to remove the software right away, or select **Run: Later** to schedule a date and time for software removal.
5. Click **Next**.
6. Review the summary information and click **Submit**. The job is successfully created and added to the current jobs.
7. To view the current software removal jobs click the Current Jobs tab.
8. Click **Close** to exit the wizard.

OS Deployment Wizard

The OS Deployment wizard deploys operating systems to managed devices. Operating systems are deployed in either attended or unattended mode. See the Configuration tab's section, OS Management on page 175 to select the deployment mode.

To deploy an operating system using the OS Deployment wizard

1. From the Management tab, OS Management section, click the **Operating Systems** tab.
2. Select the operating system for deployment, then click the **Deploy Operating System** toolbar button.
3. Click **Next** to begin the wizard.

   ➤ Groups created for OS deployment should follow some basic guidelines, for example, all devices within the group should have similar, compatible hardware.

4 Select the groups for operating system entitlement and deployment.

5 Click **Next**.

6 Select the OS deployment method you will use for this job.

— **Local Service Boot (LSB):** Select this option if you want to install LSB in order to deploy the OS. An advantage of LSB is that existing devices do not need to be PXE-enabled and the boot order does not need to be configured locally in the BIOS for each target device.

— **Local CD or PXE Server:** Select this option if you will be using a PXE Server or Service CD to install the operating system on your devices.

7 You are prompted to select whether or not to **Migrate User Data and Settings**. Select **Yes** to backup user data and settings prior to the OS deployment and to restore them afterwards. During the operating system deployment, the Personality Backup and Restore Utility runs silently to back up user data. After the new operating system is installed, the Personality Backup and Restore Utility must be run by the end user to restore user data. The end user should select **Restore from operating system migration** in the Personality Backup and Restore Utility to restore settings that were saved during the backup.

➤ Personality Backup is supported only on source computers that are running Windows 2000, XP, or Vista. Personality Restore is supported only on destination computers that are running Windows XP or Vista. In addition the current operating system and the operating system image being deployed must include an installation of USMT 3.0.1 (see Chapter 12, Personality Backup and Restore).

8 Configure the run schedule for the job. Select **Run: Now** to deploy the OS right away, or select **Run: Later** to schedule a date and time for OS deployment. To configure a recurring schedule, select **Every ‘x’ Hours, Days,** or **Weeks** then select the **Interval** from the drop-down list.

➤ Recurring job schedule options (Every 'x' Days, for example) are available when creating group-related jobs only.

9 Configure any additional job tasks in the **Additional Parameters** section.

10 Click **Next**.

11 Review the summary information and click **Submit**. The job is successfully created and added to Current Jobs.

12. To view the current OS deployment jobs click the **Current Jobs** tab.
13. Click **Close** to exit the wizard

Infrastructure Deployment Wizard

Use the Infrastructure Deployment Wizard to install the Infrastructure service to Infrastructure Servers to enable remote services such as data caching.

To deploy the Infrastructure service

1. From the Configuration tab, Infrastructure Management section's Servers tab click the **Deploy the Infrastructure Service** toolbar button to launch the wizard.
2. Enter deployment credentials and click **Next**.
3. Select the installation drive for the Infrastructure Service and click **Next**.
4. Configure the run schedule for the job. Select **Run: Now** to deploy the service right away, or select **Run: Later** to schedule a date and time for deployment.
5. Click **Next**.
6. Review the summary information and click **Submit**.
7. Click **Close** to exit the wizard

Infrastructure Removal Wizard

Use the Infrastructure Removal Wizard to remove the Infrastructure service from devices in the Infrastructure Servers group.

To remove the Infrastructure service

1. Launch the wizard from the Configuration tab, Infrastructure Management section's Servers tab toolbar.

2. Select the devices from which you want to remove the Infrastructure Service and click **Remove the Infrastructure Service** toolbar button.
3. Select **Run: Now** to remove the service immediately after the wizard is complete, or select **Run: Later** and enter a date and time for removal.
4. Click **Next**.
5. Review the summary information and click **Submit**.
6. Click **Close** to exit the wizard.

Infrastructure Location Creation Wizard

Use the Infrastructure Location Creation Wizard to add new Infrastructure Locations (subnets) to which Infrastructure Servers can be assigned.

To add a new Location

1. Launch the wizard from the Configuration tab, Infrastructure Management section, Location tab toolbar.
2. Click the **Create a New Location** toolbar button
3. Type a description for the Location as well as the subnets you want to include as part of this Infrastructure Location. Use the Subnet Address Calculator to help determine which subnet addresses to use.
4. Click **Create**.
5. Click **Close** to exit the wizard.

9 Preparing and Capturing OS Images

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

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

➤ HPCA Starter supports Thin Client operating system deployment, only.

For Thin Client operating systems, see:

- Preparing and Capturing Thin Client Images on page 201

Preparing and Capturing Thin Client Images

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

- Windows XPe OS images on page 202
- Windows CE OS Images on page 205
- Embedded Linux OS Images on page 208

Windows XPe OS images

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

- Task 1 – Prepare the XPe Reference Machine on page 202
- Task 2 – Run the Image Preparation Wizard on page 202

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

Task 1 – Prepare the XPe Reference Machine

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

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

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

1. Log in to Windows XPe as Administrator.
2. From the XP Embedded Feature Pack 2007, copy `etprep.exe` to `C:\Windows`
3. From the XP Embedded Feature Pack 2007, copy `fbreseal.exe` to `C:\Windows\fba`
4. Install the HPCA agent. See Installing the HPCA Agent on HP Thin Clients on page 65 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 Prep 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 C:\Program Files\Hewlett-Packard\HPCA\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 XPe images can be deployed to target machines with flash drives of equal or greater size. The file contains an embedded file system that will be accessible when the image is installed.

   — `ImageName.EDM`

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

A comprehensive log (`*machineID*.log`) is also available in `the upload` directory 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.

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

3 Click **Browse** to open the `\image_preparation_wizard\win32\` directory.

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

5 Click **Next**. The End User Licensing Agreement window opens.

6 Click **Accept**.

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

 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.

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

14 Accept the defaults and click **Next**. The Summary window opens.

15 Click **Start**.

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

17 Click **OK**.

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

 ⚠ If the device does not boot to the CD (boots to Windows instead) you will need to restart the process from Task 1 – Prepare the XPe Reference Machine on page 202.

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

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

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

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

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

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

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

Now you can use the Publisher to publish the image file to the HPCA server for distribution to managed devices.

Windows CE OS Images

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

- Task 1 - Prepare the CE Reference Machine on page 205
- Task 2 - Run the Image Preparation Wizard on page 206

Task 1 - Prepare the CE Reference Machine

To prepare a CE thin client for image capture, you will need the following:

- HPCA media
- Image Preparation CD-ROM

Before you capture the image, you must install the HPCA agent to the Windows CE device. See Installing the HPCA Agent on HP Thin Clients on page 65 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 Prep 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 C:\Program Files\Hewlett-Packard\HPCA\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`

> While these files are being transferred, network speed will be less than optimal as the operating system image is compressed during transfer.
>
> A comprehensive log (*`machineID`*`.log`) is also available in `the upload` directory 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.
2. If autorun is enabled, the HPCA OS Preparation and Capture CD homepage opens.
3. Click **Browse** to open 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 reserved for OS imaging is 3469.

   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 press F10 during the reboot process and change the boot order in the configuration settings).

   ⚠ If the device does not boot to the CD (boots to Windows instead) you will need to restart the process from Task 1 - Prepare the CE Reference Machine on page 205.

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

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

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

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

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

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

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

Now you can use the Publisher to publish the image file to the HPCA server for distribution to managed devices. See on page .

Embedded Linux OS Images

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

- Task 1 - Prepare the Embedded Linux Reference Machine on page 208
- Task 2 - Run the Image Preparation Wizard on page 209

Task 1 - Prepare the Embedded Linux Reference Machine

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

- HPCA media
- Image Preparation CD-ROM

Before you capture the image, you must install the HPCA agent to the embedded Linux device. See Installing the HPCA Agent on HP Thin Clients on page 65 for details.

For additional thin client device information and instructions for running the installation using NFS, see the installation chapter in the guide or the README file included with `ThinClient.tar`.

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 Prep 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 C:\Program Files\Hewlett-Packard\HPCA\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. Embedded Linux images can be deployed only to target machines with flash drives of equal size. The file contains an embedded file system that will be accessible when the image is installed.

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

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

A comprehensive log (`*machineID*.log`) is also available in `the upload` directory 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 reserved for OS imaging is 3469.

   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 press F10 during the reboot process and change the boot order in the configuration settings).

⚠ If the device does not boot to the CD (boots to Windows instead) you will need to restart the process from Task 1 - Prepare the Embedded Linux Reference Machine on page 208.

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

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

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

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

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

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

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

Now you can use the Publisher to publish the image file to the HPCA server for distribution to managed devices.

Publishing and Deploying OS Images

After you have captured an image, use the Publisher to publish it to the HPCA database. For instructions, see the Publishing information in the HPCA documentation.

When published to HPCA, refresh the OS Library to view the new image. Use the HPCA console toolbar to deploy the image to selected devices.

10 Using the Publisher

Use the Publisher to publish software, BIOS configuration settings, HP Softpaqs, and operating system images to HP Client Automation (HPCA). All published software is available in the Software Management, Software tab of the main HPCA console. Published operating systems are available within the OS Management, Operating Systems tab.

After publishing software, it must be entitled and deployed to managed devices in your environment.

➤ The Publisher is installed automatically to the HPCA Core during the installation of the HPCA Core. If the agent is already installed on the machine, the Publisher will be installed in the agent's folder. If you want to install it to 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 *HP Client Automation Core and Satellite Getting Started and Concepts Guide* for more information.

To start the Publisher

1 On the device where you installed the Publisher, use the **Start** menu and go to:

   Start > **All Programs > HP Client Automation Administrator > HP Client Automation Administrator Publisher**

2 To log in to the Publisher use the HPCA user name and password. By default, the user name is **`admin`** and the password is **`secret`**.

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

Table 20 on page 214 shows which publishing options are available for each of the three license levels.

Table 20 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 Add-ons/extra POS drivers	No	No	No
Thin Client OS Image	Yes	Yes	Yes

- The following sections explain how to use the Publisher for the publishing options for your license. Publishing HP Softpaqs on page 214
- Publishing BIOS Settings on page 216
- Thin Client Publishing on page 218

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.

To publish a Softpaq

1. Start the Publisher (see To start the Publisher on page 213).
2. At the Logon window, type your administrator User ID and password and click **OK**.

   > Log in to the Publisher using the 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.

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

If the sample BIOS settings file does not include the options you require, or you would like to create a settings file for a specific device, see Creating a BIOS Settings File on page 217.

To publish BIOS settings

1 Start the Publisher (see To start the Publisher on page 213).

2 At the Logon window, type your administrator User ID and password and click **OK**.

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

3 In the Publishing Options area, select **HP BIOS Configuration** and click **OK**. The Select window opens.

4 Select the BIOS settings file to publish. The sample BIOS settings file (`Common HP BIOS Settings.xml`) is located by default in: `C:\Program Files\Hewlett-Packard\HPCA\Agent\BIOS`.

5 In the **Current BIOS Admin Password** area, type and then confirm a BIOS password if required. This is required to change any settings if the target devices have a BIOS password.

6 If you want to change the current BIOS password, select, **Change BIOS Password**, then type and confirm the new password. This is required only if you want to change the BIOS password on a client device.

7 Click **Next**. The BIOS Options window opens.

8 To select the BIOS settings to publish click the check box to the left of the BIOS setting name.

9 If you need to change the value of a BIOS setting, click the setting name and adjust the available options as necessary.

10 Click **Next**. The Application Information window opens.

11 View, and if necessary, modify the application information. Application information is pre-determined based on what is available from the settings file.

12 Click **Next**. The Summary window opens.

13 Review the summary information and when satisfied, click **Publish**.

14 When the publishing process is complete, click **Finish** to close the Publisher.

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

Creating a BIOS Settings File

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

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

To create a BIOS settings file

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

2 Type the following:

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

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

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

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

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

3 When you are ready to publish BIOS settings, select this file in step 6 of To publish BIOS settings on page 216.

Thin Client Publishing

The following options are available when publishing for Thin Clients:

- Thin Client Component Select Publishing on page 218
- Thin Client OS Image Publishing on page 220

Thin Client Component Select Publishing

To publish software other than Windows Installer files, use the Component Select option and select the software you want to publish.

To publish using Component Select

1 Start the Publisher (see To start the Publisher on page 213).

2 At the Logon window, type your administrator User ID and password and click **OK**.

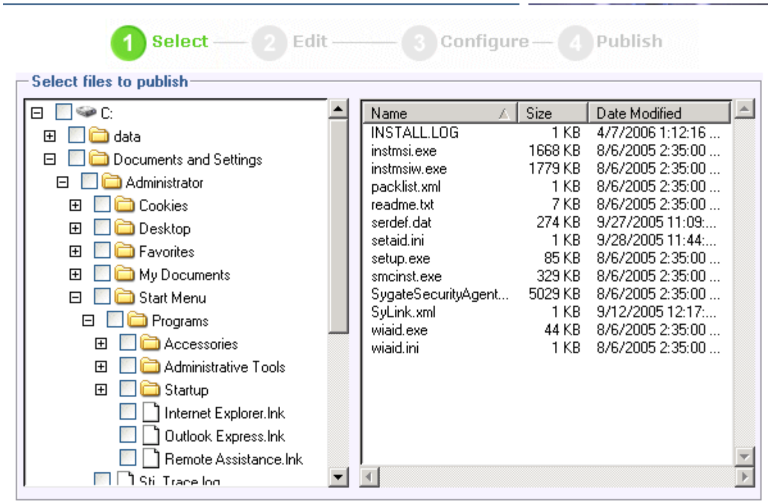
> ➤ Log in to the Publisher using the HPCA user name and password. By default, the user name is **`admin`** and the password is **`secret`**.

3 In the Publishing Options area:

— Select **Thin Client Publishing**.

— From the drop-down list, select **Component Select**.

4 Click **OK**. The Select files to publish window opens.



1 Select — 2 Edit — 3 Configure — 4 Publish

Select files to publish

```
⊟ □ C:
  ⊞ □ data
  ⊟ □ Documents and Settings
    ⊟ □ Administrator
      ⊞ □ Cookies
      ⊞ □ Desktop
      ⊞ □ Favorites
      ⊞ □ My Documents
      ⊟ □ Start Menu
        ⊟ □ Programs
          ⊞ □ Accessories
          ⊞ □ Administrative Tools
          ⊞ □ Startup
            □ Internet Explorer.lnk
            □ Outlook Express.lnk
            □ Remote Assistance.lnk
      □ Sti_Trace.log
```

Name	Size	Date Modified
INSTALL.LOG	1 KB	4/7/2006 1:12:16 ...
instmsi.exe	1668 KB	8/6/2005 2:35:00 ...
instmsiw.exe	1779 KB	8/6/2005 2:35:00 ...
packlist.xml	1 KB	8/6/2005 2:35:00 ...
readme.txt	7 KB	8/6/2005 2:35:00 ...
serdef.dat	274 KB	9/27/2005 11:09:...
setaid.ini	1 KB	9/28/2005 11:44:...
setup.exe	85 KB	8/6/2005 2:35:00 ...
smcinst.exe	329 KB	8/6/2005 2:35:00 ...
SygateSecurityAgent...	5029 KB	8/6/2005 2:35:00 ...
SyLink.xml	1 KB	9/12/2005 12:17:...
wiaid.exe	44 KB	8/6/2005 2:35:00 ...
wiaid.ini	1 KB	8/6/2005 2:35:00 ...

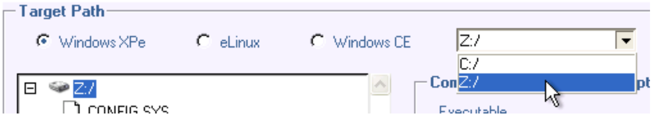
5 Select the files to publish and click **Next**.

> 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 Select the install point, as shown in the following figure.



Target Path

● Windows XPe ○ eLinux ○ Windows CE

Z:/
C:/
Z:/

⊟ Z:/
CONFIG.SYS

Con pt

Executable

.

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.

Thin Client OS Image Publishing

Operating system images created using the Image Preparation wizard are stored on the HPCA server in `C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload`. Use the Publisher to publish operating system image files (`.IMG`) for distribution to managed devices.

The following section describes how to use the Administrator Publisher to publish Thin Client operating system images.

To publish operating system images

1. Start the Publisher (see To start the Publisher on page 213).
2. At the Logon window, type your administrator User ID and password and click **OK**.

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

3. In the Publishing Options area:

- Select **Thin Client Publishing**.
- From the drop-down list, select **OS Image**.

4 Click **OK**. The Select OS image file window opens.

5 Use the Select window to find and select the file you want to publish. (Images created using the Image Preparation Wizard are stored on the HPCA server in the `C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload`).

6 Use the **Description** area to verify the file before you continue. You can also add information to the description if you choose.

7 Click **Next**.

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

a From the **Deployment method** drop-down list box, select ImageX.

b Leave the **Sources Directory** blank. This is not required.

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

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

8 Click **Next**. The Application Information window opens.

9 Use the **Application Information** section to enter the service information.

10 Click **Next**. The Summary window opens.

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

12 Click **Finish** to exit the Publisher when the publishing process is complete.

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

You can view the published operating system image service in the OS Management section, Operating Systems OS Library list.

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.

11 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 on page 224
- Application Self-service Manager Overview on page 224
- Using the Application Self-service Manager User Interface on page 228
- Customizing the User Interface on page 235
- HPCA System Tray Icon on page 241

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.**

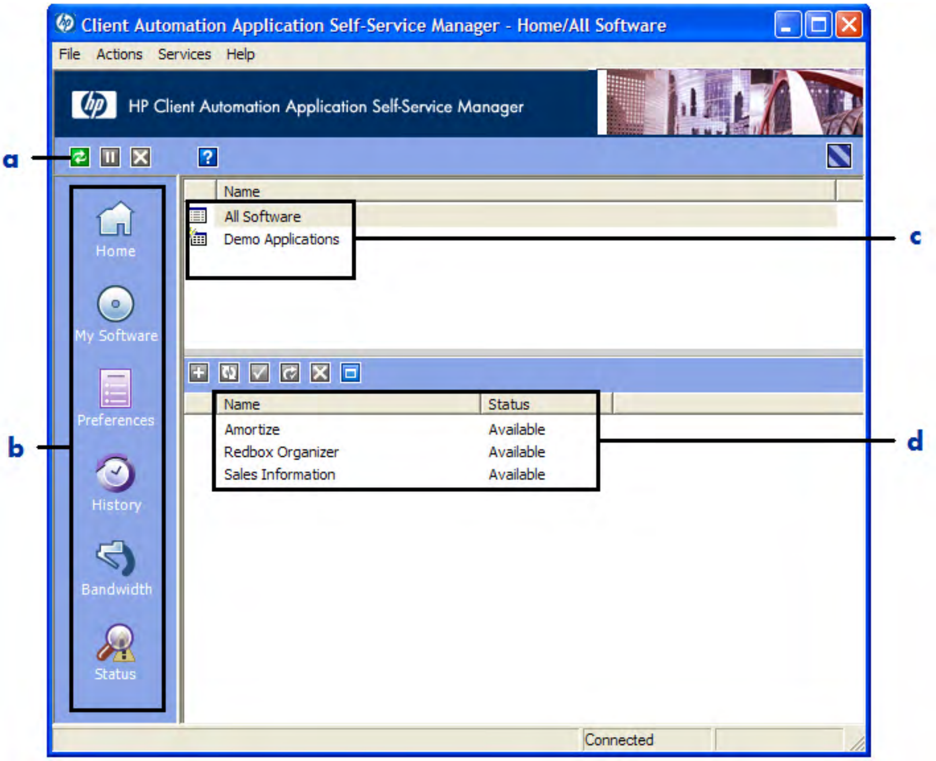
  or

- Double-click the **Client Automation Application Self-Service Manager** desktop shortcut.

Application Self-service Manager Overview

The Self-service Manager interface (see Figure 14 on page 225) 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 14 Application Self-service Manager user interface


Client Automation Application Self-Service Manager - Home/All Software
File
Actions
Services
Help
HP Client Automation Application Self-Service Manager
a
b
c
d
Home
My Software
Preferences
History
Bandwidth
Status
Connected

Name
All Software
Demo Applications

Name	Status
Amortize	Available
Redbox Organizer	Available
Sales Information	Available

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 below
- The Menu Bar on page 226
- Catalog List on page 227
- Service List on page 227

Global Toolbar

The Global Toolbar allows you to refresh the catalog, pause the current action, or cancel the current action. When an action has been paused, no other action can take place until you either resume the action by clicking the **Pause** button again, or cancel the paused action by clicking the **Cancel** button.

Any time one of the buttons in the Global Toolbar is not available for the current action, it will appear grayed-out.

To refresh the catalog

- To refresh the selected catalog using the Global Toolbar, click **Refresh** ⟳.

To pause or resume the current action

- To pause the current action using the Global Toolbar, click **Pause** ⏸.
- To resume a paused action, click **Resume** ▶. (The **Pause** button is replaced with this button after you pause an action).

To cancel the current action

- To cancel the current action using the Global Toolbar, click **Cancel** ☒.

The Menu Bar

Use the Menu Bar to configure and customize the Application Self-service Manager. The following sections describe each icon on the Menu Bar.

Home: Click this button to access your home catalog.

My Software: Click this button to display only those 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

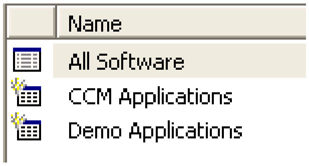
The Catalog List section lists the available software catalogs and any virtual catalogs.

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:



Name
All Software
CCM Applications
Demo Applications

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, see Preferences: Click this button to access various display options, application list options, and connection options for the Self-service Manager. on page 226 for more information.

Table 21 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.
↻	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 229
- Refreshing the Catalog on page 230
- Viewing Information on page 230
- Removing Software on page 231

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:

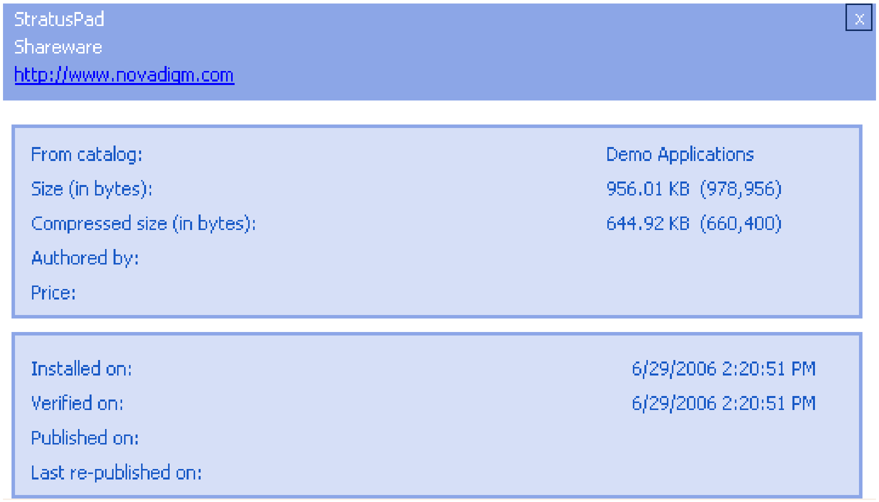
- Adding these columns to the Service List.
- Clicking **Show Extended Information** in the expanded service box.

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.



StratusPad
Shareware
http://www.novadigm.com

From catalog:	Demo Applications
Size (in bytes):	956.01 KB (978,956)
Compressed size (in bytes):	644.92 KB (660,400)
Authored by:	
Price:	

Installed on:	6/29/2006 2:20:51 PM
Verified on:	6/29/2006 2:20:51 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.

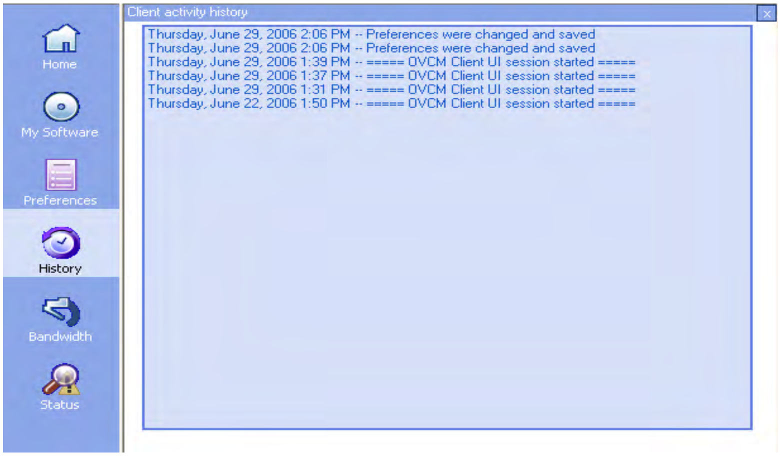
To repair software

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 15 History window



```
Thursday, June 29, 2006 2:06 PM -- Preferences were changed and saved
Thursday, June 29, 2006 2:06 PM -- Preferences were changed and saved
Thursday, June 29, 2006 1:39 PM -- ===== OVCM Client UI session started =====
Thursday, June 29, 2006 1:37 PM -- ===== OVCM Client UI session started =====
Thursday, June 29, 2006 1:31 PM -- ===== OVCM Client UI session started =====
Thursday, June 22, 2006 1:50 PM -- ===== OVCM Client UI session started =====
```

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.

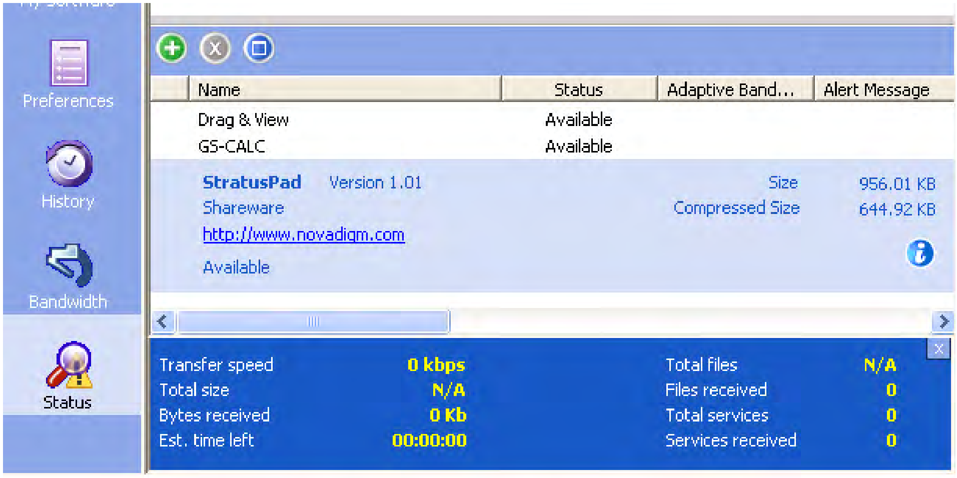
To adjust the bandwidth settings using the bandwidth slider

- Click and drag the slider to increase or decrease the amount of bandwidth throttling desired.
- You can also adjust bandwidth throttling from within the Preferences, Connection options section.

Viewing Status

In the Menu bar, click **Status** to display the status of the current action including the size, estimated time, progress, and available bandwidth.

Figure 16 Status display for selected application



Name	Status	Adaptive Band...	Alert Message
Drag & View	Available		
GS-CALC	Available		

StratusPad Version 1.01

Shareware

http://www.novadigm.com

Available

Size 956.01 KB

Compressed Size 644.92 KB

Transfer speed	0 kbps	Total files	N/A
Total size	N/A	Files received	0
Bytes received	0 Kb	Total services	0
Est. time left	00:00:00	Services received	0

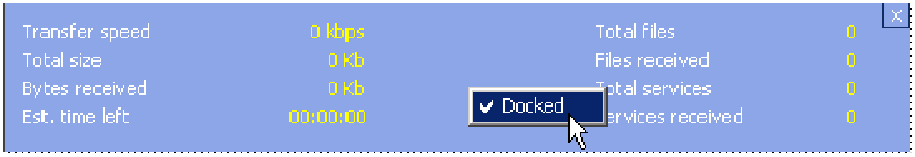
The Status window can be docked or un-docked from the Application Self-service Manager. This enables you to position it anywhere on your screen. The Status window is docked by default.

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.



Transfer speed	0 kbps	Total files	0
Total size	0 Kb	Files received	0
Bytes received	0 Kb	Total services	0
Est. time left	00:00:00	ervices received	0

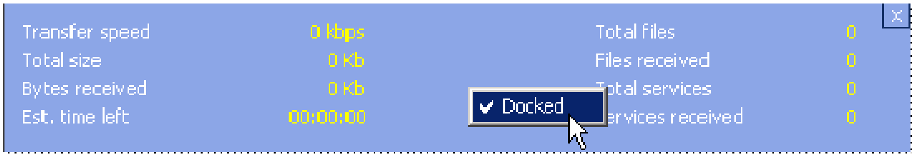
The Status window will be released from the Application Self-service Manager interface, allowing you to position it anywhere on your screen.

To dock the Status window

1 Click **Status** in the Menu Bar.

2 Right-click in the Status window that opens.

3 Select **Docked** from the shortcut menu (only if there is no check mark present).



Transfer speed	0 kbps	Total files	0
Total size	0 Kb	Files received	0
Bytes received	0 Kb	Total services	0
Est. time left	00:00:00	Services received	0

The Status window will be docked into the Application Self-service Manager interface.

Customizing the User Interface

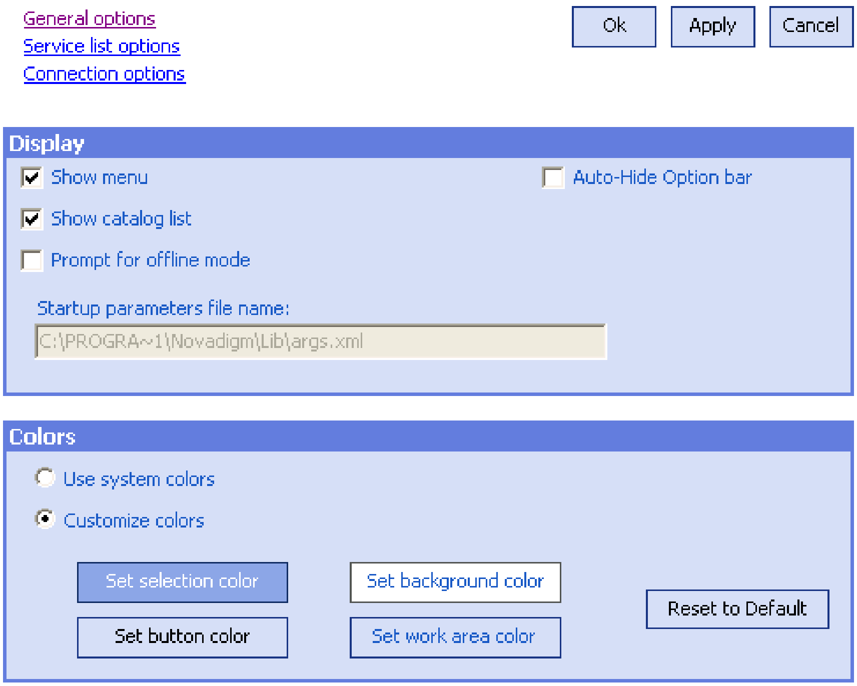
Click the **Preferences** button in the Menu Bar to view the available customization options. The following sections describe each customization area.

- General Options on page 235
- Service List Options on page 237
- Connection Options on page 240

General Options

Use the General options window to modify the appearance of the Application Self-service Manager interface.

Figure 17 General options window



☑ Show menu

□ Auto-Hide Option bar

☑ Show catalog list

□ Prompt for offline mode

Startup parameters file name:
C:\PROGRA~1\Novadigm\Lib\args.xml

○ Use system colors

● Customize colors

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 automaticallyhidden, select **Auto-Hide Option bar**.

To modify the colors

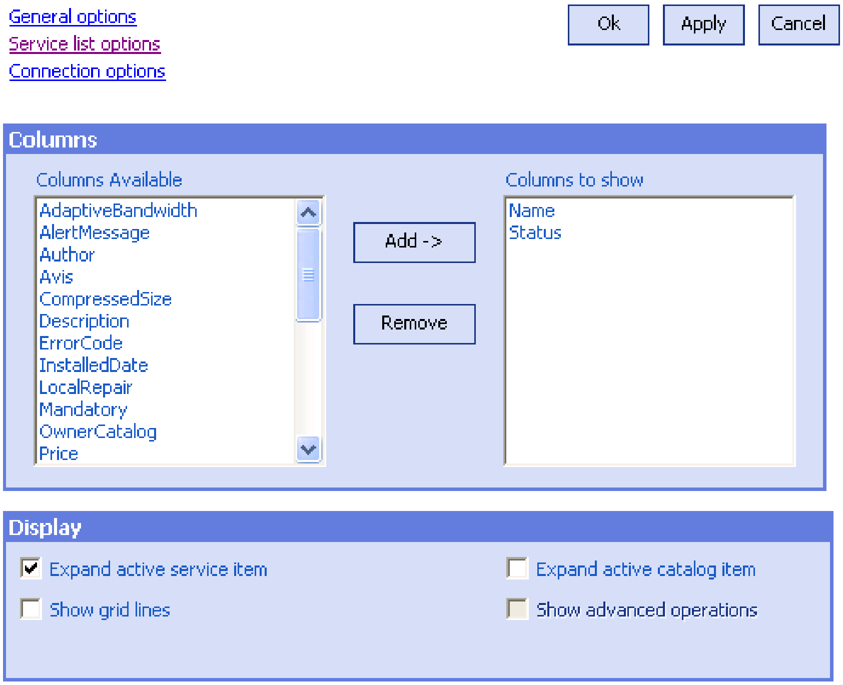
- If you want to use the system colors, select **Use system colors**.
- If you want to customize the color scheme, select **Customize colors**.
  — After selecting Customize colors, click the box labeled:

- **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 18 Service List options



General options
Service list options
Connection options

Ok Apply Cancel

Columns

Columns Available

AdaptiveBandwidth
AlertMessage
Author
Avis
CompressedSize
Description
ErrorCode
InstalledDate
LocalRepair
Mandatory
OwnerCatalog
Price

Add ->
Remove

Columns to show

Name
Status

Display

☑ Expand active service item
□ Expand active catalog item
□ Show grid lines
□ Show advanced operations

To customize the column names in the Service List

Use the Columns area to customize the columns that appear in your Service List. The right column lists the 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 238.

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 22 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 22 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.

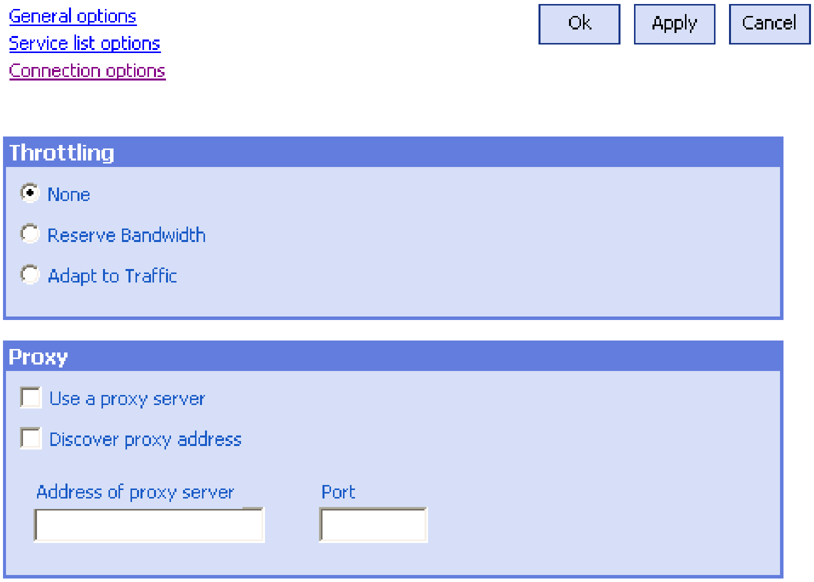
Table 22 Column headings available for the Service List

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 19 on page 240, to select the type of bandwidth throttling to use and to specify proxy server settings.

Figure 19 Connection Options



Throttling

● None

○ Reserve Bandwidth

○ Adapt to Traffic

Proxy

☐ Use a proxy server

☐ Discover proxy address

Address of proxy server

Port

- **Throttling**
  - — Select **None** for no throttling.

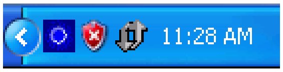
- Select **Reserve Bandwidth** to slide along the scale to indicate the maximum percentage of the network bandwidth to use. The reserve bandwidth can be changed in the interface by the user as the download is happening.
- Select **Adapt to traffic** to slide along the scale to indicate the minimum percentage 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 *`SystemDrive`*`:\Program Files\Hewlett-Packard\HPCA\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 20 HPCA System Tray Icon



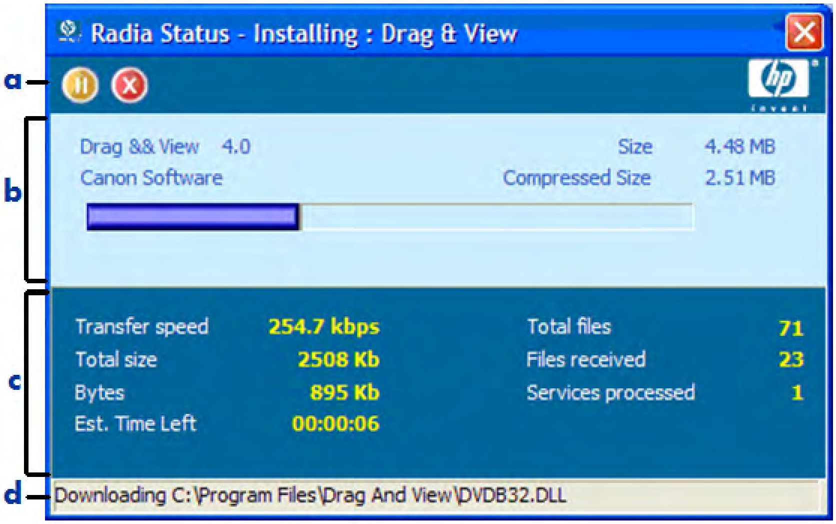
Move your cursor over the icon to see HPCA states:

- **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 21 HPCA Status



Radia Status - Installing : Drag & View

Drag && View 4.0 Size 4.48 MB
Canon Software Compressed Size 2.51 MB

Transfer speed 254.7 kbps
Total size 2508 Kb
Bytes 895 Kb
Est. Time Left 00:00:06

Total files 71
Files received 23
Services processed 1

Downloading C:\Program Files\Drag And View\DVDB32.DLL

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.

12 Personality Backup and Restore

Personality Backup and Restore allows 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.

The HPCA Personality Backup and Restore solution is based on the Microsoft User State Migration Tool (USMT) and also contains a user interface (HPCA Personality Backup and Restore Utility) developed by Hewlett-Packard to facilitate the backup and restore process.

The features and components of USMT are discussed in User State Migration Tool on page 247. You use migration rules to define what user files and settings on the source computer should be captured in the backup.

The Personality Backup and Restore Utility is discussed in Using the HPCA Personality Backup and Restore Utility on page 251. It is deployed to agent computers during the agent installation and is used to back up and restore those files and settings.

➤ After upgrading to the latest version of HPCA, you must perform new backups of your user files and settings. Backups created with previous versions of HPCA cannot be restored.

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

- Requirements on page 246
- User State Migration Tool on page 247
- Using the HPCA Personality Backup and Restore Utility on page 251
- Troubleshooting on page 256

Requirements

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

Operating Systems

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

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

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

- Windows XP
- Windows Vista

Disk Space

Before you begin, you will need to determine if your source computer, destination computer, and Core Server have adequate disk space to store the files and settings being backed up. To estimate the disk space that will be needed for the backup, refer to “Determine Where to Store Data” on the Microsoft TechNet web site at: **http://technet.microsoft.com/en-us/library/cc722431.aspx**. Note that the storage location is automatically set by the Personality Backup and Restore Utility, and each of the source computer, destination computer, and 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. The 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.

Software

You need the following two applications:

- **Microsoft USMT version 3.0.1**
  This application needs to be installed on the source and destination computers. See User State Migration Tool on page 247.

  ⚠ This solution requires that you use Microsoft USMT version 3.0.1. No other version of USMT is supported.

- **HP Client Automation Personality Backup and Restore Utility**
  This application needs to be installed on both the source and destination computers. It is installed automatically with the HP Client Automation agent when that agent is deployed from the Core Console to one of the supported HPCA Personality Backup and Restore platforms. However, if you install the agent manually (refer to the *HPCA Application Manager and Application Self-service Manager Installation and Configuration Guide*) you will need to make the following modifications to the `Install.ini` as indicated in the comments in that file:

```
;To install Personality Backup and Restore (PBR), add
NVDINSTALLPBR to the following line (preceded by a comma)
```

```
ADDLOCAL=NVDINSTALLRAM,NVDINSTALLRSM,NVDINSTALLRIM,NVDINSTAL
LRLAE,NVDINSTALLROM,NVDINSTALLPATCH,NVDINSTALLPLUSHP
```

Be certain that you include all the other command line parameters indicated here.

User State Migration Tool

Since 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 **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 251.

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

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

- As an administrater you want to become familiar with the capabilites 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 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. No other version of USMT is supported.

Obtaining Microsoft USMT 3.0.1

Go to the Microsoft web site at **http://www.microsoft.com/downloads/details.aspx?FamilyID=799ab28c-691b-4b36-b7ad-6c604be4c595&displaylang=en** to acquire the application. There are two versions: 32-bit and 64-bit. Select the appropriate version for your environment.

Installing Microsoft USMT 3.0.1 on Managed Devices

You can install USMT on managed devices in two ways. It can be installed manually, or it can be packaged into a service using the HPCA Administrator Publisher (see Chapter 10, Using the Publisher) and then entitled or deployed to managed devices. USMT must be installed to the default installation directory of `C:\Program Files\USMT301` on the source and destination client devices. The default installation directory is the same for 32-bit and 64-bit machines.

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

Migration Files

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

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

Before you implement this solution in your environment you must obtain these files and store them on the HPCA Core Server (see Storing the Migration Rules on the Core Server on page 250).

To obtain these files you must install USMT on one of its supported platforms (see Obtaining and Installing Microsoft USMT 3.0.1 on page 248). The installation places these files in `C:\Program Files\USMT301`.

You can then edit these files (see Editing the Rules on page 250) 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. Go to **http://technet.microsoft.com/en-us/library/cc766203.aspx** to learn how to customize these files.

Storing the Migration Rules on the Core Server

When you are finished editing these files, or even if you choose not to edit them, save them to `Data\PersonalityBackupAndRestore\conf` on the HPCA Core Server, where `Data` is the user-configurable data directory specified during the HPCA Core installation.

➤ These three files, whether you have modified them or not, must be placed in `Data\PersonalityBackupAndRestore\conf` and must have the same file names as the original files obtained from the Microsoft USMT 3.0.1 installation.

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"
```

where *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 the HPCA Personality Backup and Restore Utility

This section explains how to use the HPCA Personality Backup and Restore Utility to back up files and settings on a source computer and how to restore those files and settings to a destination computer. Each time this utility is run, it downloads the migration xml files (see Migration Files on page 249) from the Core Server to use during the migration.

Berfore you begin, make sure you have enough disk space available on the Core Server, and on the source and destination computers (see Disk Space on page 246.)

To start the Personality Backup and Restore Utility:

- On the 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 Personality Backup and Restore Utility.

- Personality Backup on page 252
- Personality Restore on page 253

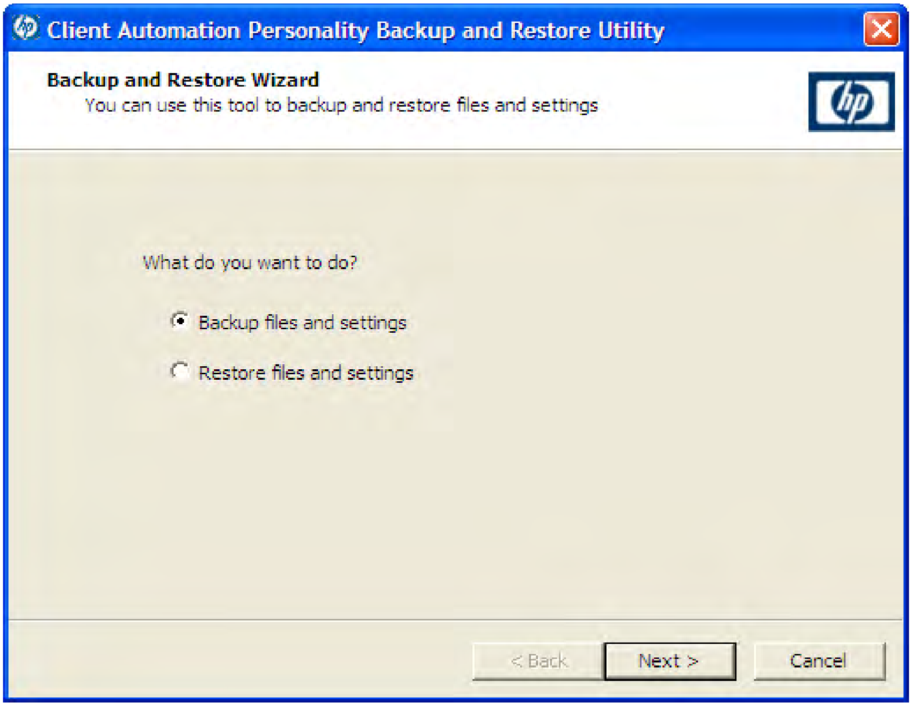
Personality Backup

You must run the Personality Backup and Restore Utility from a user account with administrative credentials.

Close as many open files and running applications as is possible before you run a backup to help ensure a successful 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 client device start the Personality Backup and Restore Utility. The Backup and Restore Wizard opens.



Client Automation Personality Backup and Restore Utility

Backup and Restore Wizard

You can use this tool to backup and restore files and settings

What do you want to do?

● Backup files and settings

○ Restore files and settings

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

3. Enter the computer name of the computer 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 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 applcation.

Stored Files and Settings

Each time you back up files and settings, they are stored on the Core Server under `Data\PersonalityBackupAndRestore\backups` where `Data` is the user-configurable data directory specified during the installation of the Core Server. A subdirectory is created under the `backups` folder that contains the computer name and an encoding of the password supplied by the user. All of the backup information that is required for a restore is stored under this subdirectory.

The backup data on the Core Server are never deleted. If backup data for a particular computer are no longer needed, the subdirectory containing that backup data can be deleted manually by an administrator.

Personality Restore

You must run the Personality Backup and Restore Utility from a user account with administrative credentials.

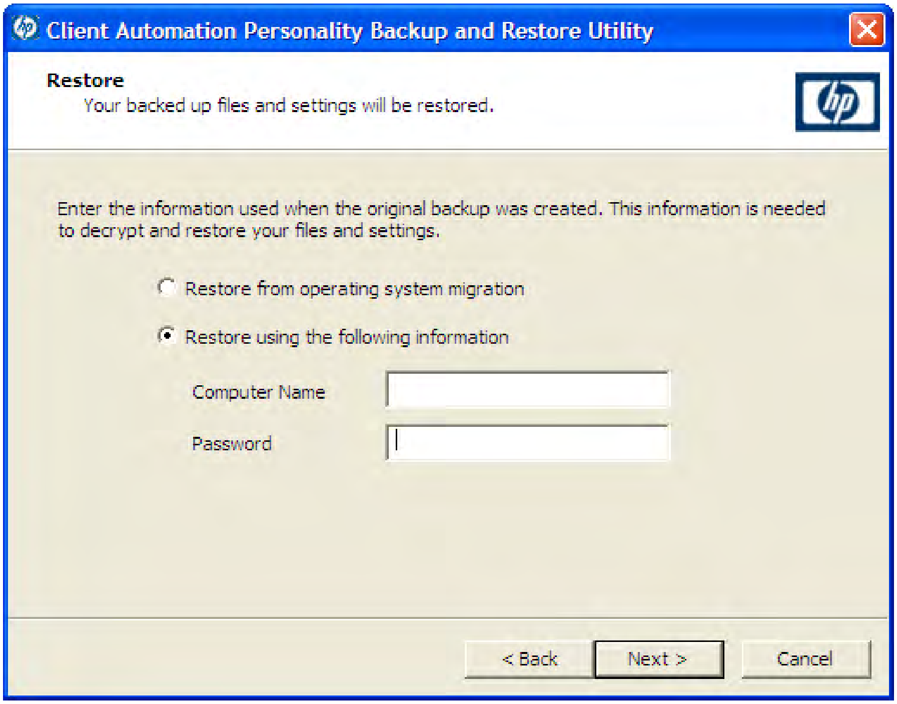
Close as many open files and running applications as is possible before you run a restore to help ensure a successful restore. Do not launch new applications or open files while the restore is running, as this can cause the restore to fail.

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 as was used for the backup. You should also do a restore to the same locale (for example, US English) as was used for the backup.

To restore files and settings using Computer Name and Password

1. On the destination computer start the Personality Backup and Restore Utility. The Backup and Restore Wizard opens.
2. Select **Restore files and settings** and click **Next**. The Restore dialog box opens.



Client Automation Personality Backup and Restore Utility

Restore

Your backed up files and settings will be restored.

Enter the information used when the original backup was created. This information is needed to decrypt and restore your files and settings.

○ Restore from operating system migration

● Restore using the following information

Computer Name

Password

If you have a Starter license, the Restore from operating system migration option is not supported.

3 Select **Restore using the following information** and type the Computer Name and Password that were used during the backup. Then click **Next**. The Summary dialog box opens.

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

5 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.

Troubleshooting

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

Backup or Restore did not Complete Successfully

If the backup or restore did not complete successfully, check the `pbr.log` under the agent's `Log` directory for any errors that may have occurred during the backup or restore. The default `Log` directory is `C:\Program Files\Hewlett-Packard\HPCA\Agent\Log`.

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

Users Forget Password and Cannot Restore Data

To perform a restore you need both the computer name and password that the user supplied in the Personality Backup and Restore Utility. 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 Core Server that contains the user files and settings. This directory resides under *`Data`*`\PersonalityBackupAndRestore\backups`, where *`Data`* is the user-configurable data directory specified during the installation of the Core. The subdirectories are named *`ComputerName_Encoded ComputerNameAndPassword`*.
2. The administrator runs the Personality Backup and Restore Utility to perform a backup. This backup should *not* be performed on the computer of the user that 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 finds the new directory created under `Data\PersonalityBackupAndRestore\backups`, deletes the *contents* of that directory, and copies the contents from the original backup directory discussed in step 1.
4. The end user runs the Personality Backup and Restore Utility, entering the original computer name and the password created by the administrator, to restore his files and settings.

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

13 FAQs

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

- How do I publish an OS image? on page 268
- How do I deploy an OS image? on page 268

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 148.

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 182 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 183.
- Follow the steps in the wizard on page 183 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 185 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 186 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 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 10, Using the Publisher for more information.

How do I publish setup.exe?

- Use the Publisher and select **Component Select** as the Type of Data to Publish. Select the files to publish and follow the steps in the Publisher to make the file available for distribution to your managed devices.

  Refer to the Publisher online help or Chapter 10, Using the Publisher for more information.

How do I know that all my devices received the software?

1. In the Management area, click Software Management.
2. On the Reporting tab, click **Software Summary.** The Reporting area is displayed with a summary of all devices, managed services, and failed services.

You can also use the Software Details window, Devices tab to view the status of software organized by device.

1. Click the description link for any software to open the Software Details window.
2. Click **Devices** tab.
3. View the Software Status column to see which managed devices have the software installed. Only entitled devices are displayed.

How do I make software available for a user to install?

By adding software entitlement to a group of devices, that software is then available for the user to install from the Application Self-service Manager.

- From the Group Management section of the Management tab, click the **Groups** tab.
- Click any Group description link to open the Group Details window.
- Click the **Software** tab to display all entitled software for that group.
- To entitle additional software, click **Add Software Entitlement**.
- Select the software to entitle and click **Add Entitlement**.

When entitled, software is available for deployment from the Console or from the Application Self-service Manager on the individual devices.

How do I generate a device compliance report?

- Use the Reporting tab to define which patch bulletin you want to see compliance for.
- In Data Filters, click **Patch Management Related**.
- Click **Patch Compliance Status**.
- Enter a bulletin name or partial name, and click **Apply**.
- Use the tools at the top of the report list to export or print the report.

How do I capture an OS image?

Use the Image Preparation Wizard to prepare and capture operating system images.

1 Create the Image Preparation CD from the `ImageCapture.iso` file. The file is located on the HPCA media in the `\Media\iso\roms` directory.

2. Follow the preparation steps in the Image Preparation Wizard online help or see Chapter 9, 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 C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload directory on the HPCA server.

  Refer to the Publisher online help or Chapter 10, Using the Publisher for more information.

How do I deploy an OS image?

First, create a Static Group containing all devices to receive the OS image.

1. Within the Group Management, General tab, click **Create a new Static Group**.

2. The Group Management Wizard opens. Follow the steps in the Group Creation wizard to create the group.

Now you can deploy software to devices in the newly created group.

1. In the Management tab, click **OS Management**.
2. Click **Deploy Operating System**. The OS Deployment Wizard opens.
3. Follow the steps in the wizard to select the newly created group and the software for deployment. An OS Management Job is created.

14 Troubleshooting

Use the following sections to troubleshoot common problems you may encounter while using HPCA.

- Log Files on page 271
- Agent Deployment Issues on page 273
- OS Deployment Issues on page 274
- Application Self-service Manager Issues on page 275
- Power Management Issues on page 275
- Patch Management Issues on page 276
- Troubleshooting the HPCA Server on page 276
- Browser Issues on page 280
- Dashboard Issues on page 282
- Other Issues on page 283

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 23 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: 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.
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 23 Agent Deployment Job Messages and Troubleshooting

Message	Troubleshooting Steps
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 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.

Application Self-service Manager Issues

This section describes common HP Client Automation Application Self-service Manager (ASM) issues and the steps to follow to resolve possible problems.

Application installation failed, Catalog displays as installed

Issue

The application may display as installed in the Catalog if the installation program returned a zero upon failure.

Possible Resolutions

The ASD relies on a return code to detect whether or not the installation was a success. The installation must return a code of non-zero in order for the ASM to detect the failure.

This can be accomplished by wrapping the installation in a command file and using logic to validate whether the process was a success or not by returning the proper code.

Power Management Issues

This section describes issues and possible resolutions for tasks related to the 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 95 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 276

Troubleshooting HPCA Core Components

The following sections describe how to troubleshoot issues related to the Core server components.

- HPCA Core Configuration Files on page 276
- HPCA Core Log Files on page 279

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 `C:\Program Files\Hewlett-Packard\HPCA\`*`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 24 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`
		`MessagingServer\etc\usage.dd.acfg`
OS Manager Server		`OSManagerServer\etc\HPCA-OSM.rc`
		`OSManagerServer\etc\roms.cfg`
		`OSManagerServer\etc\roms_upd.cfg`

Table 24   HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (C:\Program Files\Hewlett-Packard\HPCA\...)
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
		ReportingServer\etc\rum.cfg
		ReportingServer\etc\scm.cfg
		ReportingServer\etc\vm.cfg
Thin Client		TC\etc\HPCA-TC.rc
		TC\etc\rmms.cfg

Table 24 HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (`C:\Program Files\Hewlett-Packard\HPCA\...`)
Tomcat	Enterprise Manager	`tomcat\webapps\em\WEB-INF\Console.properties`
	Enterprise Manager	`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 on page 280
- Cannot Enable HTTP 1.1 with Internet Explorer 6 and SSL on page 280

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:

In Internet Explorer 6, perform the following steps:

1. Click **Tools→Internet Options**.
2. Click the **Advanced** tab.
3. Scroll down to the HTTP 1.1 settings.
4. Clear the **Use HTTP1.1** box.

Then, close Internet Explorer, and open a new browser window. Simply refreshing the current Internet Explorer window will not fix the problem.

Alternative solution: Upgrade to Internet Explorer 7.

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 on page 282
- Dashboard Panes in Perpetual Loading State on page 282

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 Console is 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.

Other Issues

The following troubleshooting tips pertain to issues not addressed in the previous topics:

- Cannot Open a Report on page 283
- Additional Parameters Disregarded by the HPCA Job Wizard on page 284
- Virtual Machines Will Not Start on page 285
- Query Limit Reached on page 285

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.

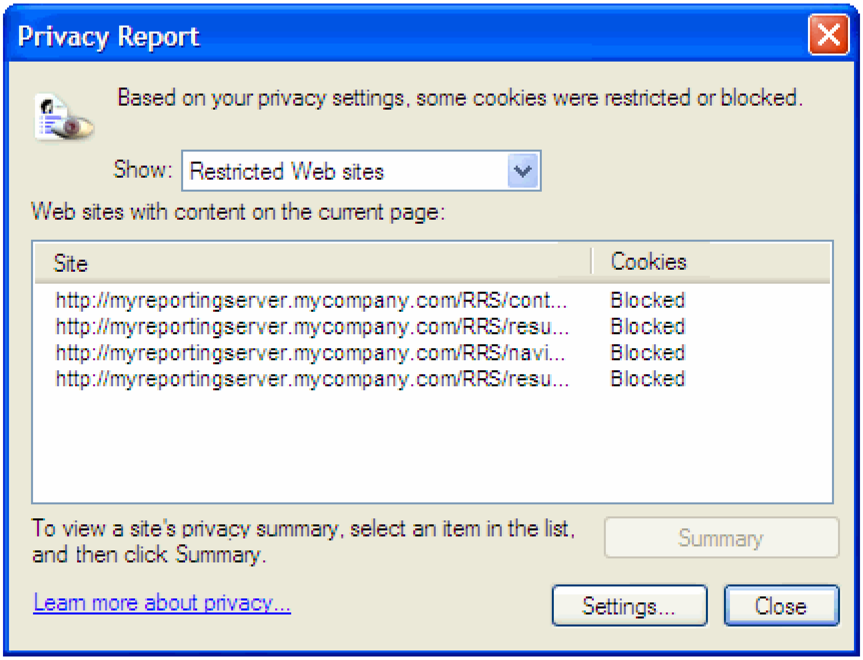
This behavior is most prevalent with Internet Explorer 6 and 7 on the Windows 2003 Server platform. It can, however, happen on any supported platform.

Solution:

1 Open the list of blocked URLs.

In Internet Explorer 7, for example, click the eye-shaped icon with the red circle in the lower browser bar:

You will see a dialog something like this:



Based on your privacy settings, some cookies were restricted or blocked.

Show: Restricted Web sites

Web sites with content on the current page:

Site	Cookies
http://myreportingserver.mycompany.com/RRS/cont...	Blocked
http://myreportingserver.mycompany.com/RRS/resu...	Blocked
http://myreportingserver.mycompany.com/RRS/navi...	Blocked
http://myreportingserver.mycompany.com/RRS/resu...	Blocked

To view a site's privacy summary, select an item in the list, and then click Summary.

2 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.

```
C:\Program Files\Hewlett-Packard\HPCA\tomcat
```

After modifying the `Console.properties` file, be sure to restart the HPCA 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 on page 287
- SSL in an HPCA Environment on page 288
- The SSL Certificate Fields on the Consoles on page 289

For additional information, refer to the *HP Client Automation SSL Implementation Guide*.

SSL Parts

Refer to Chapter 1 of the *HP Client Automation SSL Implementation Guide* for a comprehensive look at:

- Certificates
- Certificate Authorities
- Generating Certificates
- Private Key Files
- Public Key Files

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.

➤ Refer to Chapter 1 of the *HP Client Automation SSL Implementation Guide* for information on SSL Certificate Authorities, SSL certificates, and generating SSL certificates.

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 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 152.

Refer to Chapter 1 of the *HP Client Automation SSL Implementation Guide* for information on SSL certificates, SSL Certificate Authorities, and generating SSL certificates.

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:

`C:\Program Files\Hewlett-Packard\HPCA\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 in as "trusted."

After the file has been uploaded (located and **Save** clicked) it is saved to:

```
C:\Program Files\Hewlett-Packard\HPCA\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 291
- Changing the Locale on page 292

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

Supported Languages

Table 25 on page 291 presents the list of supported languages and their valid language codes.

Table 25 Supported Languages and Codes

Language	**Language Code**
Korean	ko_KR
English	en_US
Japanese	ja_JP
Simplified Chinese	zh_CN

Changing the Locale

To add support for a supported language in a PXE environment

1. Use a text editor to open `\X86PC\UNDI\linux-boot\linux.cfg\default`. The file looks similar to the following:

   ```
   DEFAULT bzImage

   APPEND initrd=rootfs.gz root=/dev/ram0 rw ISVR=10.10.10.1
   ISVRPORT=3466
   ```

2. Add the **`LANG`** parameter to the end of the `APPEND` line and specify a valid language code (see Table 25 on page 291).

   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 25 on page 291 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.

Index