

HP Client Automation

Core and Satellite

Enterprise Edition

for the Windows® and Linux 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

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

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

Trademark Notices

The Apache Software License, Version 1.1

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)

Copyright © 1999-2001 The Apache Software Foundation. All rights reserved.

Linux is a registered trademark of Linus Torvalds.

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

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER

Copyright © 1996-1999 Intel Corporation.

TFTP SERVER

Copyright © 1983, 1993

The Regents of the University of California.

OpenLDAP

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.

Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License
Copyright © 1998-2001 The OpenSSLProject.

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

DHTML Calendar
Copyright Mihai Bazon, 2002, 2003

Lab PullParser
Copyright © 2002 The Trustees of Indiana University. All rights reserved
This product includes software developed by the Indiana University Extreme! Lab. For
further information please visit <http://www.extreme.indiana.edu/> .

Documentation Updates

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

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

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

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

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

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

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

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

Support

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1	Introduction	21
	About This Guide	21
	HPCA Documentation	21
2	Getting Started	23
	Accessing the Web-based HPCA Console	24
	Implement HPCA	25
	Mandatory Tasks	25
	Optional Tasks	26
	Import Devices	26
	Deploy the HPCA Agent	26
	Configure Policy	27
	Configuring Internal Policy	27
	Configuring External Policy	28
	Verifying Policy Resolution	30
	Manage Vulnerabilities	30
	Configure Client Operations Profiles	30
	Create Server Access Profile Instances	31
	Modify Service Access Profiles for Patch Distribution using the Gateway	33
	Connect SAP Instances to a Location Class Instance	34
	Enable Client Operations Profiles in HPCA Agents	35
	Synchronize the Satellites	36
	Configure Patch Management	36
	Patch Management Administration Tasks	37
	Limitation on Modifying Configuration Files	38
	Deploy Operating System Images	38
	Core and Satellite Server Functions	39
	HPCA OS Manager Notes	39

HPCA OS Manager System Administrator Guide Notes	39
Enable Out of Band Management	40
Features	40
Configuration Tasks	41
Operations Tasks	41
3 Security and Compliance Management	43
Introduction	44
Vulnerability Management.	44
Compliance Management.	46
Security Tools Management.	49
HPCA and HP Live Network.	50
License Requirements	50
Software Prerequisites.	51
How Security and Compliance Management Works in HPCA	52
How HP Live Network Content is Updated	53
Scanning Services in Detail	57
Configuring Security and Compliance Management.	60
Common Security and Compliance Management Tasks	60
Update HP Live Network Content.	60
Schedule or Trigger a Scan.	61
Entitle A Device for Scanning.	62
Create an HPCA Job to Schedule or Trigger a Scan	63
Start a Scan from a Target Device	64
View the Results of a Scan or Update	65
Find Vulnerability Remediation Information	65
Find Information about Compliance Failures.	67
Find Information About Security Tools	69
Advanced Topics.	70
Use the Command Line Utility	70
Required Settings	71
Optional Settings.	73
Stored Settings.	75
Examples	75
Run the HP Live Network Connector Manually.	76
Next Steps	78

Move HP Live Network Content from a Test Environment to a Production Environment	78
More Information about Security and Compliance Management	80
4 Using the Dashboards	83
Dashboard Overview	84
Dashboard Perspectives	88
Dashboard Filters	89
HPCA Operations Dashboard	89
Client Connections	90
Service Events	92
12 Month Service Events by Domain	94
Vulnerability Management Dashboard	96
Vulnerability Impact by Severity (pie chart)	97
Historical Vulnerability Assessment	99
Vulnerability Impact	101
HP Live Network Announcements	106
Vulnerability Impact by Severity (bar chart)	107
Most Vulnerable Devices	109
Most Vulnerable Subnets	110
Top Vulnerabilities	112
Compliance Management Dashboard	115
Compliance Status	116
Compliance Summary by SCAP Benchmark	118
Historical Compliance Assessment	119
Top Failed SCAP Rules	121
Top Devices by Failed SCAP Rules	123
Security Tools Management Dashboard	125
Security Product Status	126
Security Product Summary	128
Most Recent Definition Updates	130
Most Recent Security Product Scans	131
Patch Management Dashboard	134
Device Compliance by Status (Executive View)	134
Device Compliance by Bulletin	136
Device Compliance by Status (Operational View)	138

Microsoft Security Bulletins	139
Most Vulnerable Products	140
5 Managing the Enterprise	143
Managing Directory Policies	144
View an Object's Properties	146
Search for an Object	148
Manage Policy for Directory Objects	150
Service Information	153
Importing Devices	153
Managing Groups	154
Deploying the HPCA Agent	156
Managing Jobs	158
Current and Past Jobs	159
Jobs and Job Executions	160
Targets	160
Schedules	161
Job Details for DTM Jobs	162
Job Details for Notify Jobs	163
Job Details for RMP Jobs	164
Job Execution Details	164
Job Execution States	165
Create a New DTM or Notify Job	166
Delete a Job	167
Refresh DTM Schedules on Targets	167
Device Resolution for Notify Jobs	169
Device Resolution for DTM Jobs	169
Removal of Old Job Execution Records	170
Creating Satellite Synchronization Jobs	171
Managing Virtual Machines	173
Creating New Virtual Machines	177
Controlling Devices Remotely	180
Requirements for Remote Connections	181
Requirements for Windows Remote Desktop Connection	182
Requirements for VNC	182
Requirements for Windows Remote Assistance	183

Firewall Considerations	184
Remote Control Auditing	185
Managing Operating Systems	186
OS Management Terms	187
Prerequisites for OS Management	188
Deployment Scenarios	189
Requirements for Target Devices	190
Deploying Thin Client Factory Images	192
How it Works	192
View the OS Deployment State	193
Deploy an OS Image	193
OS Management Wizard	194
Using LSB	196
Using Network Boot	196
Using an ImageDeploy CD or DVD	197
Perform a One-Time Hardware Maintenance Operation	198
View the Status of OS Management Activities	200
Viewing Out Of Band Details	200
6 Using Reports	203
Reports Overview	204
Navigating the Reports	206
Types of Reports	208
HPCA Management Reports	209
Inventory Management Reports	209
HP Hardware Reports	210
Patch Management Reports	210
Vulnerability Management Reports	211
Compliance Management Reports	213
Security Tools Management Reports	215
Drilling Down to Detailed Information	219
Filtering Reports	219
Vulnerability Management Filters	223
Compliance Management Filters	224
Security Tools Management Filters	226

7	Operations	229
	Infrastructure Management	230
	Server Status	230
	Support	231
	Downloading Log Files	232
	Live Network	232
	Schedule Automatic Live Network Updates	234
	Update the HP Live Network Content Now	235
	View the Results or Status of an Update	235
	Download the HP Live Network Connector	236
	Out of Band Management	237
	Provisioning and Configuration Information	237
	DASH Configuration Documentation	238
	DASH Configuration Utilities	238
	Device Management	239
	Group Management	240
	Alert Notifications	241
	Patch Management	241
	Start Acquisition	241
	Perform Synchronization	243
	View Agent Updates	244
	View Acquisition History	247
	View Logs	247
	Delete Devices	247
	Gateway Settings	248
	View Cache Statistics	249
	Cache Content Details	250
	Export URL Requests	250
	Import URL Requests	251
	OS Management	252
	CD Deployment	252
8	Configuration	253
	Licensing	254
	Upstream Host	254
	Access Control	255

Core Console Access Control	255
Users Panel	255
Roles Panel	258
Satellite Console Access Control	259
Configuration	261
Data Cache	261
Infrastructure Management	263
Proxy Settings	263
SSL	264
SSL Server	264
SSL Client	265
Policy	265
Database Settings	267
Directory Services	267
Navigate the Directory Services Page	269
View Directory Service Details	269
Modify Directory Service Property Settings	271
Configure a Connection to the Configuration Server Directory Service	272
Configure Connections to External Directory Services	273
Job Action Templates	276
Create a New Template	277
Sample Templates	280
Multicast	280
Live Network	281
Configure the Connection to the HP Live Network Server	281
Test Your Live Network Settings	282
Device Management	284
Alerting	284
CMI	284
Thin Clients	285
Configure Remote Control	286
Patch Management	287
Database Settings	287
Patch Distribution Settings	288
Agent Options	291

Agent Updates	294
Preferences	295
Vendor Settings	297
SuSE Requirements for Patch Management	309
SuSE 10 Registration Requirements	310
Acquisition Jobs	311
Out of Band Management	314
Enablement	314
Device Type Selection	314
DASH Devices	315
vPro Devices	315
Both	315
Configuration and Operations Options Determined by Device Type Selection . .	316
vPro System Defense Settings	316
OS Management	317
Settings	318
Dashboards	318
HPCA Operations	319
Vulnerability Management	319
Compliance Management	321
Security Tools Management	322
Patch Management	323
9 Patch Management Using Metadata	325
Overview	325
Configuring Patch Management for Metadata Distribution (Microsoft only)	329
Configuring the Patch Agents	331
Agent Configuration for Gateway Access	331
Agent Configuration for Offline Scanning	332
Offline Scanning Requirements	332
Agent Configuration for Download Manager	333
Entitling Agents to Patches	335
Patch Acquisition and Gateway Operations	336
10 Preparing and Capturing OS Images	337
Preparing and Capturing Images	338

Capturing pre-Windows Vista for Legacy Deployment	338
Task 1: Prepare the Reference Machine.	339
Task 2: Prerequisites	340
Task 3: Run The Image Preparation Wizard	340
Capturing pre-Windows Vista for ImageX Deployment	340
Task 1: Copy utilities to the HPCA Server.	341
Task 2: Prepare the Reference Machine.	341
Task 3: Prerequisites	342
Task 4: Run The Image Preparation Wizard	342
Capturing Windows Vista for ImageX Deployment	342
Task 1: Copy utilities to the HPCA Server.	342
Task 2: Prepare the Reference Machine.	343
Task 3: Prepare unattend.xml	343
Task 4: Run The Image Preparation Wizard	344
Capturing Windows Server 2008 for ImageX Deployment.	344
Task 1: Copy utilities to the HPCA Server.	344
Task 2: Prepare the Reference Machine.	344
Task 3: Prepare unattend.xml	345
Task 4: Run The Image Preparation Wizard	345
Capturing pre-Windows Vista for Windows Setup Deployment	345
Task 1: Prepare the Reference Machine.	346
Task 2: Create Unattend.txt	347
Task 3: Install the HPCA Windows Native Install Package	348
Task 4: Run the HPCA Windows Native Install Package	349
Capturing Windows Vista for Windows Setup Deployment.	352
Task 1: Copy utilities to the HPCA Server.	352
Task 2: Prepare the Reference Machine.	353
Task 3: Run The Image Preparation Wizard	353
Capturing Windows Server 2008 for Windows Setup Deployment	353
Task 1: Copy utilities to the HPCA Server.	354
Windows AIK is available from the Microsoft web site. It is not included as part of a normal Vista installation.	354
Task 2: Prepare the Reference Machine.	354
Task 3: Run The Image Preparation Wizard	355
Using Microsoft Sysprep	355
How Sysprep.inf files are prioritized	357

About the Image Preparation Wizard	358
Using the Image Preparation Wizard Exit Points	359
Preparing To Capture Remote Images	359
Using the Image Preparation Wizard	360
Using the Image Preparation Wizard in Unattended Mode.	365
Preparing and Capturing Thin Client Images	367
Windows XPe OS images	367
Task 1 – Prepare the XPe Reference Machine	367
Task 2 – Run the Image Preparation Wizard	368
Windows CE OS Images.	371
Task 1 - Prepare the CE Reference Machine	371
Task 2 - Run the Image Preparation Wizard	371
Embedded Linux OS Images	373
Task 1 - Prepare the Embedded Linux Reference Machine	374
Task 2 - Run the Image Preparation Wizard	374
Publishing and Deploying OS Images	377
11 Using the Publisher	379
Publishing Software.	381
Publishing Windows Installer Files.	381
Publishing Using Component Select	383
Publishing Operating System Images	385
Prerequisites for publishing .WIM images of a Vista OS.	385
About the .subs and .xml files.	386
Example of Substitution	387
Preparing filename.xml.	388
Publishing OS Images	388
Publishing OS Add-ons/extra POS Drivers	390
Prerequisites	390
Publishing BIOS Settings	392
Creating a BIOS Settings File	393
Publish Hardware Configuration Elements	394
Viewing Published Services.	396
HP Client Automation Administrator Agent Explorer	396
12 Using the Application Self-service Manager	397

Accessing the Application Self-service Manager	398
Application Self-service Manager Overview.....	398
Global Toolbar.....	400
The Menu Bar.....	400
Catalog List.....	401
Virtual Catalogs.....	401
Service List.....	401
Using the Application Self-service Manager User Interface.....	402
Installing Software.....	403
Refreshing the Catalog.....	404
Viewing Information.....	404
Removing Software.....	405
Verifying Software.....	406
Repairing Software.....	406
Viewing History.....	406
Adjusting Bandwidth.....	407
Viewing Status.....	407
Customizing the User Interface.....	409
General Options.....	409
Service List Options.....	411
Customizing the Display.....	412
Connection Options.....	414
HPCA System Tray Icon.....	415
HPCA Status Window.....	416
13 Troubleshooting.....	419
Log Files.....	419
OS Deployment Issues.....	420
Application Self-service Manager Issues.....	421
Power Management Issues.....	421
Patch Management Issues.....	422
Troubleshooting the HPCA Server.....	422
Troubleshooting HPCA Core Components.....	422
HPCA Core Configuration Files.....	423
HPCA Core Log Files.....	425

Troubleshooting HPCA Satellite Components	426
HPCA Satellite Log Files	426
Browser Issues	427
Cannot Refresh Page Using F5	427
Cannot Enable HTTP 1.1 with Internet Explorer 6 and SSL	427
Browser Error Occurs when Using Remote Control	428
Job Issues	428
DTM Jobs Not Working Correctly / RMP Jobs Missing	428
Dashboard Issues	430
Delete Dashboard Layout Settings	430
Most Vulnerable Products Dashboard Pane Loads Slowly	430
Dashboard Panes in Perpetual Loading State	430
Security and Compliance Issues	431
HP Live Network Connector Unable to Connect	432
Managed and Scanned Device Counts are Zero	432
Report Presentation is Slow	432
Other Issues	433
Cannot Open a Report	434
Additional Parameters Disregarded by the HPCA Job Wizard	435
Virtual Machines Will Not Start	435
Query Limit Reached	436
A SSL Settings on the HPCA Core and Satellite Servers	439
SSL Parts	439
SSL in an HPCA Environment	440
Supporting SSL Communications to Remote Services	440
Providing Secure Communications Services to Consumers	440
The SSL Certificate Fields on the Consoles	441
SSL Server	441
SSL Client	442
B About Double-Byte Character Support	443
Supported Languages	443
Changing the Locale	444
Double-byte Support for Sysprep Files	444

C IPv6 Networking Support	445
IP Networking Terms and Basics	445
Terms	446
IP Address Shortcuts: IPv4 versus IPv6	447
Bracketing IPv6 Addresses	447
Overview of IPv6 Support in HPCA	448
IPv6 Support Limitations	448
Support for IPv6 in a Core-Satellite Environment	448
IP Communications Support Table	449
How to Enable IPv6 Server Communications	449
Prerequisites for IPv6 Support	450
Configuring HPCA Windows Servers for IPv6 Support	451
Component: HPCA Apache-based Core and Satellite Servers	451
Component: HPCA Configuration Server	451
How IPv6 is Enabled for the Configuration Server Component	452
Log Messages	453
Using IPv6 Literal Addresses with Core and Satellite Consoles	455
Core and Satellite Support of IPv6 Addresses	455
IPv6 How To's and Troubleshooting	456
Frequently Asked "How To" Questions	456
Troubleshooting an IPv6 Environment	458
From a remote browser I can access the Core or Satellite, but my login fails with Unknown login failure, or no response. Is there a solution?	458
Is it a local tool problem, such as a problem with the Web Browser?	459
Is it a local OS problem? Does the OS have IPv6 support?	459
Is it a problem with the local OS? How do I test for DNS name resolution of the hostname?	459
Is there a problem with the IP addresses I am using? How can I double check them? 460	
Is it a problem with the network between my client and the server? Again, how can I validate that?	461
Index	463

1 Introduction

HP Client Automation Enterprise 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*.

HPCA Documentation

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

2 Getting Started

After you have installed HPCA, you are ready to start using the web-based HPCA Console (the Console) to begin managing your environment.

The sections in this chapter introduce:

- The HPCA Console that you will use to perform various administrative and configuration tasks. See [Accessing the Web-based HPCA Console](#) on page 24.
- The tasks that you must complete in order to begin managing your HPCA environment. This includes configuration steps and where to get more information. See [Implement HPCA](#) on page 25.

Accessing the Web-based HPCA Console

The HPCA server uses a Console through which various administrative and configuration tasks can be performed. For more information on these tasks, see [Operations](#) on page 229 and [Configuration](#) on page 253.

There are three methods by which you can launch the HPCA Console. You can:

- Double-click the **HP Client Automation Console** desktop icon.
- Navigate the Windows **Start** menu path of the machine on which the HPCA server was installed.
- Open a Microsoft® Internet Explorer® (minimum version 6.0) or Mozilla Firefox (minimum version 2.0) 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 will launch the HPCA Console, which will prompt 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 253 for information on changing the default user name and password, and adding users to the Console-access authority list.

Important Notes

- The HPCA console may open additional browser instances when you are running wizards or displaying 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 will need to log in again to continue using the Console.
- In order to view the graphical reports in the **Reporting** section of the Console, either Java Runtime or Java Virtual Machine is required. 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.

Implement HPCA

The following sections describe the initial tasks that you will complete in order to begin using HPCA to manage your environment. All of these tasks are completed using the HPCA Core Console. Some of the tasks are required (*mandatory*) in order to establish a viable HPCA environment; others, although *optional*, are also included because they enable additional basic administrative functionality.

The tabs of the HPCA Core Console (listed below) allow you to access the various administrative tasks.

- Dashboard
- Management
- Reporting
- Operations
- Configuration



It will not be necessary to access all of these tabs in order to complete the configuration tasks.

Mandatory Tasks

The tasks that are listed in this section must be completed in order to establish a viable and functioning HPCA-managed environment.

- 1 **Import Devices:** Import your client devices into the HPCA environment so that they are “known” to the HPCA server. See [Import Devices](#) on page 26.
- 2 **Deploy HPCA Agent:** Deploy the HPCA agent to the client devices that you have imported. This will bring them under the control of HPCA.

There are several methods by which to deploy an HPCA agent; these are described in [Deploy the HPCA Agent](#) on page 26.

- 3 **Configure Policy:** Use HPCA to establish the “state” of the HPCA agents on your client devices. See [Configure Policy](#) on page 27.

Optional Tasks

The tasks that are listed in this section can be completed in order to establish additional administrative control over, and functionality within, your HPCA environment. More information about each of these tasks is presented in the respective sections.

- [Manage Vulnerabilities](#) on page 30
- [Configure Client Operations Profiles](#) on page 30
- [Configure Patch Management](#) on page 36
- [Deploy Operating System Images](#) on page 38
- [Enable Out of Band Management](#) on page 40

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.

- On the Device Management General tab, click **Import** to launch the Import Device Wizard (see [Importing Devices](#) on page 153).
- Follow the steps in the wizard to import devices.



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

When devices have been imported, you can begin deploy the HPCA agent in order to manage software, patches, and inventory.

Deploy the HPCA Agent

The HPCA agent gets deployed to and installed on a device in order to facilitate an HPCA administrator managing the device. The agent can be individually deployed to a device, or deployed to several devices that belong to a group.

The HPCA agent is deployed to devices by using the Agent Deployment Wizard (see [Deploying the HPCA Agent](#) on page 156). When the wizard completes, an Agent Deployment job is created.

For additional information about the HPCA agent, refer to the *HP Client Automation Application Manager and Application Self-Service Manager Guide*.

Configure Policy

HPCA resolves a managed agent's desired state according to the policy entitlements that an HPCA administrator has defined for a machine or user. The policy entitlements can be defined:

- **Internally:** In the PRIMARY.POLICY Domain of the Configuration Server Database (CSDB).
- **Externally:** In an LDAP directory, such as Active Directory.

The Core CSDB is preconfigured with default instances that make it easy to implement existing external policy, and the Core and Satellite servers have a setting with which to enable and configure an external policy connection.

Configuring Internal Policy

Policy for HPCA agents can be configured in the PRIMARY.POLICY.USER Class of the Core CSDB. When an HPCA agent connects to the CSDB, if its user identity has been defined as an instance in the USER Class, resolution will occur according to the policy that is defined in that instance. If you are using this method for your policy store, you should:

- Disable the policy services on the Core and Satellite servers.
- Add USER Instances to the USER Class and connect them to the services to which the users are entitled.

For more information on establishing this method of internal policy, refer to the policy chapters in the *HPCA Application Manager and Application Self-service Manager Installation and Configuration Guide*.

Configuring External Policy

Policy settings can be applied to an existing LDAP (or other external) directory and then enabled for use with an HPCA environment. The steps to enable this support are documented in [Implementing an External Policy Store](#) on page 28.

When using an external policy store, the default behavior in the Core CSDB is:

- For HPCA agent connects in which the user is not defined by a USER Instance, resolution defaults to using the machine domain name and looks for policy defined in an external LDAP directory that has been configured for access using the policy settings on the Core and Satellite Consoles.
- The resolution by machine name from an external directory is defined in the `_NULL_INSTANCE_` of `PRIMARY.POLICY.USER`. This instance includes an `_ALWAYS_` (Utility Method) connection with its attribute set to `SYSTEM.ZMETHOD.LDAP_RESOLVE`.

Implementing an External Policy Store

The policy configuration defaults for an external policy store are set up to connect to an LDAP directory, and manage policies using the fully qualified domain name of the HPCA agent-managed machines. To manage policies using different parameters, adjust the `ZMTHPRMS` attribute in the `LDAP_RESOLVE` method, as discussed in [To implement an external LDAP policy store](#) on page 28.

By default, configuring the Core for an external directory service results in the Portal also being configured to use (for policy) the same external directory service. The external directory service connection is derived from the Base DN.

To implement an external LDAP policy store

- 1 Configure the Core so that the Policy service can connect to the external directory service that is used for policy. See [To use Directory Service Accounts](#) on page 260 for instructions on how to do this.
- 2 Enable and configure full-service Satellites to connect to the external directory service.

- 3 Use the LDIF file that was generated at the Policy page of the Core Console (and which contains the schema changes) to modify your directory schema so that the HPCA policy settings are used.

The command to backup an existing LDAP is:

```
LDIFDE -f OutputFileName
```

The command to update the external directory service is:

```
LDIFDE -i -f HPCAExtensions.ldif -v
```



The **LDIFDE** command is applicable to Windows server platforms only. For additional information, refer to the Microsoft KnowledgeBase article, [Using LDIFDE to import and export directory objects to Active Directory](#).

For more information, refer to the *Policy Server Guide*.

- 4 If necessary, modify the LDAP_RESOLVE method in the PRIMARY.SYSTEM.ZMETHOD Class of the Core Configuration Server Database.

By default, the CSDB is preconfigured to use the LDAP_RESOLVE method and manage policies by the fully qualified domain name of the machine. The ZMTHPRMS attribute defines this:

```
ZMTHPRMS = ldap:\\<ADINFO.COMPDN>>
```

This requires that the machine be a member of the domain that corresponds to the directory in which policy has been defined. If the machine is not a member of the domain, ADINFO.COMPDN will be blank.

- a Adjust the ZMTHPRMS value in order to manage policy using a different value. To do this, refer to *Configuring the LDAP_RESOLVE Method* in the *Policy Server Guide*.
- b **IMPORTANT:** If you adjust the ZMTHPRMS value in the Core CSDB, always perform a synchronization with the Satellite in order to bring down the new value to each Satellite that is enabled for Configuration and Policy.

Following Policy Server configuration, use the Management tab to add, administer, and query the policy entitlements in your LDAP policy store.

Verifying Policy Resolution

To verify that policy is being resolved through a Satellite, do the following.

- 1 Use the Management tab to browse the policy directory and entitle an HPCA agent to a service through its directory service object. Refer to [Managing Directory Policies](#) on page 144.
- 2 Have the HPCA agent installed on the device, with a SAP entry directing it to the Satellite as **PRI 10**, Core as **PRI 20**.
- 3 Perform an HPCA agent connect and verify that the entitled service is available for installation (using Application Self-Service Manager) or is installed (for Application Manager).

Manage Vulnerabilities


To support HPCA Vulnerability Management, you must:

- Create Notify settings
- Review the Console settings
- Configure the **HP Live Network** settings on the Configuration tab of the Console

For additional information, refer to the *Security and Compliance Management* chapter.

Configure Client Operations Profiles

In an HPCA server environment, use **Client Operations Profiles (COPs)** to direct your HPCA agents to the Satellite access points in your enterprise for their configuration and data resources.

-  To learn more about COPs, and for advanced Server Access Profile options, refer to the Configuring Client Operations Profiles chapter in the *HPCA Application Manager and Application Self-Service Manager Installation and Configuration Guide for Windows*.

Create Server Access Profile Instances

The SAP Class of the Core Configuration Server Database contains samples for each type of **Server Access Profile (SAP)**.

You need to create new instances for each Satellite in your environment. Full-service Satellites generally have two instances each, and streamlined Satellites a single instance, as discussed in this section.

▶ The Configuration Server Database changes that are detailed in this must be done on a Core CSDB.

A Satellite server CSDB is a replication of its upstream server CSDB (either a Core or another Satellite) and should never be modified.

- **hostname_RCS Instance:** Use the CORE_RCS instance to create a *hostname_RCS* instance for full-service Satellites.

The URI value of the *hostname_RCS* instance must be modified to point to the hostname of the machine that is hosting the Satellite.

- **hostname_RPS Instance:** Use the CORE_RPS instance to create a **SAT_RPS** instance for each full-service and each streamlined Satellite. For a friendly name, you could use *hostname - Data* to represent its role of providing data resources to HPCA agents.

The URI value of the *hostname_RPS* instance must be modified to point to the hostname of the machine that is hosting the Satellite.

▶ Refer to the *HPCA OS Manager System Administrator User Guide* for SAP information that is specific to OS Manager.

Example

Assume an environment that includes two Satellites (PARISSAT3 and EUROSAT1) and requires the three SAP instances that are listed in [Table 1](#) on page 32.

Table 1 Sample SAP Instances for Two Satellites

Hostname	Satellite Mode	SAP Instance Name (Friendly Name)	SAP Type	SAP Priority
PARISSAT3	Streamlined	PARISSAT3_RPS (PARISSAT3 - DATA)	Data	10
EUROSAT1	Full-service	EUROSAT1_RPS (EUROSAT1 - DATA)	Data	20
EUROSAT1	Full-service	EUROSAT1_RCS (EUROSAT1 - RCS)	RCS	30

To create a Server Access Profile instance for a Satellite

- 1 On the Core server, use the HPCA Admin CSDB Editor to navigate to the **Primary File, Client Domain, Service Access Profile (SAP) Class** of the CSDB.

For information on how to access the HPCA Administrator, refer to the *HPCA Administrator User Guide*.

- 2 From the PRIMARY.CLIENT.SAP Class, copy the CORE_RCS Instance (friendly name: Core - RCS) to an instance named *hostname_RCS* with a friendly name of *hostname - RCS*. (In the example, the EUROSAT1_RCS instance has a friendly name of EUROSAT1 - RCS.)
- 3 Select and modify the *hostname_RCS* Instance; change the URI attribute to point to the hostname of the machine that is hosting the Satellite, as in:

```
URI = tcp://satellite_hostname:3464  
TYPE = RCS  
ROLE = OSMR
```

- 4 Copy the CORE_RPS Instance (friendly name: Core - RPS) to a CLIENT.SAP.*hostname_RPS* instance with a friendly name of *hostname - Data*.

Data indicates that this SAP entry addresses the server's role of providing data resources to the HPCA agents. (In the example, the EUROSAT1_RPS instance has a friendly name of EUROSAT1 - Data.)

- 5 Select and modify the new *hostname_RPS* Instance; change the URI attribute to point to the full-service Satellite's hostname, as in:

```
URI = http://satellite_hostname:3466  
becomes http://EUROSAT1:3466  
TYPE = DATA  
ROLE = DZ
```

- 6 Copy the newly created *hostname_RPS* Instance to create another instance for the streamlined Satellite. (In the example, the PARISSAT3_RPS instance has a friendly name of PARISSAT3 - Data.)
- 7 Modify the newly created SAP instance and set the URI attribute to point to the streamlined Satellite's hostname.
- 8 Save the changes.

Modify Service Access Profiles for Patch Distribution using the Gateway

If you are patching Microsoft devices, you can use a lightweight patching model by configuring the following patch distribution settings.

- Enable Download of Patch Metadata only
- Enable Gateway

When using these patch distribution settings, make sure that the SAP instances for the Core and Satellites that are defined with a TYPE of **DATA**, also include a ROLE of **P**. These instances are typically named *Core_RPS* and *satellite_hostname_RPS*.

If these SAP entries do not include the Role of **P**, modify them using the following procedure.

To modify your SAP instances to deliver patch binaries from the gateway

For basic information on creating or editing SAP instances, see [Create Server Access Profile Instances](#) on page 31.

- 1 From the Core server, use the CSDB Editor to open the SAP instance for the *CORE_RPS* (the one with TYPE = DATA) and make the following changes:

- α Add a ROLE value of **P**.

The values should include the addition in bold:

```
TYPE = DATA  
URI = http://hostname:3466  
ROLE = DZP
```

- 2 Save your changes to the CORE_RPS instance.
- 3 Apply the same ROLE change from Step 1 to your Satellite SAP instances defined with TYPE = DATA. These instances are generally named *satellite_hostname_RCS*.
- 4 Save all changes to the * _RPS instances for the Satellites.

Connect SAP Instances to a Location Class Instance

On the Core server, use PRIMARY.CLIENT.LOCATION Class instances to define the SAP priorities based on location criteria. The priority for a SAP is defined directly above the connection to that SAP instance in the SAPPRI attribute.

By default, the Core_RPS and Core_RCS instances are connected to the CLIENT.LOCATION._BASE_INSTANCE_ with priorities of 60 and 70, respectively.



The priority values run low to high; the lower the number, the higher the priority. So, by assigning a lower number priority to Satellites, HPCA agents will attempt to connect to them as their preferred access points. They will use the Core (with a higher priority number) as the failover access point.

To connect the Core and Satellite SAP instances to a LOCATION Class Instance

- 1 On the Core server, use the HPCA Admin CSDB Editor to set a priority for each SAP instance for each LOCATION Class Instance.

For example, the following image shows SAP Instances connected to the CLIENT.LOCATION._BASE_INSTANCE_ so that all HPCA agents will use the Satellites as the preferred access points.

The image shows a configuration tree on the left and a table of connections on the right. The tree shows a hierarchy starting with CLIENT, followed by LOCATION, and then BASE_INSTANCE_. Under BASE_INSTANCE_, there are several sub-items including Default Core Settings, Default Diagnostics, and various SAP instances like PARISSAT3 - Data, EUROSAT1 - Data, EUROSAT1 - RCS, Core - RPS, and Core - RCS. The table on the right lists connections with columns for connection type, name, and priority.

UI Class Connection		
Hardware Class Connection		
Connect To Class		
Connect To Class		
SAP Priority	10	
Connect To		CLIENT.SAP.PARISSAT3_RPS
SAP Priority	20	
Connect To		CLIENT.SAP.EUROSAT1_RPS
SAP Priority	30	
Connect To		CLIENT.SAP.EUROSAT1_RCS
SAP Priority	40	
Connect To		
SAP Priority	50	

- 2 Connect the CLIENT.SAP.PARISSAT3_RPS Instance to the first available connection in the CLIENT.LOCATION._BASE_INSTANCE_ and give it a priority of 10.
- 3 Connect the CLIENT.SAP.EUROSAT1_RPS Instance to the second available “Connect To” connection and give it a priority of 20.
- 4 Connect the CLIENT.SAP.EUROSAT1_RCS Instance to the third available “Connect To” connection and give it a priority of 30.

By giving the Satellite SAP instances higher priorities than the Core SAP instances, HPCA agents will first attempt to connect to the Satellites. If the Satellites are unavailable, they will attempt to connect to the Core.

Enable Client Operations Profiles in HPCA Agents

There are several ways to enable COPs in your HPCA agents, depending on whether the HPCA agents are already installed. For all options, refer to the *Configuring Client Operations Profiles* chapter in the *HPCA Application Manager and Application Self-service Manager Installation & Configuration Guide for Windows*.

If an HPCA agent is already installed on a device, you can modify the `args.xml` file to include the `<COP>Y</COP>` entry. Place the entry above the `</ARGUMENTS>` entry and save the changes.



The `args.xml` file is located in `\lib` of the directory in which the HPCA agent was installed. The default is `C:\Program Files\Hewlett-Packard\HPCA\Agent`.

Alternatively, use `COP=Y` in the actions when running `radskman` (or any command to run an HPCA agent connect) from a command line. For more information, refer to the *Application Manager Guide*.

Synchronize the Satellites

To ensure that these changes to the Core CSDB take effect on the Satellites, run a synchronization from each Satellite Console.

Configure Patch Management

Before setting up an HPCA environment to include patch management, be sure that your HPCA databases are appropriately configured. Refer to the *HP Client Automation Core and Satellites Getting Started and Concepts Guide* for details.

Patch management implementation involves setting up the Core and Satellite servers, and then using the Core Console to configure the vendor and acquisition-related settings, and begin patch acquisitions.

Use HPCA to deploy and manage Microsoft, RedHat, and SuSE patches, and HP Softpaqs. Configure the server architecture using the following procedure.

- Create a SQL database for patch and inventory report data.
- Define an ODBC DSN.
- Install a Core server and configure the following:
 - Infrastructure Management
 - Patch Management

- Policy (if using an external policy directory)

▶ When the Patch ODBC settings are saved in the Core Console, the Core server automatically runs an initial synchronization between the Patch Management database and the Core Configuration Server Database.

- Install a Satellite server (recommended).

Completing the above tasks creates the HPCA server environment for Patch Management.

Patch Management Administration Tasks

- 1 Enable Patch during the Core installation.
- 2 Complete all Patch Management configuration settings from the Configuration tab of the Console.
 - Create acquisition jobs for obtaining Microsoft, RedHat and SuSE patches, as applicable.
 - ▶ HP recommends enabling Patch Management using Metadata for Microsoft patches. This feature reduces the time it takes to acquire patches and the overall load on the Core Configuration Server. For details, see [Patch Management Using Metadata](#) on page 325.
 - HP Softpaqs use a single, preconfigured acquisition job. To take advantage of this, run an inventory against HP managed devices so that their HP Softpaq SysIDs can be automatically added to the acquisition settings for HP Softpaqs.
- 3 Perform patch acquisitions from the Core Console **Operations** tab.
- 4 After acquiring patches and publishing them to the Core CSDB, synchronize the content of the Core and Satellite servers using either a scheduled job or a Satellite Console Operations task.
 - Use the Core Console Management tab to create and run jobs to synchronize the content of the Core and Satellite servers.
 - Use the Satellite Console **Operations** tab to synchronize the Core and Satellite servers. The Satellite Console can be accessed at **http://*satellite_hostname*:3466**.

- 5 The next time the agents connect, a patch scan is run to discover which bulletins are applicable to which devices. Use the Dashboards and Reports tabs to view the results of the patch scans.
- 6 Apply policy to entitle bulletins to your managed devices. The applicable patches will be deployed without user intervention. Use the Dashboards and Reports to see the Patch compliance status of the managed devices.

Limitation on Modifying Configuration Files

HP discourages the customizing of configuration files for any of the components that are installed with the Core and Satellite servers.



The functionality of the HPCA Core and Satellite servers includes environmental differences as compared with classic HPCA infrastructure server environments.

Do not follow any of the instructions in the *Patch Manager Installation and Configuration Guide* that instruct you to modify the Patch Manager configuration file.

If you need further support, contact HP Customer Support.

Deploy Operating System Images

HPCA can be used to deploy and manage operating system images. In order to do this, HP recommends that you:

- 1 Enable the OS Manager service on the Core server.
 - On the Core Console, Configuration tab, OS Management option, Settings area, select **Enable**.

The *Operations*, *Configuration*, and *Managing the Enterprise* chapters of this guide further discuss OS Manager settings in the Core Console.
- 2 Leave the default Core server name (zone) of **HP**.
- 3 Enable the OS Manager service on at least one Satellite server.
 - On the Satellite Console, Configuration tab, Operating Systems area, select **Enable**.

The *Configuration* chapter of this guide further discusses OS Manager settings in the Satellite Console.

Your HPCA server environment is now set up to use the OS Manager with its default configuration.

Core and Satellite Server Functions

The HPCA servers perform the following OS Manager-related functions.

- The Core server hosts the tools and services that are used for:
 - Publishing the operating system images to the authoritative CSDB.
 - Performing OS Manager administrative tasks on the Console.
 - Creating policy entitlements.
- The Satellite server assumes the role of the OS Manager Server and Proxy Server; it handles requests for operating system images from the Configuration Server and provides the resources for these images to the managed devices.

After you have published operating system images to the Core CSDB, use the Satellite Console **Operations** tab to *synchronize* and *preload* the operating system image resources onto the Satellite Server.

HPCA OS Manager Notes

- By default, when the OS Manager is installed with a Core or Satellite server, it is configured to use the Linux Service OS—it is not set up to run WinPE as the Service OS.

To convert the environment to use WinPE as the default Service OS, refer to Chapter 3 in the *OS Manager Guide for Windows*.

- The HPCA Thin Client server can be installed via the HPCA Console; it can also be enabled and disabled there.
- Refer to the *HPCA OS Manager System Administrator User Guide* for SAP information that is specific to OS Manager.

HPCA OS Manager System Administrator Guide Notes

The *OS Manager Guide* contains additional information that is necessary for configuring the OS Manager in a Core-Satellite environment. It should be used in conjunction with the HPCA Core and Satellites documentation. The following are important notes regarding some of the information in that guide.

- The chapter, *Installing and Configuring the Server Architecture*, is not relevant to the OS Manager in a Core-Satellite environment.
- Ignore information in any section that discusses customizing and/or modifying configuration files for components that are automatically installed with the Core and Satellite servers.
- The **Thin Client server** that is installed on Core and Satellite servers is referred to as the **Mini Management Server** in the *OS Manager Guide*.

Enable Out of Band Management

Out of Band Management (OOBM) refers to operations that are performed on a computer when it is in one of the following states.

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

The HPCA Console supports OOBM of **Intel vPro** and **DASH**-enabled devices.

This section provides an overview of HPCA OOBM. For more detailed information on the features and functionality of HPCA OOBM, refer to the *HPCA Out of Band Management User Guide*.

Features

The OOBM feature in the HPCA Console:

- Takes advantage of hardware-based management capabilities in PCs with vPro technology, as well as those with an implementation of the DASH standard.
- Improves hardware and software inventories, and reduces the need for desk-side visits.
- Provides *System Defense* capabilities for vPro devices that allow for selective network isolation.
- Provides *Agent Presence* capabilities that allow for the monitoring of local agents running on vPro systems.

- Provides an operating system-independent and tamper-resistant worm-containment system for vPro devices.
- Provides a secure communications channel through **Hypertext Transfer Protocol (HTTP)** authentication and **Transport Layer Security (TLS)**.

Configuration Tasks

This section briefly describes some of the Administrator-based tasks that are performed on the **Configuration** tab of the HPCA Console. An HPCA administrator should perform these configuration tasks as preparation for managing OOB devices. For more information on these tasks, refer to the *HPCA Out of Band Management User Guide*.

- **Enable Out of Band Management:** The first thing an HPCA administrator must do in order to perform OOBM tasks.
Under Out of Band Management, click **Enablement**.
- **Select the Device Type:** The HPCA Console offers three choices for device type: DASH Devices, vPro Devices, and Both.
Under Out of Band Management, click **Device Type Selection**.
- **Manage vPro System Defense:** This option appears only if vPro Devices was selected as the device type to be managed.

Under Out of Band Management, click **vPro System Defense Settings**.



System Defense settings do not apply to DASH devices.

Operations Tasks

This section briefly describes some of the tasks that can be performed in the Administrator and Operator roles of HPCA. These OOB device-management tasks are performed on the **Operations** tab of the HPCA Console by an HPCA *administrator* or *operator*. For more information on these tasks, refer to the *HPCA Out of Band Management User Guide*.

- **Provision Devices:** vPro devices must be provisioned before HPCA can discover and manage them.

Under Out of Band Management, click **vPro Provisioning**.



This option does not appear on the **Operations** tab if you have opted to manage only DASH devices because it is not relevant for these devices.

- **Manage Devices:** HPCA administrators and operators can manage multiple and individual OOB devices.

Under Out of Band Management, click **Device Management**.

- **Manage Groups:** HPCA administrators and operators can manage groups of vPro devices.

Under Out of Band Management, click **Group Management**.

- **View Alerts:** HPCA administrators and operators can view the alerts generated by provisioned vPro devices if you have an alert subscription to the device.

Under Out of Band Management, click **Alert Notifications**.

3 Security and Compliance Management

The Security and Compliance Management features in HPCA enable you to monitor and manage security vulnerabilities, configuration compliance, and security tool performance across your environment. This chapter includes the following topics:

- [Introduction](#) on page 44
- [HPCA and HP Live Network](#) on page 50
- [License Requirements](#) on page 50
- [Software Prerequisites](#) on page 51
- [How Security and Compliance Management Works in HPCA](#) on page 52
- [Configuring Security and Compliance Management](#) on page 60
- [Common Security and Compliance Management Tasks](#) on page 60
- [Advanced Topics](#) on page 70
- [More Information about Security and Compliance Management](#) on page 80

Introduction

Your HPCA security and compliance management solution includes the following areas:

- [Vulnerability Management](#) on page 44
- [Compliance Management](#) on page 46
- [Security Tools Management](#) on page 49

An overview of each area is provided in this chapter.

Vulnerability Management

Vulnerability management is the process of identifying, locating, and rectifying software security and vulnerability issues in the enterprise. There are three main steps in this process:

- 1 Obtain updated vulnerability definitions and scanner.
- 2 Scan the managed devices in the enterprise for the presence of vulnerabilities.
- 3 Report the vulnerability assessment of the devices scanned, including summary information for the enterprise as a whole.

The following terms are used throughout the HPCA vulnerability management solution:

Table 2 Vulnerability Management Terms

Term	Definition
vulnerability	A weakness in a system, its configuration, or its software that allows an individual to compromise the system's integrity to gain unauthorized access to its resources.
exposure	Exposure can refer to a measurement of the various vulnerabilities in an environment. It also can be used to refer to a piece of software that provides information or capabilities that a hacker might use to attack or exploit a system.

Table 2 Vulnerability Management Terms

Term	Definition
CVE	<p>Common Vulnerabilities and Exposures</p> <p>The CVE is a dictionary of common names (CVE Identifiers) for publicly known information security vulnerabilities and exposures.</p> <p>The CVE was started in 1999. It is currently sponsored by the United States Department of Homeland Security and managed by the MITRE Corporation.</p> <p>For more information, refer to http://cve.mitre.org</p>
NVD	<p>National Vulnerability Database</p> <p>The NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.</p> <p>For more information, refer to http://nvd.nist.gov</p>
CVSS	<p>Common Vulnerability Scoring System</p> <p>The CVSS is a standard severity scoring system for information security vulnerabilities. CVSS includes three groups of metrics: Base, Temporal, and Environmental.</p> <p>For more information, refer to http://www.first.org/cvss/index.html</p>

Table 2 Vulnerability Management Terms

Term	Definition
OVAl	<p>Open Vulnerability and Assessment Language</p> <p>OVAl is the standard used to encode and transmit security information and system details. It is based on three XML schemas that represent the three security vulnerability assessment process steps: representing system configuration, expressing a specific machine state, and reporting the results of the assessment.</p> <p>The purpose of the CVE is to catalog all known vulnerabilities. The purpose of OVAl is to describe how to identify specific vulnerabilities. Most OVAl definitions are based on a CVE, but some are not. HP Live Network transmits information in OVAl and CVE format to HPCA.</p> <p>For more information, refer to http://oval.mitre.org/oval/about</p>

Compliance Management

Compliance management is the process of identifying, locating, and rectifying software configuration problems on managed client devices in the enterprise. There are three main steps in this process:

- 1 Obtain updated compliance benchmarks and scanner.
- 2 Scan the managed client devices in the enterprise to determine whether their configuration is in or out of compliance with the pertinent policy or regulatory standard defined by the compliance benchmarks.
- 3 Report the results of the compliance scans, including summary information for the enterprise as a whole.

At this point, the administrator can take steps to resolve any configuration issues identified.

The following terms are used throughout the HPCA compliance management solution:

Table 3 Compliance Management Terms

Term	Definition
CCE	<p>Common Configuration Enumeration</p> <p>The CCE is a dictionary of names for software security configuration issues (for example, access control settings and password policy settings). By providing unique identifiers for system configuration issues, the CCE facilitates fast and accurate correlation of configuration data across multiple information sources and tools.</p> <p>The CCE is currently managed by the MITRE Corporation.</p> <p>For more information, refer to http://cce.mitre.org</p>
FDCC	<p>Federal Desktop Core Configuration</p> <p>The FDCC is a security configuration mandated by the Office of Management and Budget (OMB) for all U.S. government agencies. The FDCC currently exists for Microsoft Windows Vista and XP operating system software.</p> <p>The Windows Vista FDCC is based on the <i>Microsoft Security Guide for Vista</i>, which was developed through a collaborative effort of the Defense Information Security Agency (DISA), the National Security Agency (NSA), and NIST. The guide reflects the consensus recommended settings from DISA, NSA, and NIST for the Windows Vista platform.</p> <p>The Windows XP FDCC is based on a U.S. Air Force customization of the Specialized Security-Limited Functionality (SSLF) recommendations in NIST SP 800-68 and Department of Defense (DoD) customization of the recommendations in <i>Microsoft's Security Guide for Internet Explorer 7.0</i>.</p> <p>There are also FDCC benchmarks for Windows XP Firewall, Windows Vista Firewall, and Internet Explorer 7.</p> <p>For more information, refer to http://nvd.nist.gov/fdcc</p>

Table 3 Compliance Management Terms

Term	Definition
SCAP	<p>Security Content Automation Protocol (pronounced ess-kap)</p> <p>SCAP is a framework of interoperable and automatable security standards established by the National Institute of Standards and Technology (NIST). SCAP enables organizations to automate security monitoring, vulnerability management, and security policy compliance evaluation.</p> <p>SCAP incorporates the following specifications:</p> <ul style="list-style-type: none">• CVE (see Vulnerability Management on page 44)• CCE (see above)• Common Platform Enumeration (CPE), a naming convention for hardware, operating system (OS), and application products• Extensible Configuration Checklist Description Format (XCCDF), an XML specification for structured collections of security configuration rules used by OS and application platforms• OVAL (see Vulnerability Management on page 44)• CVSS (see Vulnerability Management on page 44) <p>Because SCAP uses XML-based standards, SCAP content is both human and machine readable.</p> <p>NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD).</p> <p>For more information, refer to http://nvd.nist.gov/scap.cfm</p>

SCAP provides a way to group a set of compliance requirements into something known as a **benchmark** (for example, FDCC-Windows-Vista). Benchmarks can be revised. A benchmark is given a new version when it is revised.

Each set of SCAP requirements are further refined to a specific **profile**, which may be used to define different levels of compliance within a benchmark. When a compliance scan is run on a client device, it evaluates the requirements for a specific benchmark's profile.

The profile requirements are defined as an **SCAP rule**. Each rule includes one or more automated tests that are used to determine whether or not a client device meets the requirements specified by that profile's rule. Each rule is assigned a weight based on the potential impact and exposure to the enterprise if client devices do not comply with that rule. When a compliance scan is performed on a client device, a score is determined that reflects how many compliance rules passed and failed. This score represents a device's compliance with respect to a particular benchmark profile (SCAP checklist).

The benchmark, profiles, and rules are all delivered as a bundle of files called an **SCAP datastream**. These files are read by SCAP-capable tools, such as the HPCA compliance scanner.

Security Tools Management

HPCA has the ability to scan the managed client devices in your enterprise to determine what types of security tools are present and to collect pertinent information regarding the products detected. The following types of security products are supported:

- Anti-spyware tools
- Anti-virus tools
- Software firewalls

HPCA determines which specific security products are installed, which are enabled, when the most recent anti-virus and anti-spyware scan was performed on each client device, and when virus and spyware definitions were most recently updated on the client devices.

The collected information is then aggregated and displayed in the Security Tools Management dashboard and related reports.

HPCA is integrated with HP Live Network, which provides an executable security tool scanner. This scanner is updated via HP Live Network whenever support for new security products are added.

The security tools management scanner contains embedded knowledge about various security products. It is updated whenever new products are added to the list of products that it can detect.

HPCA and HP Live Network

Your HPCA installation comes with a small subset of the HP Live Network security and compliance management content for demonstration purposes. To obtain updated definitions and scanners—and use the security and compliance management features in the HPCA Console—you must purchase and activate an HP Live Network subscription. You will then receive a user ID, password, and content server URL that you can use to configure the Live Network settings on the Configuration tab.



The HP Live Network content server URL that you receive with your subscription may be different than the default URL shown on the Live Network settings configuration page. Use the URL that comes with your subscription.

After you receive your HP Live Network credentials, you can configure your Live Network settings. See [Live Network](#) on page 281 for details.

See your HP representative for more information about purchasing an HP Live Network subscription.

License Requirements

To use the vulnerability management, compliance management, and security tools management features in HPCA, you will need the following:

- License for the HPCA Security and Compliance Manager
- Subscription to the HP Live Network and valid login credentials
- License for the HPCA Patch Manager

If you do not have these items, the pertinent dashboards will be empty. The first two items are required for the vulnerability management, compliance management, and security tools management dashboards. The Patch Manager license is required for the patch management dashboard.

Additional [Software Prerequisites](#) are also required by the dashboards.



The demo scanning services included with your HPCA software does not require HP Live Network credentials. This demo does not include a scanner for security tools management, however. You must have an active HP Live Network subscription to perform security tools management in HPCA.

Software Prerequisites

At a minimum, the HPCA security and compliance management solution requires the following prerequisites:

- The Configuration Server and Configuration Server Database (CSDB) must be installed and properly configured.
- The Messaging Server must have the `core.dda` module enabled. Along with inventory data, collected scan results are handled by the `core.dda`. Refer to the *Messaging Server Guide* for instructions.
- The following report packs must be enabled for full dashboard capability:
 - The Inventory Management report pack drives the Inventory Management reports and the HPCA Operations dashboard.
 - The Vulnerability Management report pack drives the Vulnerability Management reports and dashboard.
 - The Compliance Management report pack drives the Compliance Management reports and dashboard.
 - The Security Tools Management report pack drives the Security Tools Management reports and dashboard.
 - The Patch Management report pack drives the Patch Management reports and dashboard.

Refer to the *Reporting Server Guide* for information about enabling these report packs.



In a Core and Satellite installation, the prerequisites listed here are automatically addressed.

In a classic (traditional) CAE installation, you must explicitly ensure that all these prerequisites are satisfied.

How Security and Compliance Management Works in HPCA

HP Client Automation offers a security and compliance management solution that enables you to detect security vulnerabilities and configuration policy compliance issues on managed client devices in your enterprise. This solution enables you to quickly assess the severity and scope of the related risk. You can then take steps to remediate problems identified.

HPCA is integrated with the HP Live Network, a subscription service that tracks, triages, and analyzes the latest security vulnerability and regulatory compliance information available. See [Figure 1](#) on page 55.

You can use the HPCA Console to configure HPCA to automatically download new security and compliance content from the HP Live Network on a periodic basis, rather than depending on a manual process. This content includes the following:

- Security and compliance scanners for client devices
- Detailed information about individual vulnerabilities, including descriptions, disclosure dates, severity levels, and available vendor patches or bulletins
- The current FDCC SCAP data stream available from NIST

The HP Live Network content is then pushed to the Configuration Server Database (CSDB) as deployable services, and managed client devices can be subsequently scanned for security and compliance issues according to the schedule and policy that you specify. This content is also pushed to the Reporting database.

The HPCA Console provides dashboards that show the security and compliance status of your enterprise at a glance. It also provides a Patch Management Dashboard to help you quickly assess patch policy compliance across the enterprise. For more information, see [Using the Dashboards](#) on page 83.

For HPCA 7.50, security and compliance scanning is supported for managed client devices with the following operating systems:

Table 4 Platforms Supported

Scan Type	Supported Operating Systems
Vulnerability	Windows 2000, Windows 2003, Windows 2008, Windows XP, and Windows Vista
Compliance	Windows XP and Windows Vista (because the FDCC standard pertains only to desktop devices)
Security Tools	Windows XP, Windows Vista, Windows 2003, and Windows 2008

How HP Live Network Content is Updated

HP Live Network provides two types of security and compliance management content:

- Data – vulnerability definitions and SCAP data
- Scanners – a vulnerability scanner, a compliance scanner, and a security tools management scanner

In order to access the HP Live Network content, HPCA uses the HP Live Network Connector. The Connector first determines what content is available and then downloads the appropriate content from the HP Live Network subscription site.

A default version of the HP Live Network Connector is installed and configured when HPCA is installed. It is self-updating. Any changes to the connector are automatically downloaded when you update your HP Live Network content.

If you want to re-install the HP Live Network Connector for any reason, you can download a new copy at any time. See [Download the HP Live Network Connector](#) on page 236.



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

When you update your HPCA security and compliance management content - either from HP Live Network or from the file system - the following three things happen:

- 1 Both the updated scanners and data are copied into a temporary directory.
- 2 The data is pushed from the temporary directory to the Core database. This drives the detailed definition reports and primes the database for processing the collected scan results.
- 3 Both the data and scanners are loaded into the CSDB.

When a client device with a configured security policy subsequently makes a connection to the SECURITY Domain in the CSDB, the data and scanners are deployed to that client device. At this point, the client device will be scanned. The results of the scans are then sent to the Core database.

Figure 1 Security and Compliance Management in HPCA



- 1 Updated security and compliance content is downloaded and analyzed by the HP Live Network team. The HP Live Network scanners are updated, if necessary (this is rare).
- 2 Updated security and compliance content, including the HP Live Network scanners, is downloaded by HPCA from HP Live Network and published to the CSDB and the Core database.
- 3 Client devices are scanned for security and compliance problems by HPCA.

The security and compliance content that is loaded into the CSDB includes both “service” definitions and “master” definitions. The service definitions are related to the scanning services and are deployed to the platform-specific agents for performing the scans. The master definitions are used when you move content from a test environment to a production environment (see [Move HP Live Network Content from a Test Environment to a Production Environment](#) on page 78).

For vulnerability scanning, the master definitions include the National Vulnerability Database (NVD) CVE definitions and the platform-specific Open Vulnerability Assessment Language (OVAL) definitions required by HPCA. It is the combination of these two sets of definitions for each platform that enable HPCA to create the Vulnerability Management reports.

For compliance scanning, the master definitions include the compliance benchmarks in SCAP format.

For security tools management scanning, there are no definitions. The scanner simply looks for the presence of all supported security tools and determines whether each tool is enabled. For anti-virus and anti-spyware tools, the scanner also determines when each tool last updated its definitions and when it last performed a full system scan.

Scanning Services in Detail

The Configuration Server Database (CSDB) contains a SECURITY Domain, which includes the services responsible for security and compliance scanning. When you install HPCA, the following services are available in the SECURITY domain:

<Discover Vulnerabilities (Limited Edition)>

<Discover FDCC 1.0 OS Compliance>

As you perform HP Live Network content updates, additional services become available. You can use these services to run security and compliance scans on an agent system and send the results back to the Reporting database.

- ▶ The security tools management scanning service is not available until you perform your first HP Live Network content update.

<Discover Security Tools>

- ▶ When you perform your first HP Live Network content update, the vulnerability scanner service is renamed:

<Discover Vulnerabilities>

The version of the scanner shipped with HPCA is labeled “limited edition,” because it contains only a subset of the vulnerability definitions. When you perform your first update, the complete set of definitions known to HPCA becomes available for scanning.

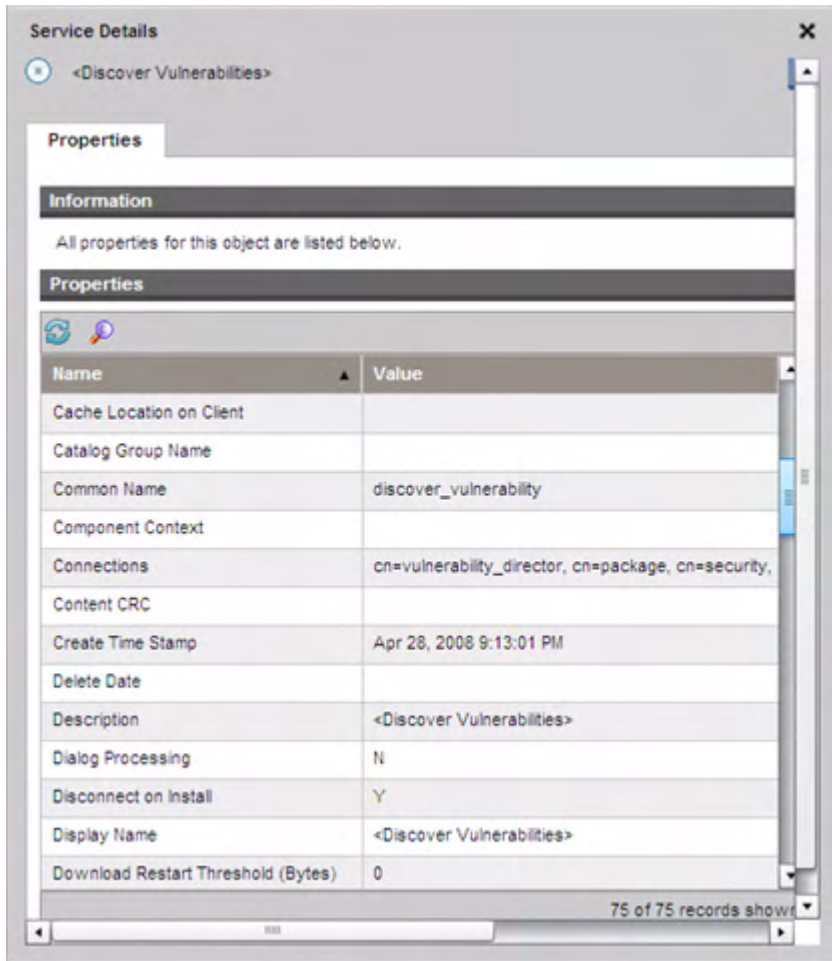
Although the name of the service changes, any entitlements that you have established do not change.

To view the scanning services:

- 1 Sign in to the HPCA Console.
- 2 Click the **Management** tab.
- 3 In the left pane, click **Services**. The list of available CSDB domains opens.
- 4 In the left pane, click **Security**.
- 5 In the Catalog pane, click one of the Security services. For example:
 - SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
 - SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS

— SECURITY.ZSERVICE.DISCOVER_SECTOOLS_AV_AS_FW

The Service Details window opens. For more information about services, see [Service Information](#) on page 153.






This image shows the DISCOVER_VULNERABILITY service. The DISCOVER_SECTOOLS_AV_AS_FW service for security tools management and the compliance management services, such as DISCOVER_FDCC_1-0_OS, are similar.

The CSDB initially contains an instance of PRIMARY.SECURITY.ZSERVICE called <Discover Vulnerabilities (Limited Edition)> for vulnerability scanning and another instance called <Discover FDCC 1.0 Compliance> for compliance scanning. As other benchmarks are added to the HP Live Network content, new instances will become available. After you perform your first HP Live Network update, the <Discover Security Tools> service is added.

The CSDB also contains an instance of PRIMARY.SECURITY.TIMER called Daily Vulnerability Scan, which determines when the vulnerability scanner is executed on target systems. Although they are separate instances, the <Discover Vulnerabilities> service has a connection to the Daily Vulnerability Scan timer.

▶ There is no built-in timer for compliance or security tools scanning. You must set up a DTM job to schedule regular compliance and security tools scans on your target devices. See [Create an HPCA Job to Schedule or Trigger a Scan](#) on page 63. Alternatively, you can set up your own compliance scanning timer in the CSDB.

The following example is a snapshot of the Admin CSDB Editor showing a subset of the parameters for the Daily Vulnerability Scan service:

 ZSCHDEF	Timer Parameter	DAILY(&ZSYSDATE,08:30:00,16:30:00)
 ZSCHTYPE	Type [IMMEDIATE/DEFERRED]	DEFERRED
 ZSCHFREQ	Frequency [PERIODIC/ONCE/RANDOM]	RANDOM

The timer does not directly invoke the scanner. When the timer expires, radskman performs a connect operation to the SECURITY Domain. This causes one of the following methods to be executed: ZCREATE, ZVERIFY, ZUPDATE, or ZREPAIR. When any of these methods is executed, the scanner is launched on the target system.

By default, the timer is configured to run daily at a randomly selected time between 08:30 and 16:30 local (system) time.

▶ You must explicitly entitle your target devices to the scanning services before you can use them. See [Schedule or Trigger a Scan](#) on page 61 for more information.

Configuring Security and Compliance Management

See [Live Network](#) on page 281.

Common Security and Compliance Management Tasks

This section contains information about the following tasks:

- [Update HP Live Network Content](#) on page 60
- [Schedule or Trigger a Scan](#) on page 61
- [View the Results of a Scan or Update](#) on page 65
- [Find Vulnerability Remediation Information](#) on page 65
- [Find Information about Compliance Failures](#) on page 67
- [Find Information About Security Tools](#) on page 69

Update HP Live Network Content

There are two ways to update your HP Live Network content (scanners and data) from the HP Live Network subscription web site:

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

See [Live Network](#) on page 232 for detailed instructions.

- Use the `content-update.bat` command line utility to manually trigger an update.

See [Use the Command Line Utility](#) on page 70 or for instructions.

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



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

Schedule or Trigger a Scan

You can use the HPCA Console to schedule a periodic vulnerability scan, compliance scan, or security tools scan – or any combination of the three – on a target device (or group of devices). You can also trigger an immediate scan. There are two steps required:

- 1 Entitle a device (or group of devices) to one or more of the Security services. When you install HPCA, the following two services are available in the SECURITY domain:

<Discover Vulnerabilities (Limited Edition)>

<Discover FDCC 1.0 OS Compliance>

As you perform HP Live Network content updates, additional services become available as new benchmarks are added. After you perform your first update, the vulnerability service is renamed, and the (Limited Edition) qualifier is deleted. The <Discover Security Tools> service also becomes available after your first content update.

See [Entitle A Device for Scanning](#) on page 62.

- 2 Schedule or trigger a scan from the HPCA Console by creating a job using the Security Connect job action template. See [Create an HPCA Job to Schedule or Trigger a Scan](#) on page 63.


You can also trigger an immediate scan on a single device by performing an agent connect operation from that target device to the SECURITY Domain in the CSDB. Scans are triggered whenever an agent connect operation from a properly entitled target device to the SECURITY Domain in the CSDB occurs. See [Start a Scan from a Target Device](#) on page 64.

For information about how HPCA performs a scan, see [Scanning Services in Detail](#) on page 57.

Entitle A Device for Scanning

Before you can initiate a vulnerability, compliance, or security tools scan on a managed client device (or group of devices), you must properly entitle the pertinent devices to the desired scanning services.

To entitle a device (or group of devices) for scanning:

- 1 On the Management tab, expand the zone containing the devices that you want to entitle.
- 2 In the left navigation tree, click **Devices** if you want to entitle a single device. If you want to entitle a group of devices, click **Group**.
- 3 From the shortcut menu for the device or group that you want to entitle, select **View/Edit Properties**. A new window Directory Object window opens.
- 4 In the left navigation tree, click **Policies**.
- 5 Click the Launch Policy Management () button to open the Policy Management Wizard.
- 6 From the Service Domain list, select **Security**.
- 7 Select the box to the left of one or more of the Security services. The following services are available “out of the box” when you install HPCA:
 - SECURITY.ZSERVICE.DISCOVER_VULNERABILITY
 - SECURITY.ZSERVICE.DISCOVER_FDCC_1-0_OS
 - Additional Security services become available after you perform a HP Live Network update.

The SECURITY.ZSERVICE.DISCOVER_SECTOOLS_AV_AS_FW service, for example, is available after your first update.
- 8 Click **Add to Selection**.
- 9 Click **Next**.
- 10 Under Policy Configuration, select **Allow**.
- 11 Under Priority, select the priority that you want the scans to have on the managed client device (or devices) when it runs.
- 12 Click **Next**.
- 13 Review the settings for the service (or services). If you want to change a setting, click **Previous**. When you are ready to proceed, click **Commit**.

- 14 Click **Close** to close the Execution Status dialog box.

Create an HPCA Job to Schedule or Trigger a Scan

To schedule or trigger a security or compliance scan on one or more target devices from the HPCA Console, you must create a job for those devices. When a job created with the Security Connect job action template runs, all services in the SECURITY domain to which these devices are entitled are executed.

To create a job to schedule or trigger a scan:

- 1 On the Management tab, expand the zone containing the devices that you want to scan.
- 2 In the left navigation tree, click **Devices** if you want to scan a single device. If you want to scan a group of devices, click **Group**.
- 3 From the drop-down menu for the device or group that you want to scan, select **Create a Job** to open the job creation wizard.

In the wizard, required fields are marked with an asterisk (*).

- 4 From the **Job Type** list, select either **DTM** or **Notify**.

In a DTM job, the agents on the target devices connect to the HPCA Core server to get a list of jobs and then execute those jobs when the job timers expire. A DTM job is most appropriate when you want to set up a regular scanning schedule for these devices.

In a Notify job, the HPCA Core server asks agent to perform the scan. A Notify job is most appropriate when you want certain target devices to perform a single scan at a specific time – or immediately.

- 5 Specify a **Name** for the job.
- 6 Specify a **Job Description**.
- 7 From the **Job Action Template** list, select **Security Connect**.
- 8 Click **Next**.
- 9 Specify the schedule for the job. See [Schedules](#) on page 161 for more information.

DTM jobs can be executed either once or on a regular schedule. Notify jobs can only be executed once, so many of the schedule settings are disabled on this page of the wizard.

- 10 Review the settings for your job. To view the devices that will be scanned, click **View Targets**. If you want to change any settings, click **Previous**. When you are ready to proceed, click **Submit**.
- 11 Click **Close** to close the Execution Status dialog box.

For more information about HPCA jobs, see [Managing Jobs](#) on page 158.

Start a Scan from a Target Device

To install the latest security and compliance management content and trigger an immediate scan on a client device, you can simply perform a client connect from that device to the SECURITY Domain in the CSDB.

To perform an agent connect to the SECURITY Domain:

On a managed client device, open a command line window, and execute the following command:

```
radskman dname=security,context=m,uid=$machine,cop=y
```

This command triggers an update to all the services in the SECURITY domain, including the security and compliance management services, to which the client device is entitled.

To trigger *only* a vulnerability scan, add the following parameter to the radskman command:

```
sname=DISCOVER_VULNERABILITY
```

To trigger *only* a compliance scan, add an sname parameter for the compliance service that you want to trigger to the radskman command. For example:

```
sname=DISCOVER_FDCC_1-0_OS
```

To trigger *only* a security tools scan, add the following parameter to the radskman command:

```
sname=DISCOVER_SECTOOLS_AV_AS_FW
```

Remember to separate the radskman options with commas but *not* spaces.



Uninstalling the management agent on a client device does not remove the scanners. To remove the security service, first remove the policy, and then perform a client connect to remove the service. Do this before you uninstall the agent.

View the Results of a Scan or Update

You can use the reports available in the HPCA Console to view the results of a vulnerability, compliance, or security tools scan. You can also view the status of HP Live Network content updates. You can filter the reports to see only the information that interests you. See [Using Reports](#) on page 203 for more information.

You can also use the dashboards to find summary information in either chart or grid format. See [Using the Dashboards](#) on page 83 for more information.

Find Vulnerability Remediation Information

By using the Vulnerability Management reports or dashboard, in many cases you can find a link to a vendor bulletin containing remediation information for a particular vulnerability. Sometimes this information is strictly advisory, and sometimes it includes a software patch for the affected application or operating system.

There are many ways to find the vendor bulletin for a specific vulnerability. The following procedures describes two simple ways to do this.

To find guided remediation information for a particular vulnerability:


- 1 On the Reporting tab, expand the list of Vulnerability Management reports.
- 2 Open a report that lists vulnerabilities, such as the Top Vulnerabilities or Application Vulnerabilities report.
- 3 Click the **CVE ID** or **OVAL Definition** for a particular vulnerability. A new report, which includes patch and advisory information, opens for this vulnerability.




If the status of a particular vulnerability is Unknown, and the CVSS score is null, be sure to investigate this vulnerability thoroughly by using the NVD, the CVE repository, and any other resources at your disposal. In this situation, HPCA may be unable to provide the information that you need to make an informed decision regarding the issue.

- 4 Click the link in the **Bulletin** column if you want to go to the vendor's site.

To find guided remediation information for a particular device:

- 1 On the Reporting tab, expand the list of Vulnerability Management reports.
- 2 Under Device Reports, click **Scanned Devices**.
- 3 Click the Details () icon for a particular device. The following reports open for this device:
 - Device Details
 - Device Vulnerability Details

You can filter the Device Vulnerability Details report by Severity or OVAL Definition ID. See [Filtering Reports](#) on page 219 for more information.

- 4 Click the Details () icon for a particular vulnerability. The following reports open:
 - Vulnerability Details
 - Vulnerability Remediation Details

You can filter the Vulnerability Remediation Details report by Severity, Vendor, or CVE ID.

- 5 Click the link in the **Bulletin** column if you want to go to the vendor's site.


If the bulletin includes a patch, you can use the Patch Management features in the HPCA Console to entitle the pertinent devices to that patch. .

In addition to the methods described here, you can also drill down to a specific vulnerability report through certain [Vulnerability Management Dashboard](#) panes.

Find Information about Compliance Failures

You can use the Compliance Management reports to drill down to detailed information about specific rules that failed on a particular device during the most recent compliance scan.


To view details for one of the ten most noncompliant devices:

- 1 On the Reporting tab, expand the list of Compliance Management reports.
- 2 Under Executive Reports, click **Top SCAP Noncompliant Devices**.
- 3 Click the Switch to Detailed View () icon to display the data in table format. Each row in the table corresponds to the test results for a particular compliance benchmark on a particular device.
- 4 Click a value in the **Rules Failed** column. A list of any compliance rules associated with this benchmark that failed for this device is displayed.

To view details about the compliance test results for any device:

- 1 On the Reporting tab, expand the list of Compliance Management reports.
- 2 Under Device Reports, click **Scanned Devices**.

Each row in the table corresponds to the test results for a particular compliance benchmark on a particular device.

- 3 Click the Details () icon in any row. The following reports open for the pertinent benchmark and device:
 - Device – information about the device itself, including hardware, IP address, and operating system
 - Benchmarks by Device – each row represents a benchmark tested on this device
- 4 In the Benchmarks by Device report, click a value in one of the following three columns:
 - **Rules Passed**

A list of any compliance rules associated with this benchmark that passed for this device is displayed.
 - **Rules Failed**

A list of any compliance rules associated with this benchmark that failed for this device is displayed.

— **All Other Rule States**

A list of compliance rules that neither failed nor passed for this device. This counter is incremented when a test returns one of the following codes:

- ERROR
- UNKNOWN
- NOT_APPLICABLE
- NOT_CHECKED
- NOT_SELECTED
- INFORMATIONAL
- FIXED

In addition to the methods described here, you can also drill down to detailed information by using certain [Compliance Management Dashboard](#) panes.

Find Information About Security Tools

HPCA gives you the ability to discover anti-virus, anti-spyware, and firewall tools running on your devices. The Security Tools Management dashboards and reports provide the following information:

Table 5

Security Tool	Information Available
Anti-virus	Name and version of the product installed Whether the tool is currently enabled Last time the tool performed a full system scan Last time the virus definitions were updated Specific version of the current definitions
Anti-spyware	Name and version of the product installed Whether the tool is currently enabled Last time the tool performed a full system scan Last time the spyware definitions were updated Specific version of the current definitions
Firewall	Name and version of the software firewall installed Whether the firewall is enabled Rules used by that firewall (As of the HPCA 7.50 release date, this applies to Windows XP SP2 or later and Windows Vista firewalls only.)

See the following topics for more detailed information:

- [Security Tools Management Dashboard](#) on page 125
- [Security Tools Management Reports](#) on page 215

Unlike compliance or vulnerability management, security tools management does not require you to download extra “definition” files. All of the knowledge about gathering information regarding security tools installed on a device are embedded in the scanner. As necessary, HP Live Network updates the scanner to support newly released security tools (anti-virus, anti-spyware, and firewalls).

Advanced Topics

This section addresses topics that, while fully supported, are outside the typical scope of daily security and compliance management activities. The following topics are included:

- [Use the Command Line Utility](#) on page 70
- [Run the HP Live Network Connector Manually](#) on page 76
- [Move HP Live Network Content from a Test Environment to a Production Environment](#) on page 78

Use the Command Line Utility

As an alternative to using the HP Live Network page under on the Operations tab to schedule or trigger a HP Live Network content update, you can use the `content-update.bat` command-line utility located in the following directory:

```
<InstallDir>\HPCA\VulnerabilityServer\bin
```

Note that this directory is not automatically placed in your PATH when HPCA is installed.

This utility has the following syntax:

```
content-update.bat [-settingName <settingValue>]...
```

This command has both [Required Settings](#) and [Optional Settings](#). Note that you must always specify a value for the `content_source` setting.

Any values that you specify on the command line override the stored configuration settings specified elsewhere (see [Stored Settings](#) on page 75). If you do not specify a value for a particular setting, the stored configuration setting is used.



The `content-update` command writes status and error messages to the `vms-commandline.log` file.

See [Examples](#) on page 75 for typical uses of the `content-update.bat` command.

Required Settings

The following table lists the required settings for the `content-update.bat` command.

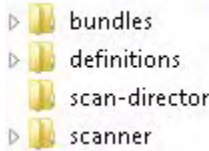


Any values that you specify on the command line override the stored configuration settings that were specified elsewhere (see [Stored Settings](#) on page 75). If you do not specify a value for a particular setting, the stored configuration setting is used.

Table 6 Required Settings for content-update.bat

Setting	Description
<code>content_source</code>	<p>This setting is required. It specifies the source for the updated content. This must be one of the following:</p> <p>LIVENETWORK – Acquire the content from the HP Live Network subscription site by using the HP Live Network Connector. The HP Live Network settings and the path to the downloaded Connector must be properly configured for this option to work. See Live Network on page 281.</p> <p>FILESYSTEM – Acquire the content from a location in the file system. The content must have previously been downloaded from HP Live Network to this file system location. The <code>content_path</code> setting must also be specified, either on the command line or on the HP Live Network page under Infrastructure Management on the Operations tab. See Live Network on page 281.</p> <p>CSDB_MASTER – Acquire the content from master content previously published to the configuration server database (CSDB). This data will be used to load the Reporting database. Service deployment content will NOT be republished. This is intended for use when a test configuration server Security deck has been imported into a production configuration server. See Advanced Topics on page 70.</p>

Table 6 Required Settings for content-update.bat

Setting	Description
content_path	<p>The fully qualified path to the file system location containing the content that you manually obtained from HP Live Network. This setting is only required if you specified FILESYSTEM as the content_source.</p> <p>This path can specify either a directory or a ZIP archive file. The directory structure (or ZIP file structure) must exactly match the structure of directories and files created when an automatic HP Live Network update is performed:</p>  <p>You must also replicate the sub-directories under these folders to match the automatic update structure.</p> <p>In some cases, HP Live Network updates only a subset of the content. In this case, some of these directories may not be delivered during a HP Live Network update. In any case, when you update from the File System, your directory structure must match that delivered by HP Live Network.</p>

Optional Settings

The following settings for the `content-update.bat` command are optional.



Any values that you specify on the command line override the stored configuration settings that were specified elsewhere (see [Stored Settings](#) on page 75). If you do not specify a value for a particular setting, the stored configuration setting is used.

Table 7 Optional Settings for content-update.bat

Setting	Description
<code>csdb_host</code>	Configuration Server network addressable system name. This can be a fully qualified host name, localhost, or an IP address.
<code>livenetwork_connector_executable</code>	The fully qualified path to the HP Live Network Connector on the local file system. By default, this is: C:\Program Files\Hewlett-Packard\HPCA\LiveNetwork The HP Live Network Connector is a tool used by HPCA to create a secure connection to the HP Live Network content distribution server and download the updated vulnerability management content.
<code>livenetwork_connector_maxruntimeinminutes</code>	Time (in minutes) that the HP Live Network Connector will be allowed to run before forcing a failure. Minimum value should be 60.
<code>livenetwork_contenturl</code>	URL for the HP Live Network content distribution site. This is the location that the HP Live Network Connector will use to download new content.
<code>livenetwork_username</code>	User name for the HP Live Network subscription.
<code>livenetwork_password</code>	Password for the HP Live Network subscription.
<code>livenetwork_proxy_http_server</code>	HTTP proxy server used to connect to the HP Live Network download site. This option must have the following form: <http https>://<host>:<port>

Table 7 Optional Settings for content-update.bat

Setting	Description
livenetwork_proxy_http_username	User name for the HTTP proxy server, if any, used to connect to the HP Live Network download site.
livenetwork_proxy_http_password	Password for the HTTP proxy server, if any, used to connect to the HP Live Network download site.
reporting_db_databasename	Named database instance for the Reporting database (for example: inventory).
reporting_db_drivename	Name of the database driver to use (either <code>oracle</code> or <code>sqlserver</code>). This must map to a supported driver.
reporting_db_server	Network addressable server name where the Reporting database is located.
reporting_db_port	Reporting database port number. This must be empty if the port is dynamic. If the port is static, it must be a value between 1 and 65536.
reporting_db_username	User name for the Reporting database.
reporting_db_password	Password for the Reporting database.

Stored Settings

If you do not specify a value for one of the `content-update` settings, the values specified on the following Live Network configuration pages are used by default:

Table 8 Stored Settings for `content-update.bat`

Option	Where Specified
<code>csdb_host</code> <code>csdb_port</code> <code>csdb_username</code> <code>csdb_password</code>	HPCA First-Time Setup wizard
<code>livenetwork_connector_executable</code> <code>livenetwork_contenturl</code> <code>livenetwork_username</code> <code>livenetwork_password</code> <code>livenetwork_proxy_http_server</code> <code>livenetwork_proxy_http_username</code> <code>livenetwork_proxy_http_password</code>	Live Network page and Proxy Settings page
<code>reporting_db_databasename</code> <code>reporting_db_drivename</code> <code>reporting_db_server</code> <code>reporting_db_port</code> <code>reporting_db_username</code> <code>reporting_db_password</code>	Automatically configured when HPCA is installed

Examples

Example 1 – Perform a content update using the previously configured HP Live Network settings

```
content-update.bat -content_source LIVENETWORK
```

Example 2 – Perform a content update from a local directory

```
content-update.bat -content_source FILESYSTEM -content_path c:\mycontent
```

Example 3 – Perform a content update from a local ZIP file

```
content-update.bat -content_source FILESYSTEM -content_path  
c:\mycontent\content.zip
```

To view full usage information for `content-update.bat`, type the following command from the `<installDir>\bin` directory:

```
content-update.bat -?
```

Run the HP Live Network Connector Manually

In some situations, the HPCA Core server may not have Internet access. In this case, you can still update your HP Live Network content using a system that does have Internet access and then manually transfer the content to the HPCA Core server. This process includes four steps:

- 1 On the system with Internet access, manually download the HP Live Network Connector from the HP Live Network subscription web site. See your HP Software sales representative for instructions.
- 2 Execute the HP Live Network Connector on the system with Internet access.
- 3 Transport the content to the HPCA Core server.
- 4 Update the HP Live Network content from the file system on the HPCA Core server. See [Update HP Live Network Content](#) on page 60.

When you execute the HP Live Network Connector, it creates the folder structure described under `content_path` in [Table 6](#) on page 71 and then stores its output files within this structure.



Important Warning

Before you run the HP Live Network Connector from the command line, make sure that the directory where you will “import” the HP Live Network content is empty before you execute the Connector.

This directory is specified by the following parameter:

```
--setting=hpca.import_directory=<LNC-output-dir>
```

In this case, `<LNC-output-dir>` is the location where the HP Live Network content is placed.

If the “import” directory is not empty, there is a possibility that you will move old content into HPCA when you subsequently use the FILESYSTEM option to update your HP Live Network content. This could have negative repercussions, such as incorrectly deploying an old scanner if a new one is released that has a new name.

This warning applies only when you run the HP Live Network Connector from the command line. It does not affect HP Live Network updates that you perform through the HPCA Console.

To download the HP Live Network content:

Run the following command on the system with Internet access:

```
<LNC-install-dir>\bin\live-network-connector.bat
--url=https://dist.opsware.com
--http-proxy=<http/https://server:port>
--username=<user> --password=<pass> --product=hpca
--setting=hpca.import_directory=<LNC-output-dir>
--stream=security.hpca_scanner
--stream=security.hpca_oval
--stream=security.hpca_nvd
--stream=security.hpca_scap_fdcc
--stream=security.hpca_sectools_scanner
--stream=security.hpca_sectools_services
```

All items in *<brackets>* here are placeholders for values that you must supply.

In this case, *<LNC-install-dir>* is the file system location where you installed the HP Live Network Connector, and *<LNC-output-dir>* is the location where the Connector will create the folder structure that contains its output files. For example, if *<LNC-output-dir>* is *c:\temp*, the folder hierarchy is created under *c:\temp*.

The proxy server settings are only necessary if a proxy server exists between the system hosting the HPCA Console and the HP Live Network subscription site.

Next Steps

After you run the HP Live Network Connector on the system with Internet access, you must manually copy the folder structure to the HPCA core server hosting the HPCA Console. You can place the folder structure either directly in the file system or in a ZIP archive.

At this point, you must tell HPCA where to find this content. There are two ways to do this:

- On the HP Live Network page under Infrastructure Management on the Operations tab, select **From the File System**, and specify the location of the folder structure (or ZIP file).
- From the command line, run the `content-update` command, and specify the `FILESYSTEM` content source. Specify the location of the folder structure (or ZIP file) by using the `content_path` setting.

Move HP Live Network Content from a Test Environment to a Production Environment

You may find it useful to test your HP Live Network content in a small controlled environment prior to performing a large scale rollout. To do this, you will first create a test HPCA environment with its own “test” Configuration Server Database (CSDB) and “test” Reporting database. After completing your testing, you will export the “test” SECURITY Domain and then import that CSDB content into your production HPCA environment.



The files used to export and import CSDB content are called a “deck.”

Before following these procedures, be sure to review [How HP Live Network Content is Updated](#) on page 53.

To test your HP Live Network content in a controlled test environment:

- 1 In the test environment, perform an HP Live Network content update—either automatically from the HP Live Network subscription site, or manually from the file system.
- 2 Test the updates by running scans and reviewing the pertinent reports and dashboard panes.

To move your HP Live Network content from a controlled test environment to a production environment:



In the **raddbutil** commands shown here, there are no spaces after the commas. If you cut and paste these commands from this guide or the online help, be sure to remove any spaces introduced by the paste operation.

- 1 Connect to the test CSDB and use the **raddbutil** tool to export the Security deck:
 - a Go to the Configuration Server **bin** directory on the system where you want to export the data (the test environment).
 - b If the **RAD_MAST** user has a password, use the following command:

```
raddbutil EXPORT DATA=TRUE,WALK=TRUE,  
OUTPUT=<tempDir>,USERID=RAD_MAST,PASSWORD=<password>  
PRIMARY.SECURITY
```

If the **RAD_MAST** user does not have a password, use the following command:

```
raddbutil EXPORT DATA=TRUE,WALK=TRUE,  
OUTPUT=<tempDir>,USERID=RAD_MAST PRIMARY.SECURITY
```

In both cases, *<tempDir>* is the directory where the exported files will be placed on the test CSDB system.

For more information, refer to “Configuration Server Database Utility (RadDBUtil)” in the *Configuration Server User Guide*.

- 2 Transport the Security deck files to the production CSDB system using the file transfer mechanism of your choice.
 - 3 On the production CSDB system, use the **raddbutil** tool to import the Security deck:
 - a Go to the Configuration Server directory on the system where you want to import the data (the production environment).
 - a If the **RAD_MAST** user has a password, use the following command:

```
raddbutil IMPORT INPUT=<tempDir>,COMMIT=TRUE,  
ACCEPT=A+D+U,USERID=RAD_MAST,PASSWORD=<password>
```
- If the **RAD_MAST** user does not have a password, use the following command:

```
raddbutil IMPORT INPUT=<tempDir>,COMMIT=TRUE,  
ACCEPT=A+D+U,USERID=RAD_MAST
```

In this case, *<tempDir>* is the directory on the production CSDB system where the files were placed in [step 3](#).

- 4 In the production environment, load the production Reporting database using the “master” content in the Security deck that you just imported.

There are two ways to do this:

- **Method 1:** Use the HPCA Console
 - a Click the **Operations** tab.
 - b In the left navigation menu, select **Live Network**.
 - c Click the **Update Now** tab.
 - d Select the **From the Configuration Server** update option.
 - e Click the **Update Now** button.

See [Live Network](#) on page 281 for more information about the Update Now tab.

- **Method 2:** Use the `content-update` command-line utility

```
content-update.bat -content_source CSDB_MASTER
```

See [Use the Command Line Utility](#) on page 70 for more information about the `content-update` command.

In either case, using the `CSDB_MASTER` content source forces the update tool to only update the Reporting database content and bypass performing any updates to the packages linked to the vulnerability, compliance, or security tools management scanning services. This ensures that the service content you deployed in your test environment will exactly match the content that you will be deploying in your production environment.

More Information about Security and Compliance Management

The following sections contain information about configuring and viewing security and compliance management information in the HPCA Console:

- [Using the Dashboards](#) on page 83
- [Using Reports](#) on page 203
- [Live Network](#) on page 281

Visit the following web sites to learn more about security and compliance management:

<http://cve.mitre.org>

<http://nvd.nist.gov>

<http://nvd.nist.gov/scap.cfm>

<http://oval.mitre.org>

<http://www.us-cert.gov>

4 Using the Dashboards

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

- [Dashboard Overview](#) on page 84
- [HPCA Operations Dashboard](#) on page 89
- [Vulnerability Management Dashboard](#) on page 96
- [Compliance Management Dashboard](#) on page 115
- [Security Tools Management Dashboard](#) on page 125
- [Patch Management Dashboard](#) on page 134

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 89 shows you how much work is being done by the HPCA infrastructure.
- The [Vulnerability Management Dashboard](#) on page 96 shows you information about any publicly known security vulnerabilities that are detected on the scanned devices in your enterprise.
- The [Compliance Management Dashboard](#) on page 115 shows you how well managed client devices in your environment comply with predefined policies based on established regulations and standards, such as the Federal Desktop Core Configuration (FDCC).
- The [Security Tools Management Dashboard](#) on page 125 shows you information about the anti-spyware, anti-virus, and software firewall products installed on the managed client devices in your enterprise.
- The [Patch Management Dashboard](#) on page 134 shows you information about any patch vulnerabilities that are detected on the devices in your network


Each dashboard includes two views:

Table 9 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 318 for more information.

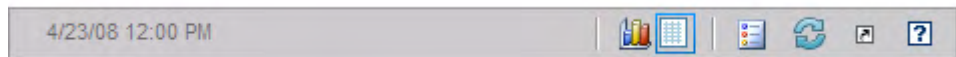
Each dashboard also includes a home page with summary statistics and links to related reports. When you click one of these links, a separate browser window opens, and HPCA displays the report.

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

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

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

Figure 2 Time Stamp



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

If there is no security and compliance management data in the Reporting database—for example, before the first scan has been performed—the dashboard panes do not display any data.

You can perform the following actions in the dashboard panes:

Table 10 Dashboard Pane Actions












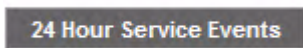
Icon	Description
	Display the information in chart format.
	Display the information in grid format.
	Display the legend for this chart.

Table 10 Dashboard Pane Actions

Icon	Description
	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.
	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 430 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.

In some grid views, trend indicators show you how a particular parameter is trending since the previous scan:

Table 11 Trend Indicators

Icon	Color	Direction	Description
	Red	Up	Parameter has increased; the trend is bad.
	Green	Up	Parameter has increased; the trend is good.
	Red	Down	Parameter has decreased; the trend is bad.
	Green	Down	Parameter has decreased; the trend is good.

For example, in the [Vulnerability Impact by Severity \(pie chart\)](#) on page 97, if the number of High severity vulnerabilities has increased, a red arrow pointing up is displayed. If the number High severity vulnerability has decreased, a green arrow pointing down is displayed.

To assess the trend, HPCA summarizes each day's data at midnight local time. For this reason, the data for the current day is incomplete. The trending indicator is based on the previous two days.

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.

You can also define up to two additional perspectives. See “Adding Custom Dashboard Perspectives and Filters” in the *Enterprise Manager Guide* for detailed instructions.

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



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

Filter or Perspective Not Applicable

Panes that are not affected are also outlined in orange.

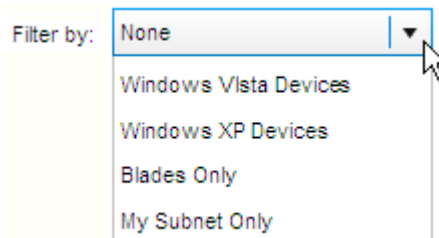
The following dashboard panes are not affected by perspectives:

- [Historical Vulnerability Assessment](#) on page 99
- [Historical Compliance Assessment](#) on page 119
- [Microsoft Security Bulletins](#) on page 139
- [HP Live Network Announcements](#) on page 106

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.

Dashboard Filters

Another way to limit the amount of data displayed in the dashboards is to use a custom Reporting filter that you have created. You can select a filter from the drop-down menu in the upper right corner of the dashboard:



The drop-down menu includes all filters currently defined in the `Console.properties` file. To add a custom filter to this menu, see “Adding Custom Dashboard Perspectives and Filters” in the *Enterprise Manager Guide*.

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 90

[Service Events](#) on page 92

The Executive View also includes the following pane:

[12 Month Service Events by Domain](#) on page 94

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 318.

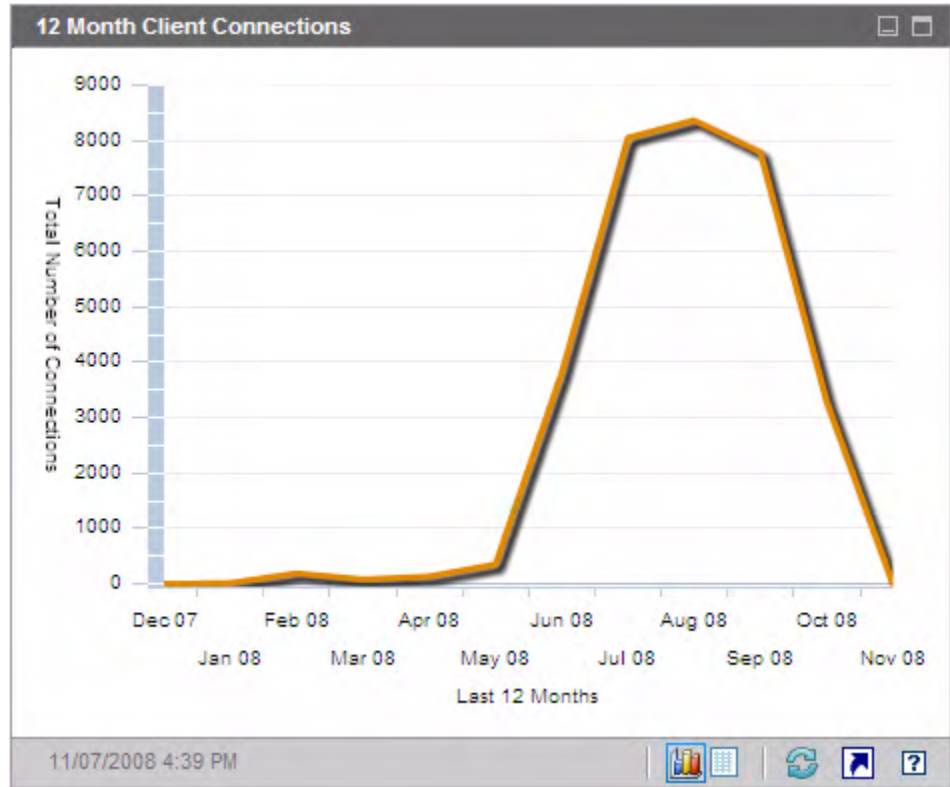


When you click HPCA Operations in the left navigation pane, the HPCA Operations home page is displayed. This page contains statistics and links to pertinent reports.

Client Connections

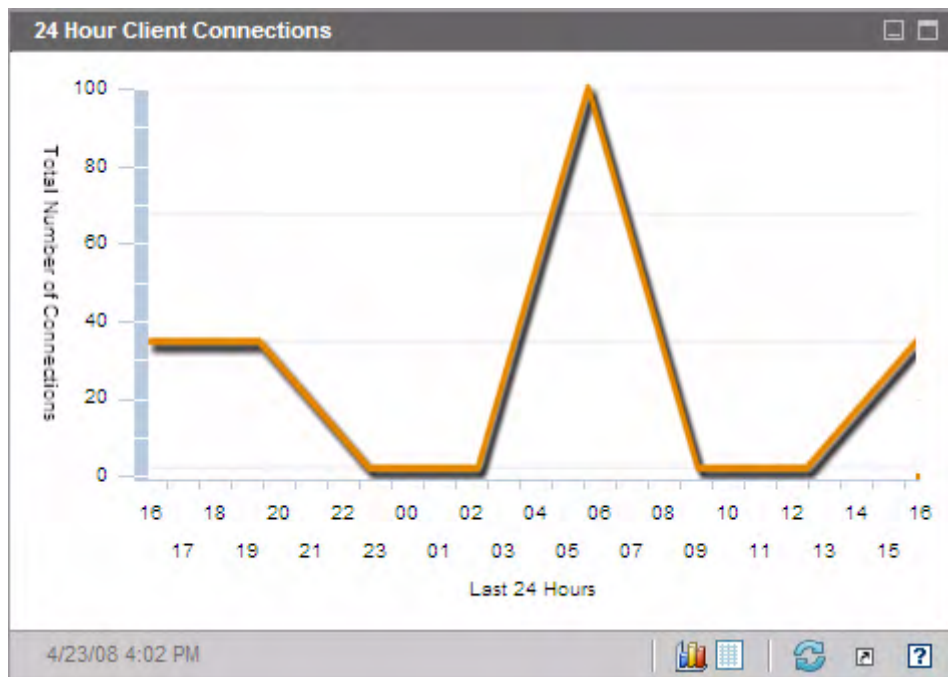
The chart view of this pane shows you the number of HPCA agent client connections that have occurred over the last twelve months (Executive View) or 24 hours (Operational View). When you rest the cursor on a data point, you can see the total number of connections for that month or hour.

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

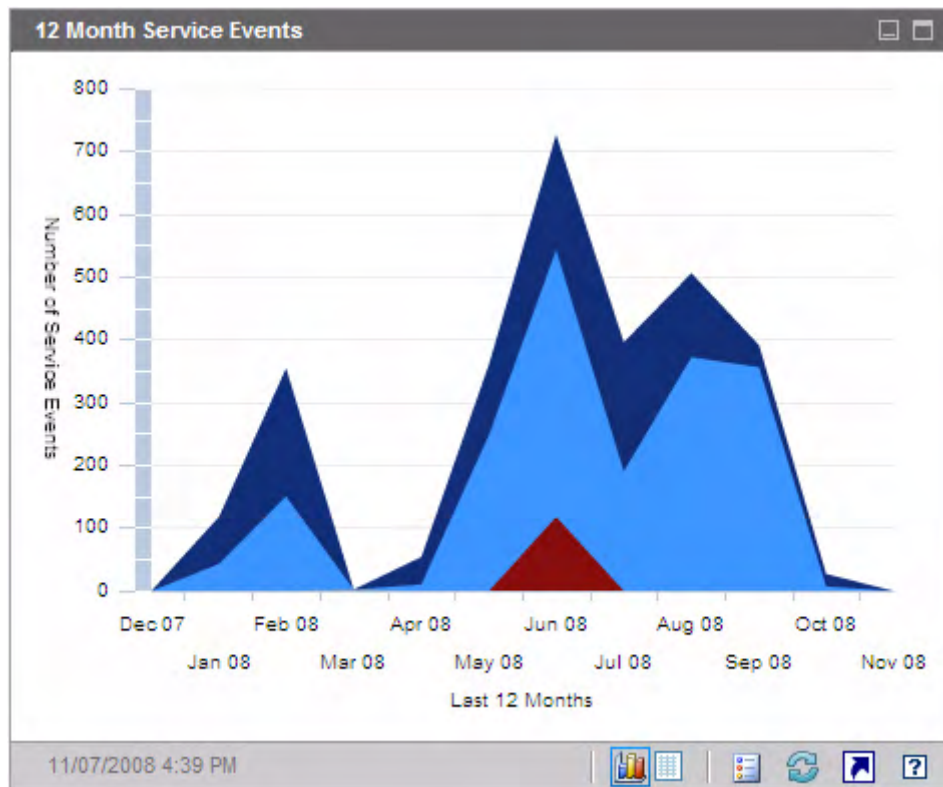
The chart view of this pane shows the number of service events that HPCA has completed over the last twelve months (Executive View) or 24 hours (Operational View) on the client devices in your enterprise. These include the number of applications that HPCA has:

- Installed
- Uninstalled

- Updated
- Repaired
- Verified

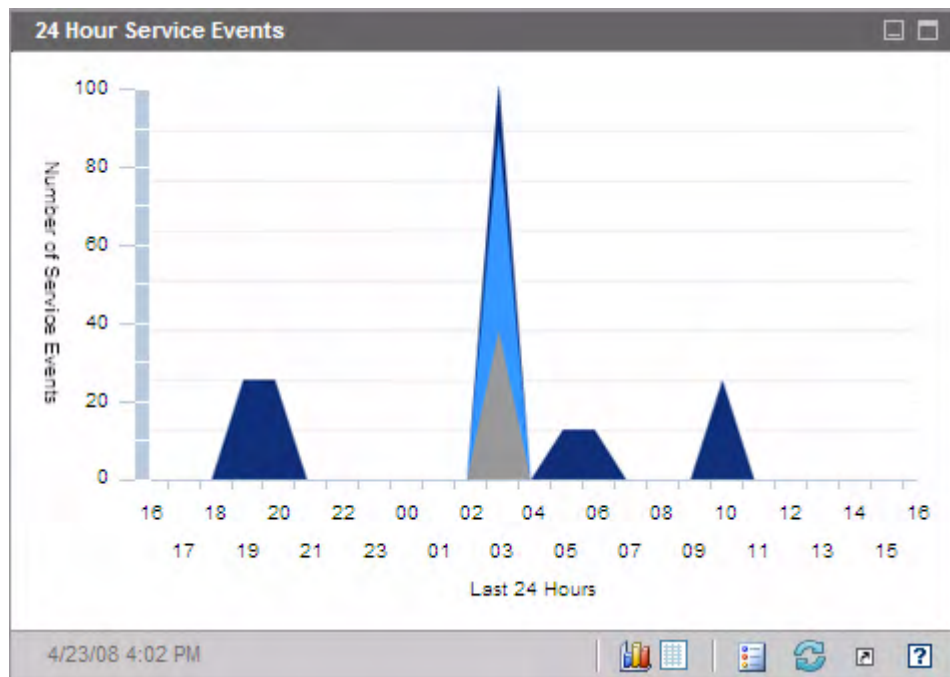
When you rest the cursor on a data point, you can see the number of service events that were completed during a particular month or hour.

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

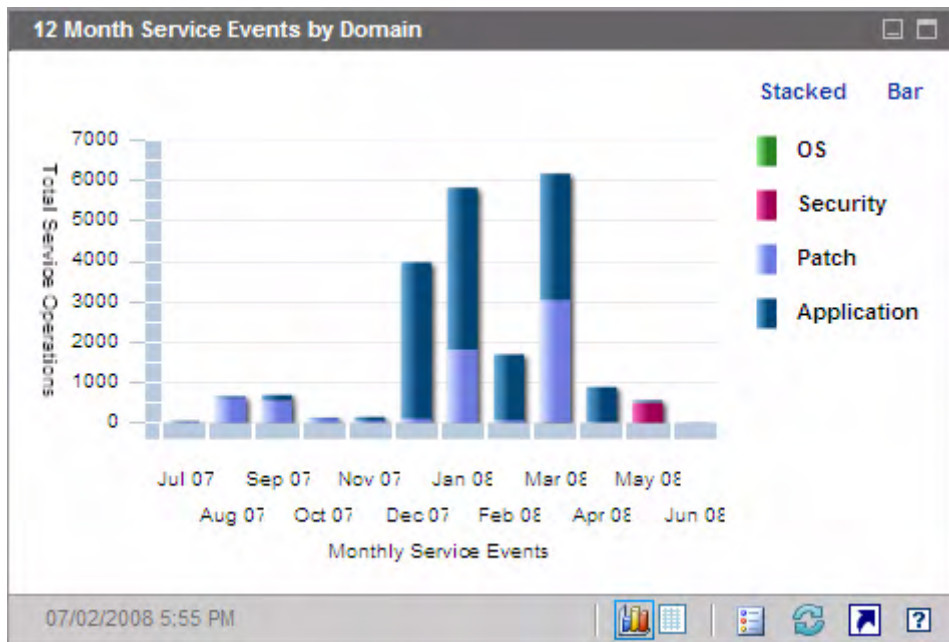
The chart view of this pane shows you how many of each of the following services that HPCA performed during each of the last 12 months:

- 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.

Vulnerability Management Dashboard






HPCA has the ability to collect security vulnerability information for each managed client system in your enterprise. This information is then aggregated and displayed in the Vulnerability Management dashboard.

HPCA is integrated with HP Live Network, which provides updated vulnerability definitions and an executable client scanner.

► For a list of common vulnerability management terms used throughout the Vulnerability Management dashboard and reports, see [Security and Compliance Management](#) on page 43.

HPCA uses the Common Vulnerability Scoring System (CVSS) Base score to place each client device in the enterprise into one of the following severity categories:

Table 12 Severity Categories

Icon	Category	Highest CVSS Base Score for this Device
	High	Between 7.0 and 10
	Medium	Between 4.0 and 6.9
	Low	Less than 3.9
	No Vulnerabilities	No vulnerabilities detected
	Unknown	No data available for this device

The highest severity vulnerability present on a device determines its category. If a device has at least one High severity vulnerability, its category is High. If a device has no High severity vulnerabilities but has at least one Medium severity vulnerability, its category is Medium, and so on.



If the severity of a particular vulnerability is Unknown, and the CVSS score is null, be sure to investigate this vulnerability thoroughly by using the NVD, the CVE repository, and any other resources at your disposal. In this situation, HPCA may be unable to provide the information that you need to make an informed decision regarding the issue.

The Vulnerability Management dashboard Executive View includes the following four information panes:

- [Vulnerability Impact by Severity \(pie chart\)](#) on page 97
- [Vulnerability Impact by Severity \(bar chart\)](#) on page 107
- [Vulnerability Impact](#) on page 101
- [Historical Vulnerability Assessment](#) on page 99

The Operational View includes the following four information panes:

- [HP Live Network Announcements](#) on page 106
- [Most Vulnerable Devices](#) on page 109
- [Most Vulnerable Subnets](#) on page 110
- [Top Vulnerabilities](#) on page 112

You can configure the dashboard to show or hide any of these panes. See [Dashboards](#) on page 318.



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

Vulnerability Impact by Severity (pie chart)

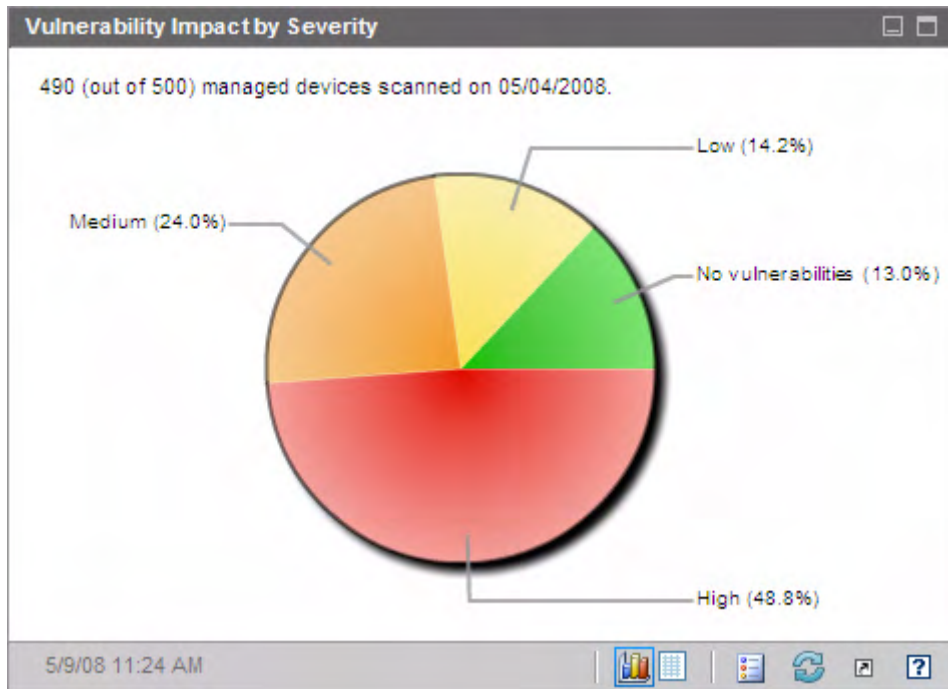
The chart view for this pane shows you the percentage of scanned devices in the enterprise that fall into each of the following five categories based on the highest severity vulnerability detected on each device:

- High (red)

- Medium (orange)
- Low (yellow)
- No Vulnerabilities (green)
- Unknown (blue)

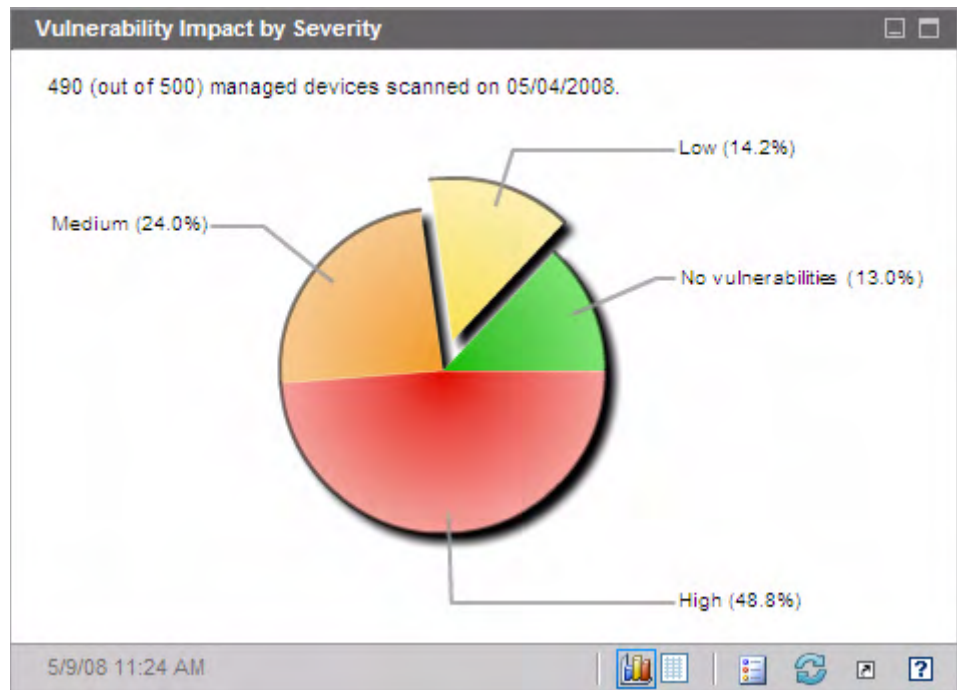
To see the number of devices in each severity category, rest the cursor on the corresponding sector of the pie chart.

Figure 9 Vulnerability Impact by Severity



If you click one of the wedges in the pie chart, a new browser window opens, and a detailed report is displayed. The report is filtered based on the severity category corresponding to the wedge that you clicked. After you click a wedge and open a report, that wedge separates from the rest of the pie, as shown here:

Figure 10 Vulnerability Impact by Severity



The grid view shows you how many devices fall into each severity category and whether the device count for that category has increased, decreased, or stayed the same since the previous vulnerability scan.

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

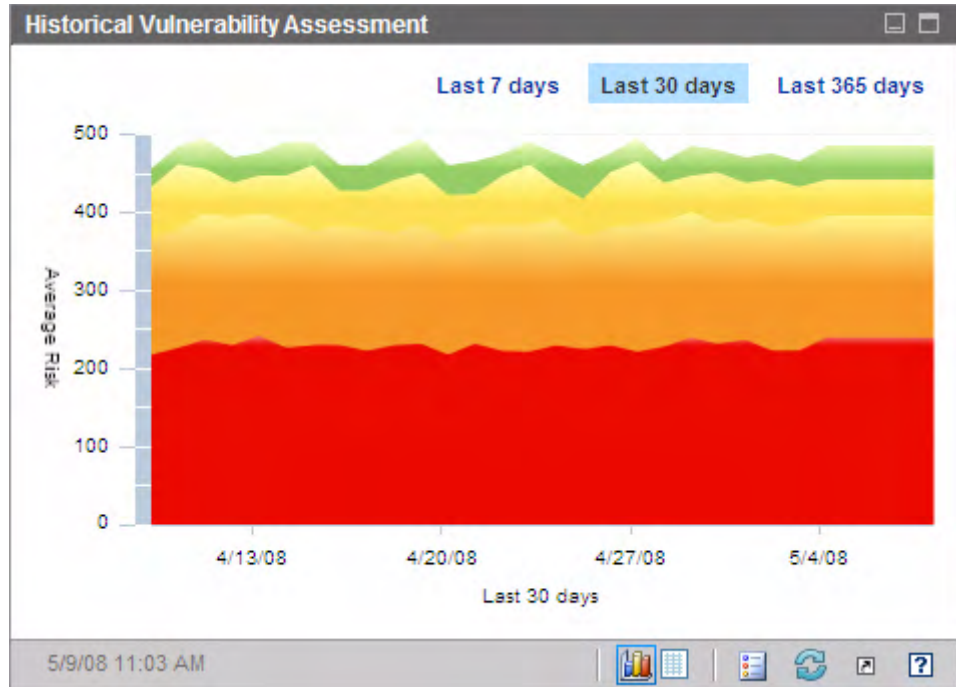
[Security and Compliance Management](#) on page 43

Historical Vulnerability Assessment

This pane shows how the information displayed in the Vulnerability Impact by Severity panes changes over time.

The chart view of this pane shows you the average aggregate risk in your enterprise over a period of time. The vertical axis represents the number of devices. The horizontal axis represents time. You can display the last seven days, 30 days, or 365 days of data. Each colored region represents the number of devices in each of the severity categories: High (red), Medium (orange), Low (yellow), No Vulnerabilities (green), and Unknown (blue).

Figure 11 Historical Vulnerability Assessment



When you rest the cursor on a data point that lies on a line between colored regions, a circle highlighting that data point appears, and a tool tip shows you the number and percentage of devices in that vulnerability category on that day.

Figure 12 Tool Tip

Scanned on : 09/01/2007 7:24 AM
230 (out of 490) devices with High Vulnerabilities. (46.9%)

In this example, 46.9% of the 490 devices scanned had at least one high severity vulnerability. The tool tip always displays information from the last vulnerability scan performed. Typically a scan is performed daily. If a scan was not performed for several days, the graph will be flat for those days, and the information in the tool tip will not change.

The tool tips always show you when the most recent vulnerability scan was performed. As you analyze your vulnerability data, be sure to check the date of the most recent scan.

Note that the appearance of the circle that appears around the data point when a tool tip is displayed will vary depending on the color of the region underneath the circle.

The grid view for this pane lists of the number of devices in each risk category on each day during the specified time period. The grid also indicates the date on which the environment was last scanned.

Although the chart does not contain a band for devices in the Unknown severity category, the grid view includes a column for these devices.

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

[Security and Compliance Management](#) on page 43

Vulnerability Impact

The chart view of this pane shows you the relative numbers of devices that are affected by a particular vulnerability. There is one circle per vulnerability, and the size of the circles indicates the number of devices affected. The color of each circle represents the severity of the vulnerability: High (red), Medium (orange), Low (yellow), and Unknown (blue).

The vertical axis represents severity as measured by the CVSS Base score; the horizontal axis represents time since the vulnerability was first published in the National Vulnerability Database (NVD). For example:

- Large red circles in the upper right portion of the chart represent severe vulnerabilities that affect a large number of devices and have been published for a relatively long time.

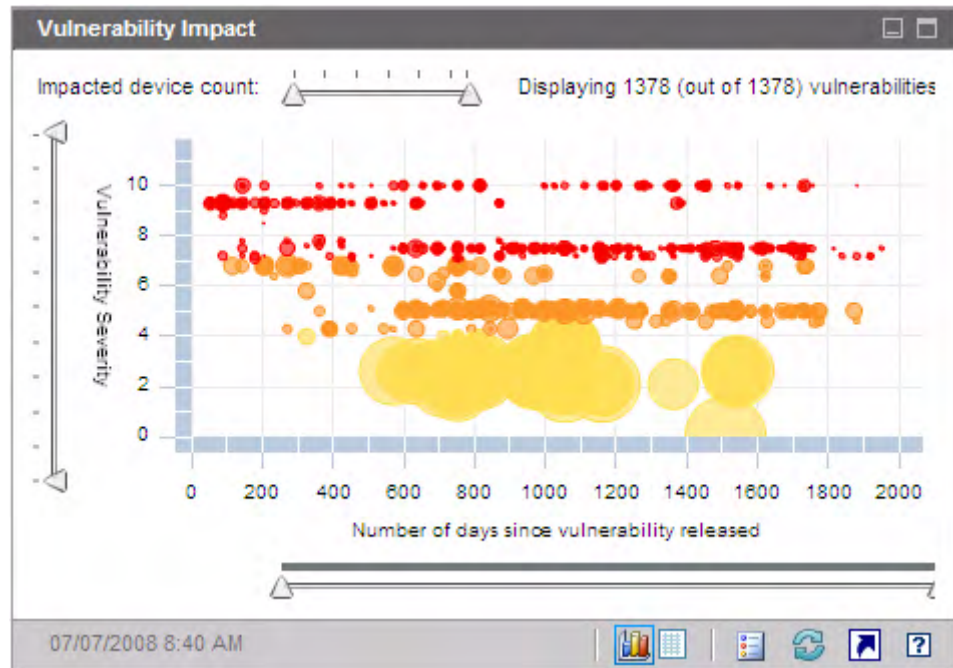
- Small yellow circles in the lower left portion represent issues that are of low severity, affect a smaller number of devices, and were published in the NVD relatively recently.
- An ideal chart would have no red bubbles in the upper right corner. This would imply that severe vulnerabilities are dealt with quickly.

When you rest your cursor on a particular circle, a tool tip shows you the following information about the vulnerability that the circle represents:

- Severity category (high, medium or low)
- CVE identifier and title
- Publication date
- Number of devices affected
- Total number of scanned devices

If you click one of the circles in the chart, a new browser window opens, and a detailed report is displayed. The report shows the number of devices affected by this vulnerability and information about the vulnerability itself. To obtain a list of affected devices, click the number of Devices Impacted in the report.

Figure 13 Vulnerability Impact



You can use the three sliders to zoom in on a particular data region. The sliders determine how many circles appear in the chart and the scale represented by each axis.

- The horizontal slider at the top of the pane enables you to specify an impact range as measured by the number of managed devices affected by a particular vulnerability.
- The vertical slider on the left enables you to zoom in on a severity range as measured by the CVSS base score.
- The horizontal slider at the bottom of the pane enables you to specify the age of the vulnerabilities displayed. The age is based on the date when a vulnerability was originally published; it does not reflect subsequent modifications to the vulnerability definition.

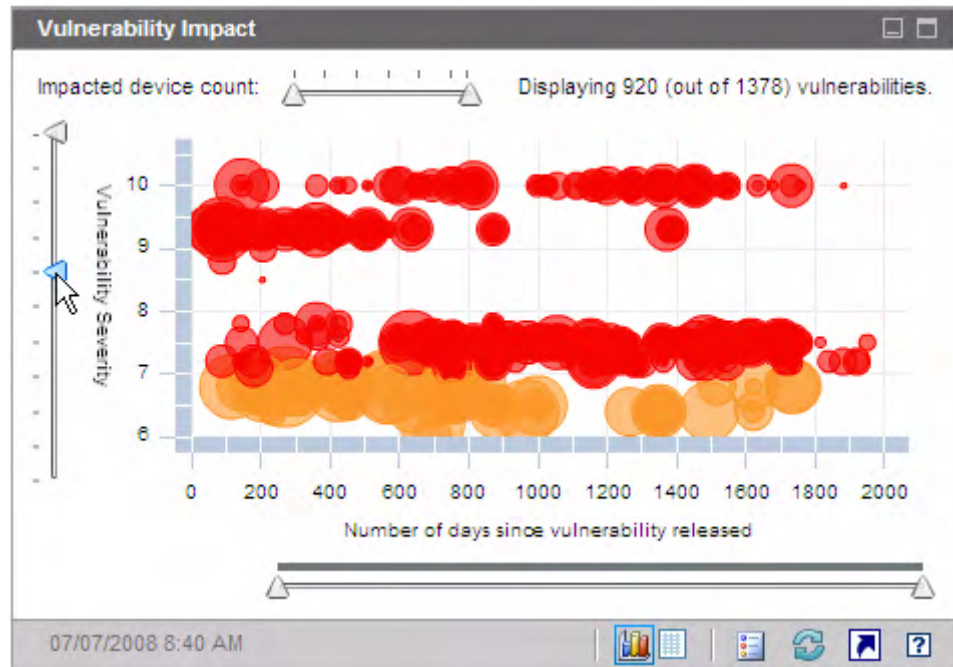
By default, the age span displayed is 45 days. You can specify this default value when you configure the Vulnerability Management dashboard. See [Dashboards](#) on page 318.

When the triangles (Δ) are at opposite ends of a slider, the entire data range is visible. When the triangles are closer together, only a subset is visible. You can adjust both triangles on each slider.

If no data appear in the chart, move the triangles to the opposite ends of all three sliders to expose the entire data range.

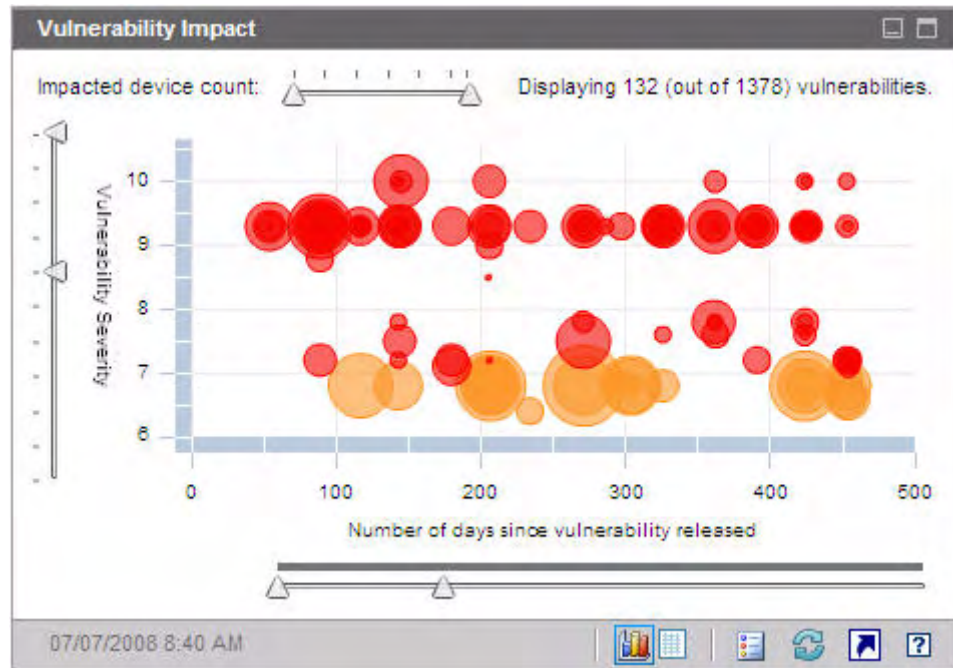
In the following example, vulnerabilities with a CVSS base score of 6 or greater are shown:

Figure 14 CVSS of 6 or Greater



In the following example, only vulnerabilities with CVSS base scores of 6 or greater that were released during the most recent 500 days are shown:

Figure 15 Most Recent 500 Days



The grid view for this pane provides the following information for each vulnerability detected:

- OVAL ID – OVAL identifier for this vulnerability
- CVE ID – CVE identifier for this vulnerability
- Description – from the OVAL definition
- Severity – High, Medium, or Low severity icon and CVSS base score for this vulnerability
- Age – Number of days since this vulnerability was published in the NVD
- Device Count – number of client devices affected

The grid view displays data corresponding to the data displayed in the chart at the time the grid view is selected. If the sliders on the chart are adjusted to show a subset of the data, only this subset will appear in the grid view.

The grid is initially sorted by Device Count. To change the sort parameter, click the pertinent column heading.

To find more information about a particular vulnerability, click its OVAL or CVE identifier.

Related Topics:

[Using the Dashboards](#) on page 83

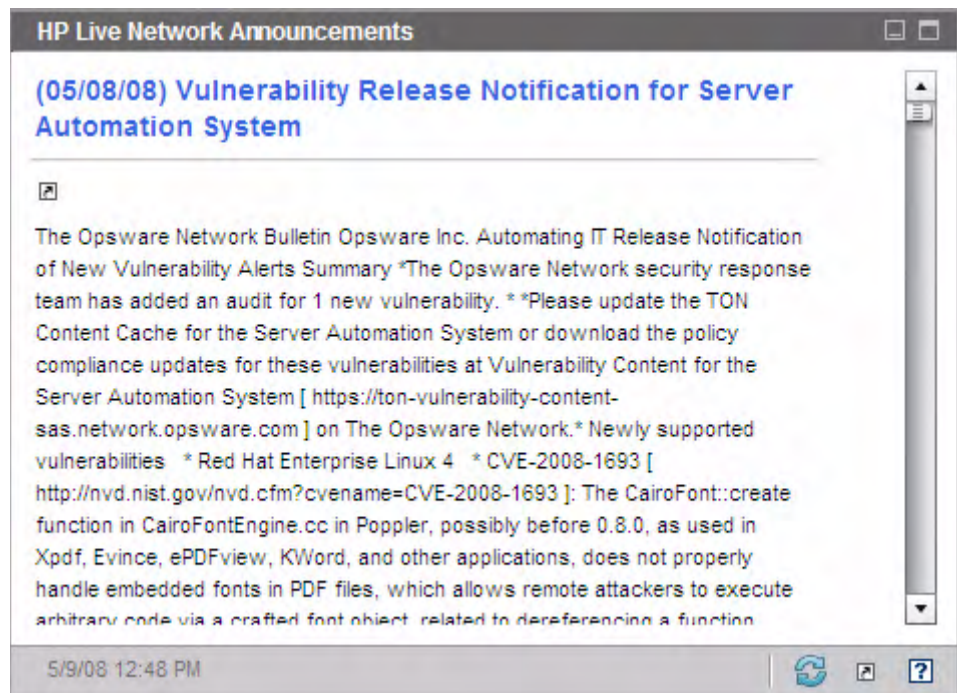
[Vulnerability Management Dashboard](#) on page 96


[Security and Compliance Management](#) on page 43

HP Live Network Announcements

This pane contains the most recently published HP Live Network vulnerability release announcements. This information is provided by an RSS feed from the HP Live Network subscription site. By default, this pane is not enabled, because it requires HP Live Network credentials to be specified before it can display information. See [Dashboards](#) on page 318 for information about configuring your HP Live Network credentials.

Figure 16 HP Live Network Announcements



To find more information about a particular announcement, click the  icon just below its title. A new browser window will open to the HP Live Network subscription support site. You must have an active HP Live Network subscription to access this site.

This pane does not have a chart view.

When you enable this pane on the Configuration tab, you can change the URL for the RSS feed, as well as the location of the HP Live Network authentication server (see [Dashboards](#) on page 318). You may also need to enable a proxy server (see [Configure the Connection to the HP Live Network Server](#) on page 281 and [Proxy Settings](#) on page 263).

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

[Security and Compliance Management](#) on page 43

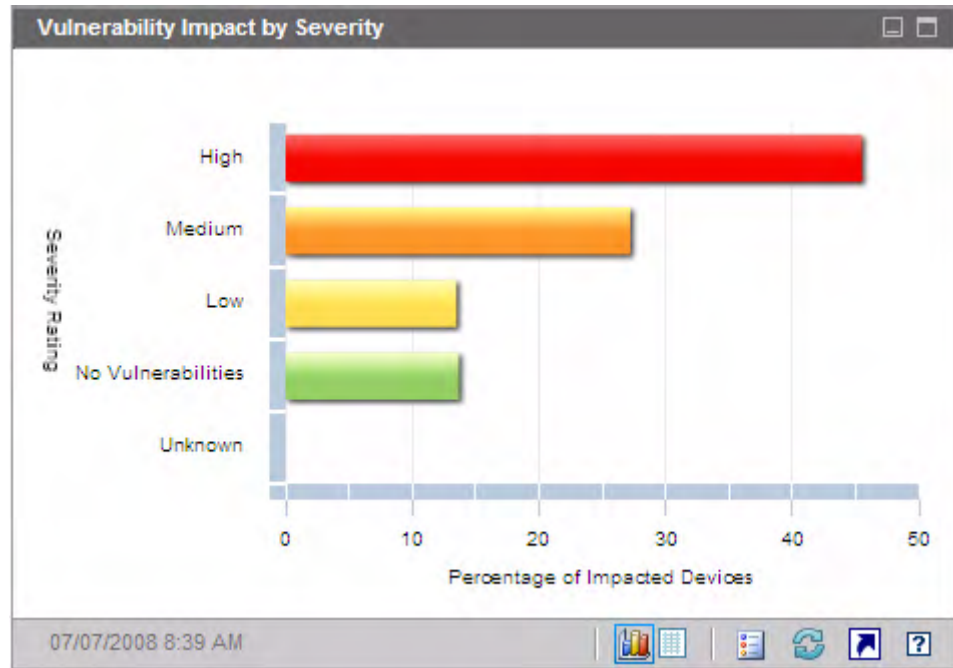
Vulnerability Impact by Severity (bar chart)

The chart view for this pane shows you the percentage of scanned devices in the enterprise that fall into each of the following five categories based on the highest severity vulnerability detected on each device:

- High (red)
- Medium (orange)
- Low (yellow)
- No Vulnerabilities (green)
- Unknown (blue)

The horizontal axis represents the percentage of devices affected in your environment. The vertical axis represents the four severity categories.

Figure 17 Vulnerability Impact by Severity



If you click one of the colored bars in the chart, a new browser window opens, and a detailed report is displayed. The report is filtered based on the severity category corresponding to the bar that you clicked.

The grid view for this pane shows the same information in text format. It has two columns:

- Status – severity by category
- Percentage of Impacted Devices – same as chart view

The grid also indicates whether the percentage of devices in each category has increased, decreased, or remained the same since the previous scan.

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

[Security and Compliance Management](#) on page 43

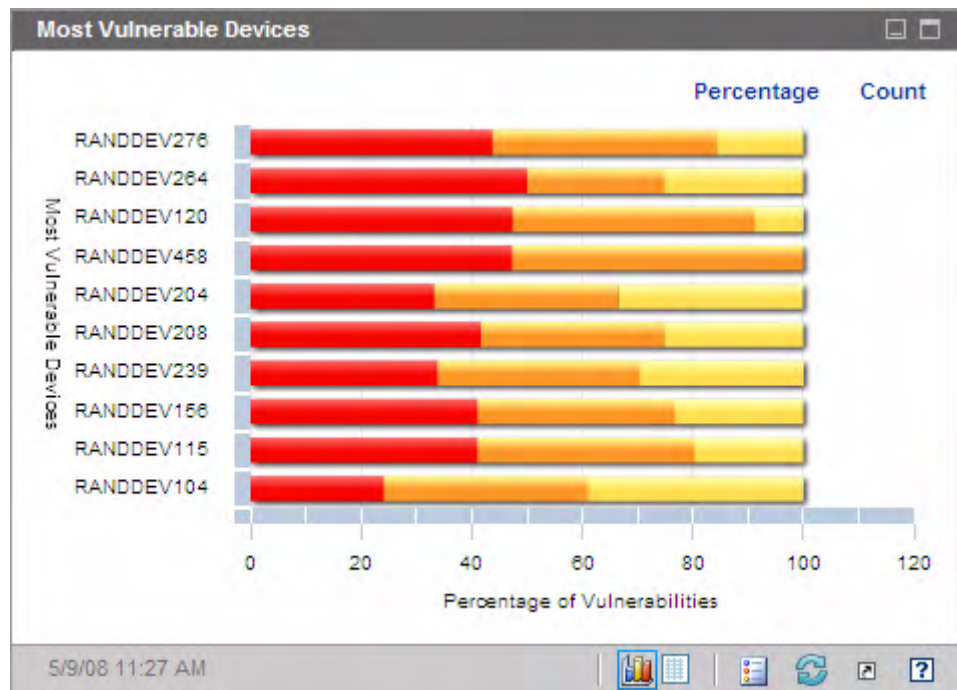
Most Vulnerable Devices

The chart view for this pane shows you the ten devices in your network that have the largest number of vulnerabilities. The colored segments in the chart represent the percentage (or number) of vulnerabilities present on a given device that fall into each of the following four categories:

- High (red)
- Medium (orange)
- Low (yellow)
- Unknown (blue)

The vertical axis lists devices by Device Identifier, and the horizontal axis shows the percentage or number of failed tests (vulnerabilities) in each risk category for this device.

Figure 18 Most Vulnerable Devices



To display the number of scanned devices instead of the percentage, click **Count**. In this case, the horizontal axis uses a logarithmic scale.



If a particular device has only one vulnerability, no data is shown for that device in the Count view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

If you click one of the colored bars in the chart, a new browser window opens, and a detailed report for this device is displayed. This report is not filtered by severity – all vulnerabilities for this device are listed regardless of which colored area you clicked.

If you rest the cursor on one of the colored bars in the chart, you can see the number (and percentage) of vulnerabilities in each severity category for a particular device.

The grid view provides the following information for each device:

- Max Severity – CVSS Base score for the highest severity vulnerability detected for this device
- Device – Device identifier
- Failed Tests – number of vulnerabilities detected
- Scan Date – date and time of the most recent HP Live Network scan

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

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

[Security and Compliance Management](#) on page 43

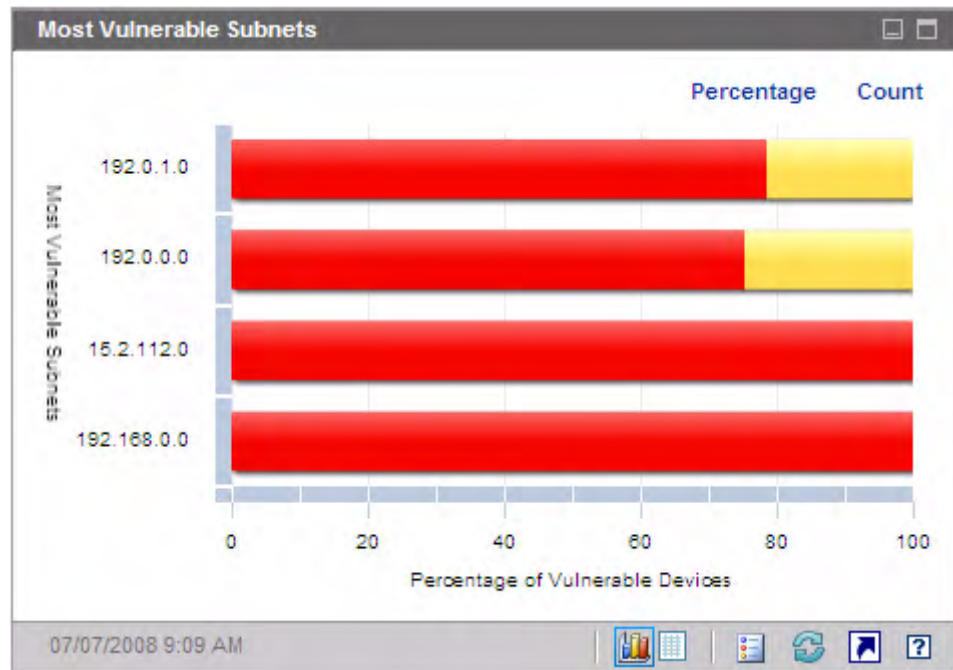
Most Vulnerable Subnets

The chart view of this pane shows you the ten most vulnerable subnets in the enterprise. It indicates the percentage of devices in each severity category: High (red), Medium (orange), Low (yellow), Unknown (blue), and No Vulnerabilities (green).

By default, this pane is disabled. To enable it, see [Dashboards](#) on page 318 .

To view information about the devices in each subnet, rest the cursor over the horizontal bar for that subnet. A pop-up box shows you the number and percentage of devices in each severity category in this particular subnet.

Figure 19 Most Vulnerable Subnets



To display the number of scanned devices instead of the percentage, click **Count**. In this case, the horizontal axis uses a logarithmic scale.



If a particular subnet has only one vulnerability, no data is shown for that subnet in the Count view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

The grid view provides the following information for each subnet:

- Subnet address
- Total number of devices in the subnet
- Number of devices in each severity category

The table is initially sorted by High Risk devices. To change the sort parameter, click the pertinent column heading.

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

[Security and Compliance Management](#) on page 43

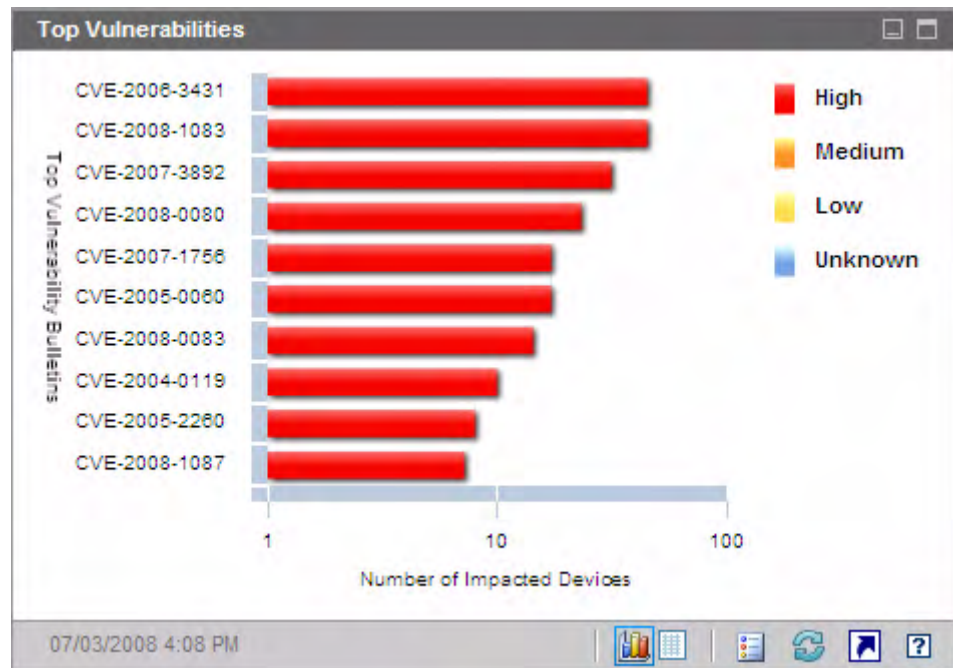
Top Vulnerabilities

The chart view of this pane shows you the ten security vulnerabilities that affect the greatest number of devices in your network. The vertical axis lists the CVE Identifiers for these ten vulnerabilities. The horizontal axis represents the number of devices affected and uses a logarithmic scale. The colors of the bars reflect the severity of each vulnerability:

- High (red)
- Medium (orange)
- Low (yellow)
- Unknown (blue)

Because this chart uses a logarithmic scale, if a particular vulnerability affects only one device, no data is shown for that vulnerability in the chart view. This is a known limitation of logarithmic scales. The data is visible in the grid view, however.

Figure 20 Top Vulnerabilities



If you rest the cursor on the colored bar for a particular vulnerability, the CVE Identifier and description, severity, and number of devices affected is shown:

Figure 21 Tool Tip

High Severity CVE-2005-1154 (Mozilla Global Pollution Vulnerability) Published on: Aug 16, 2005 12:00:00 PM
10 (out of 500) vulnerable devices.
Click on the chart to view details in HPCA Reporting Server.

If you click one of the colored bars in the chart, a new browser window opens, and a filtered report is displayed. The report lists all devices that have this vulnerability.

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

- OVAL ID – OVAL ID for this vulnerability

- CVE ID – CVE ID for this vulnerability
- Description – from the CVE
- Severity – CVSS Base score for this vulnerability
- Platform Family – general type of operating system (for example, Windows)
- Device Count – number of devices affected by this vulnerability

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

To find more information about a particular vulnerability, click its CVE ID or OVAL ID.

Related Topics:

[Using the Dashboards](#) on page 83

[Vulnerability Management Dashboard](#) on page 96

[Security and Compliance Management](#) on page 43

Compliance Management Dashboard

HPCA has the ability to collect regulatory compliance information for each managed client system in your enterprise. This information is then aggregated and displayed in the Compliance Management dashboard.

HPCA is integrated with HP Live Network, which provides updated Compliance definitions and an executable client scanner.

Client devices are scanned using compliance rules that are based on established regulatory compliance standards, such as the Federal Desktop Core Configuration (FDCC) standard. Compliance rules are specified using the Security Content Automation Protocol (SCAP).

➤ For more information about FDCC and SCAP, including a list of common compliance management terms used throughout the Compliance Management dashboard and Compliance Management reports, see [Security and Compliance Management](#) on page 43.

The Compliance Management dashboard has a summary page and two views:

The Executive View includes the following information panes:

- [Compliance Summary by SCAP Benchmark](#) on page 118
- [Compliance Status](#) on page 116
- [Historical Compliance Assessment](#) on page 119

The Operational View includes the following information panes:

- [Top Failed SCAP Rules](#) on page 121
- [Top Devices by Failed SCAP Rules](#) on page 123

You can configure the dashboard to show or hide any of these panes. See [Dashboards](#) on page 318 for additional information.

➤ When you click Compliance Management in the left navigation pane on the Home tab, the Compliance Management home page is displayed. This page shows you the number of managed client devices that have been scanned and provides links to pertinent reports.

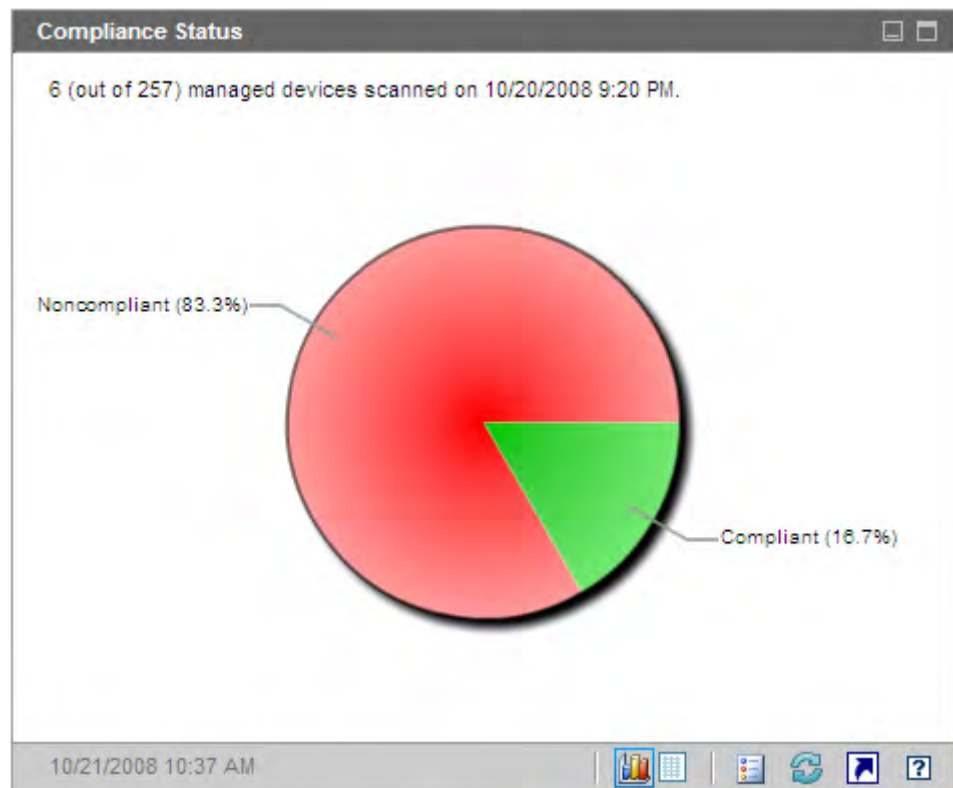
Compliance Status

This pane shows you the state of regulatory compliance across your enterprise based on the results of the most recent compliance scan completed on each managed client device. The chart view for this pane shows you the percentage of scanned devices that are in or out of compliance:

- Compliant devices (green)
- Noncompliant devices (red)

To see the number (or percentage) of devices in each state of compliance, rest the cursor on the corresponding sector of the pie chart.

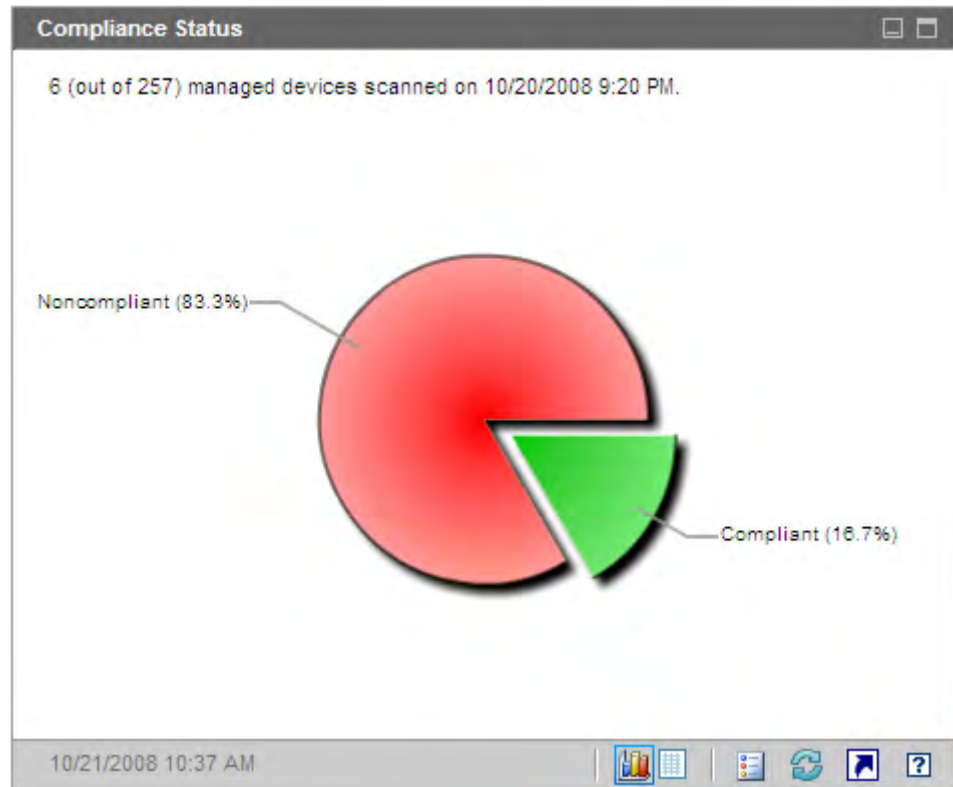
Figure 22 Compliance Status



If you click one of the wedges in the pie chart, a new browser window opens, and the Compliance Summary by SCAP Benchmark report is displayed. This report is not filtered.

After you click a wedge and open a report, that wedge separates from the rest of the pie, as shown here:

Figure 23 Compliance Status After Report Opens



The grid view shows you how many devices are compliant or noncompliant. If you click either **Compliant** or **Noncompliant** in the grid view, the Compliance Summary by SCAP Benchmark report opens in a new browser window. The report is not filtered.

Related Topics:

[Using the Dashboards](#) on page 83

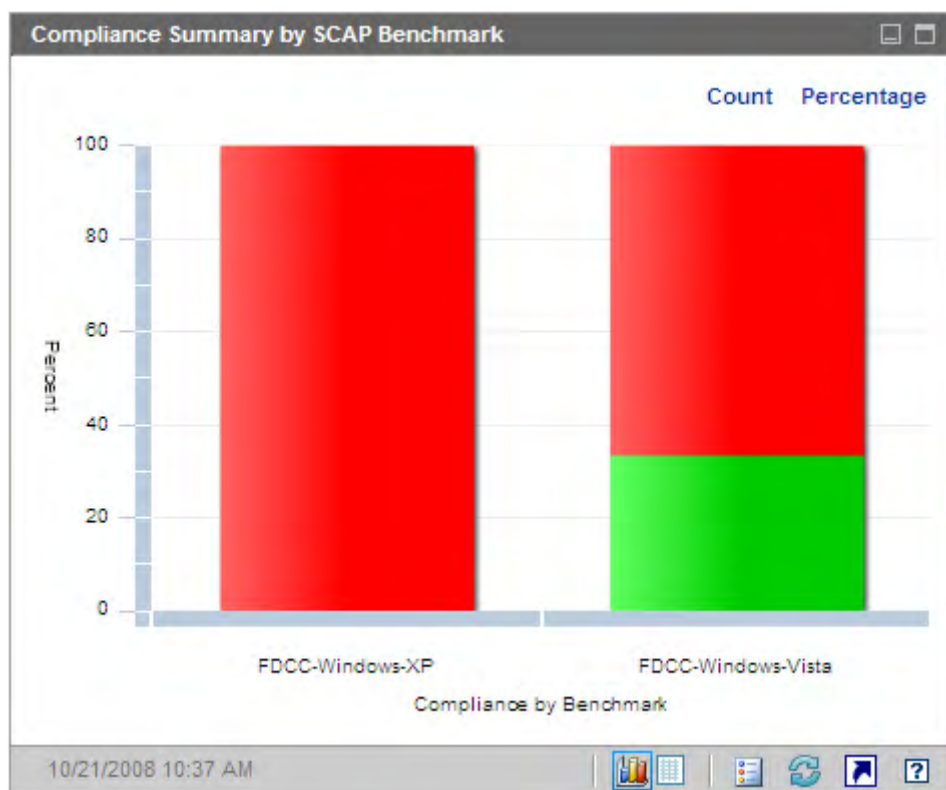
[Compliance Management Dashboard](#) on page 115

Compliance Summary by SCAP Benchmark

The chart view for this pane shows you the number (or percentage) of scanned devices in the enterprise that are in or out of compliance with the associated SCAP benchmark:

- Compliant devices (green)
- Noncompliant devices (red)

Figure 24 Compliance Summary by SCAP Benchmark



When you rest the cursor on one of the colored bars in the chart, a tool tip shows you information about the benchmark, including the number (or percentage) of devices in the pertinent state of compliance.

Figure 25 Tooltip

	Count	Percentage
FDCC-XP-Firewall v1.1.0.0	187 (out of 193)	96.9%

Click on the chart to view details in HPCA Reporting Server.

The tool tip always displays information from the last compliance scan performed. Typically a scan is performed daily.

If you click one of the colored segments in the bar chart, a new browser window opens, and the SCAP Scanned Devices report is displayed. The report is filtered based on the benchmark and compliance status corresponding to the segment that you clicked.

The grid view for this pane shows you the number (and percentage) of devices that are compliant or noncompliant with each benchmark. If you click a Benchmark ID in the grid view, the SCAP Compliance Rules by CCE report opens. The report is filtered based on the Benchmark ID you clicked.

Related Topics:

[Using the Dashboards](#) on page 83

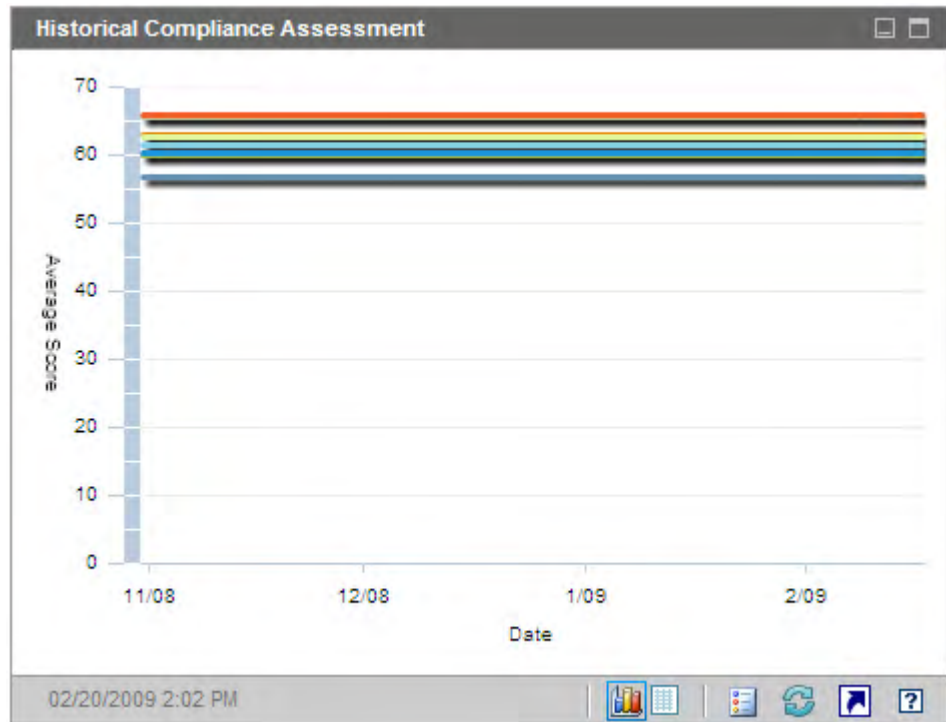
[Compliance Management Dashboard](#) on page 115

[Security and Compliance Management](#) on page 43

Historical Compliance Assessment

Once per day, HPCA takes a snapshot of the compliance scanning results across your enterprise. Based on this snapshot, an average default score is calculated for each benchmark among the devices to which that benchmark applies. This information pane shows you the average default score for each benchmark over time.

Figure 26 Historical Compliance Assessment



The vertical axis represents the average default score. The horizontal axis represents time. Each colored line represents a different benchmark (or version).

- fdcc-ie-7 v1.1.0.0
- FDCC-Vista-Firewall v1.1.0.0
- FDCC-Windows-Vista v1.0
- FDCC-XP-Firewall v1.1.0.0
- FDCC-Windows-Vista v1.1.0.0
- fdcc-ie-7 v1.0
- FDCC-Windows-XP v1.1.0.0
- FDCC-Windows-XP v1.0

The colors are assigned dynamically and are not always the same for a specific benchmark and version. Refer to the legend to see the current color assignments.

When you rest the cursor on one of the colored lines, a tool tip shows you the following information:

- Benchmark name and version
- Snapshot date
- Average default score for all devices that were scanned for this benchmark/version

The grid view for this pane lists the daily average default score for each benchmark. It also indicates how many of the applicable devices were in compliance with that benchmark on that day. The table is initially sorted by date, with the most recent snapshot date listed first.

Related Topics:

[Using the Dashboards](#) on page 83

[Compliance Management Dashboard](#) on page 115

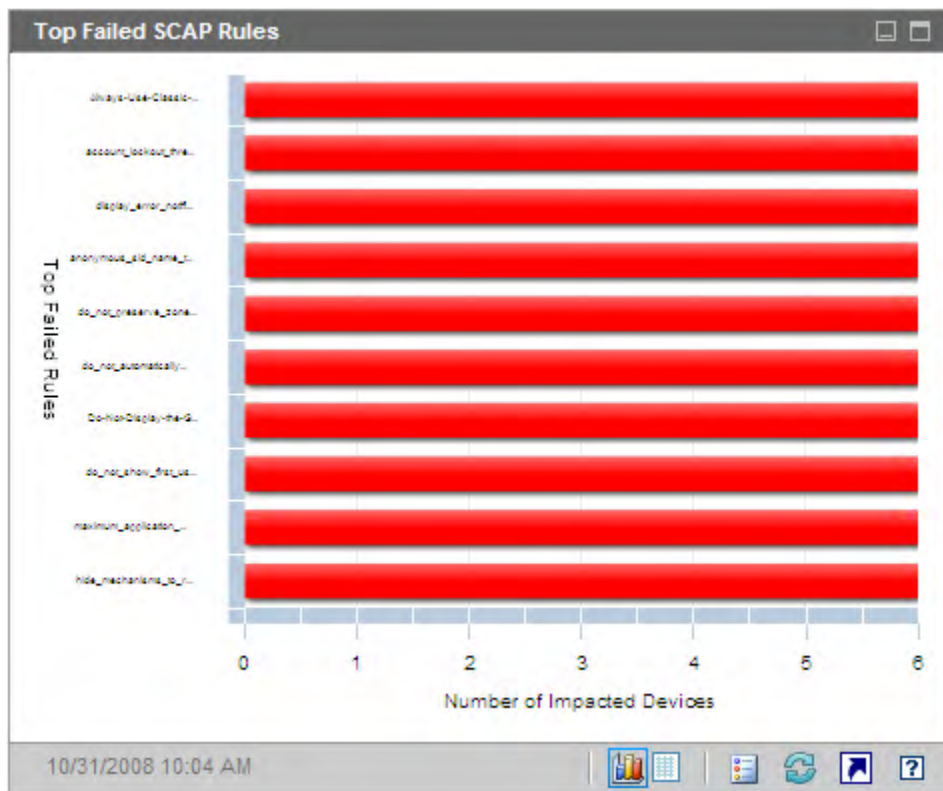
[Security and Compliance Management](#) on page 43

Top Failed SCAP Rules

The chart view for this pane shows you the ten regulatory compliance checks (SCAP rules) that failed most frequently in your enterprise. The vertical axis lists the names of the pertinent compliance rules. The horizontal axis represents the number of managed client devices that are out of compliance with each rule.

To see the exact number of devices that failed a particular rule and the severity of that rule, rest the cursor on one of the colored bars in the chart.

Figure 27 Top Failed SCAP Rules



If you click one of the colored bars in the chart, a new browser window opens, and the SCAP Compliance Rules by CCE report is displayed. The report is filtered based on the rule corresponding to the bar that you clicked.

The grid view for this pane shows you the number of devices that failed each rule as well as detailed information about the rule itself. If you click a Rule ID or Number of Devices in the grid view, the SCAP Compliance Rules by CCE report opens.

Related Topics:

[Using the Dashboards](#) on page 83

[Compliance Management Dashboard](#) on page 115

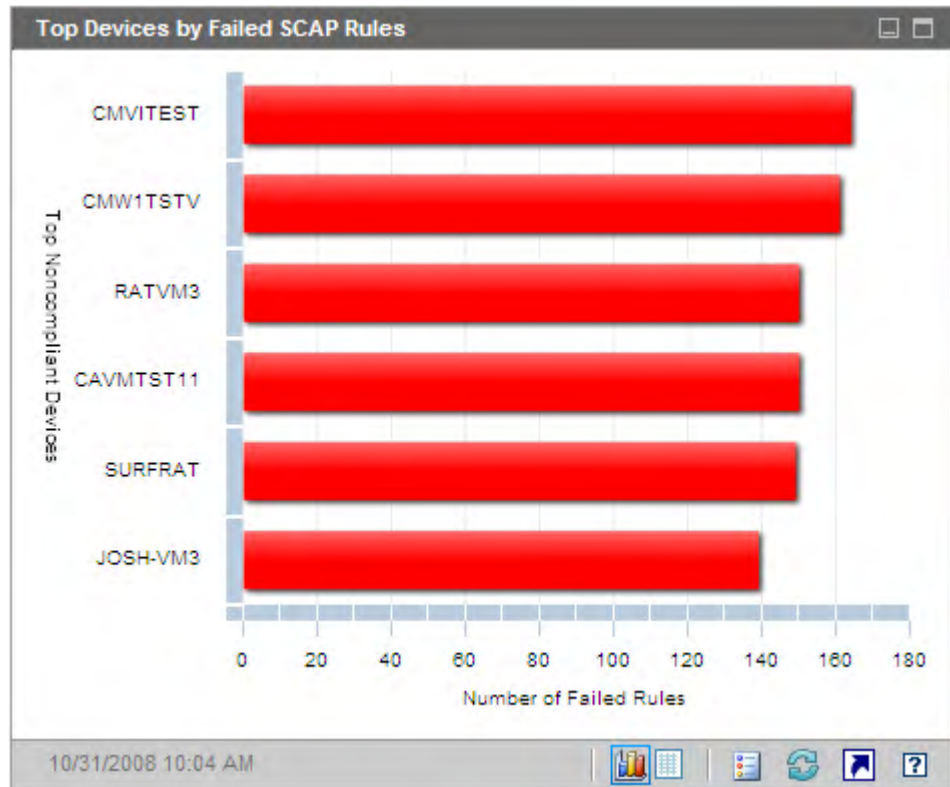
[Security and Compliance Management](#) on page 43

Top Devices by Failed SCAP Rules

The chart view for this pane shows you the ten managed client devices that failed the highest number of regulatory compliance checks (SCAP rules) in your enterprise. The vertical axis lists the names of the pertinent devices. The horizontal axis represents the number of compliance rules that failed in the most recent compliance scan for each device listed.

To see the exact number of rules that failed for a particular device, rest the cursor on one of the colored bars in the chart.

Figure 28 Top Devices by Failed SCAP Rules



If you click one of the colored bars in the chart, a new browser window opens, and a detailed report is displayed. The report is filtered based on the device corresponding to the bar that you clicked. The report has two parts:

- The SCAP Scanned Devices portion of the report shows summary information about the most recent scan results for each benchmark tested on the device.
- The SCAP Compliance Rules by CCE portion of the report shows detailed results for each rule tested during the most recent scan.

The grid view for this pane shows you the number of rules that failed, the default score, and the date of the most recent scan for each device in the chart view. If you click a Device in the grid view, the SCAP Scanned Devices report opens for that Device. The report is filtered to show the most recent scan results for each benchmark tested on this device.

Related Topics:

[Using the Dashboards](#) on page 83

[Compliance Management Dashboard](#) on page 115

[Security and Compliance Management](#) on page 43

Security Tools Management Dashboard

HPCA has the ability to scan the managed client devices in your enterprise to determine what types of security tools are present and collect pertinent information regarding the products detected. The following types of security products are supported:

- Anti-spyware tools
- Anti-virus tools
- Software firewalls

The collected information is then aggregated and displayed in the Security Tools Management dashboard.

HPCA is integrated with HP Live Network, which provides an executable security tool scanner.

The Security Tools Management dashboard has two views: the Executive View and the Operational View.

The Executive View includes the following information panes:

- [Security Product Status](#) on page 126
- [Security Product Summary](#) on page 128

The Operational View includes the following information panes:

- [Most Recent Definition Updates](#) on page 130
- [Most Recent Security Product Scans](#) on page 131

You can configure the dashboard to show or hide any of these panes. See [Dashboards](#) on page 318 for additional information.



When you click Security Tools Management in the left navigation pane on the Home tab, the Security Tools Management home page is displayed. This page provides links to pertinent reports and shows you various statistics about Security Tool Management in your environment:

Devices Managed – Number of devices that are entitled to the HPCA Security Tools service that collects information on various security products

Devices Scanned – Number of devices that have been scanned by the HPCA Security Tools service

Last Scan Date – The last time that any of the devices in your environment were scanned by the HPCA Security Tools service

Scanner Last Downloaded On – The time when the Security Tools scanner was most recently downloaded from the HP Live Network site to HPCA. See [Update HP Live Network Content](#) on page 60 for more information.

Security Product Status

The chart view for this pane shows you how many managed client devices have security tools – such as anti-spyware, anti-virus, or firewall software products – installed and enabled. You can display this information in either bar chart or stacked bar chart format. In both cases, the vertical axis shows the number of devices, and the horizontal axis shows the types of security tools detected.

The colors in the chart represent the following four conditions:

Table 13 Security Tool Detection States





Color		Interval
	Green	Product was detected, and it was enabled.
	Yellow	Product was detected, but it was not enabled.

Table 13 Security Tool Detection States

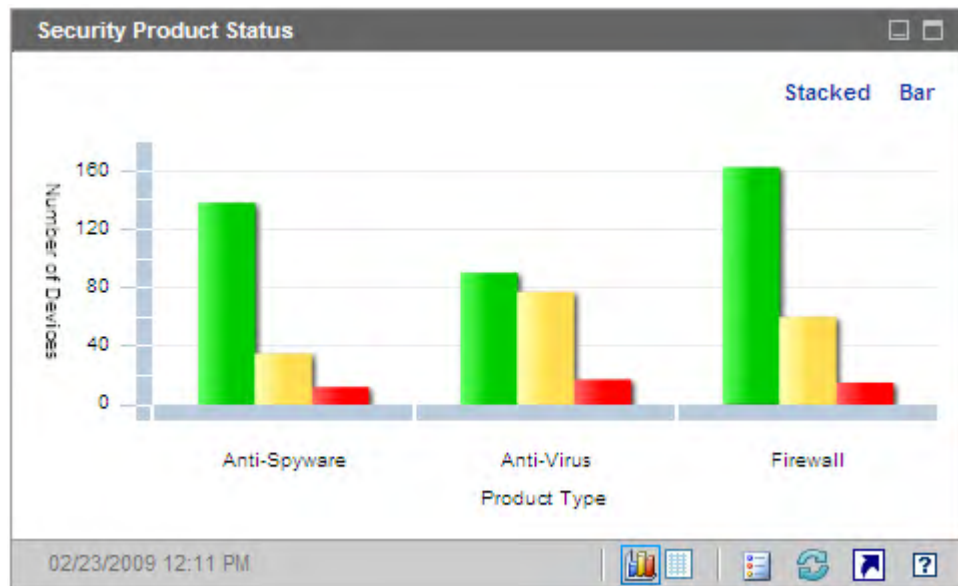
Color		Interval
	Red	Product was not detected.
	Blue	Unknown

The state of a scanned device is considered Unknown under any of the following conditions:

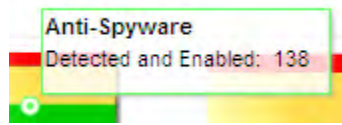
- The HP Live Network security tools scanner looked for this tool but was unable to determine its state.
- The scanner looked for this tool, but no scan records were found.
- The scanner did not look for this tool.

You can display this chart in either normal bar chart format (as shown here) or stacked bar format.

Figure 29 Security Product Status Pane



When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number of devices in the corresponding state:



If you click one of the colored bars in the chart, a new browser window opens, and a filtered report is displayed. The report shows you the number of managed client devices where that type of security product (anti-virus, anti-spyware, or firewall) is in each of the following states: detected and enabled, detected and disabled, not detected, or unknown.

The grid view for this pane shows you total number of managed client devices whose security tools are in each state.

Related Topics:

[Using the Dashboards](#) on page 83

[Security Tools Management Dashboard](#) on page 125

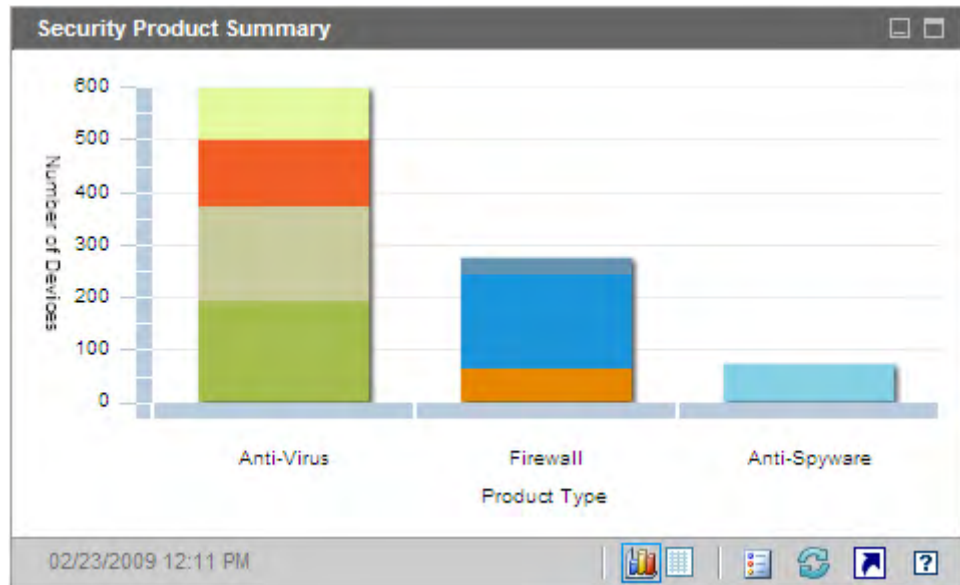
[Security and Compliance Management](#) on page 43

Security Product Summary

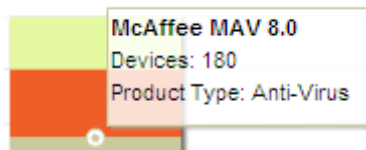
The chart view for this pane shows you which specific security products were detected on your managed client devices. The vertical axis shows the number of devices where each product was detected, and the horizontal axis shows the types of security tools detected.

The colors in the chart represent different products. Each version of a particular product is a different color.

Figure 30 Security Product Summary Pane



When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number of devices where a specific security product was detected:



If you click one of the colored segments in the chart, a new browser window opens, and a filtered report is displayed. The report shows you the number of the managed client devices that have each specific security product of this type (anti-virus, anti-spyware, or firewall) installed.

The grid view for this pane shows you number of managed client devices that have each specific security product installed.

Related Topics:

[Using the Dashboards](#) on page 83





[Security Tools Management Dashboard](#) on page 125

Most Recent Definition Updates

The chart view for this pane shows you how recently the virus and spyware definitions have been updated on your managed client devices. This information pertains to all anti-virus and anti-spyware products detected on your client devices.

You can display this information in terms of either the number (count) or percentage of devices. The colored bars represent the following update intervals:

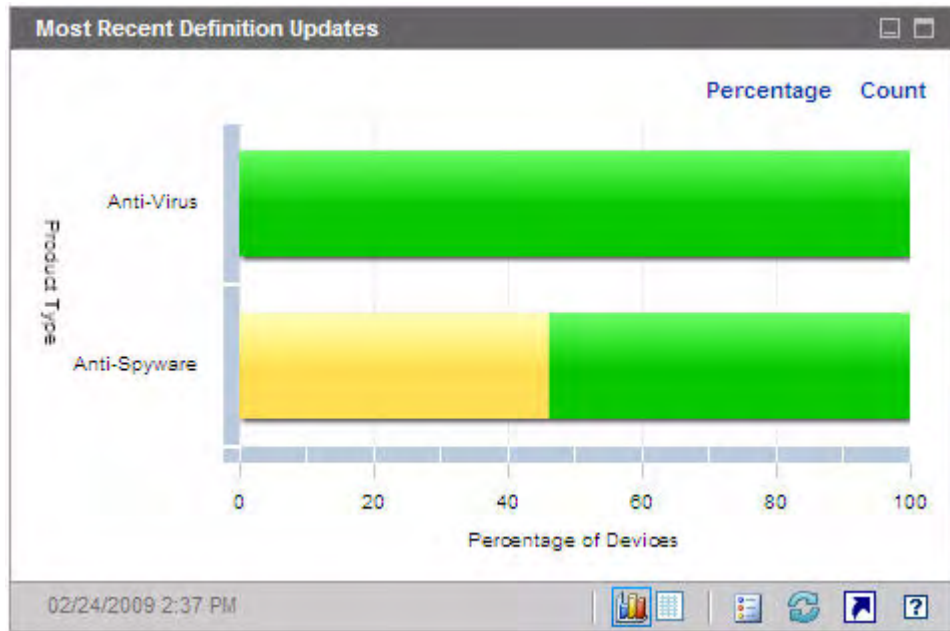
Table 14 Update Intervals

Color	Interval
 Red	More than 4 weeks
 Yellow	2 – 4 weeks
 Green	Less than 2 weeks
 Gray	Never
 Blue	Update unknown

When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number and percentage of devices that have been updated during the corresponding time interval.

Because this chart uses a logarithmic scale for the Count view, if a particular time interval contains only one device, no data is shown for that time interval in this view. This is a known limitation of logarithmic scales. The data is visible in the Percentage view, however, as well as the grid view.

Figure 31 Most Recent Definition Updates



The grid view for this pane shows you the same information in table format. Note that the grid view always uses device counts, not percentages.

If you click one of the colored bars in the chart view, a new browser window opens, and a filtered report is displayed. The report shows you the number of managed client devices where the anti-virus and anti-spyware definitions were updated during each time interval.

Related Topics:

[Using the Dashboards](#) on page 83

[Security Tools Management Dashboard](#) on page 125




[Security and Compliance Management](#) on page 43

Most Recent Security Product Scans

The chart view for this pane shows you how recently your managed client devices have been scanned for viruses and spyware. This information pertains to all anti-virus and anti-spyware products detected on your client devices.

You can display this information in terms of either the number (count) or percentage of devices. The colored bars represent the following update intervals:

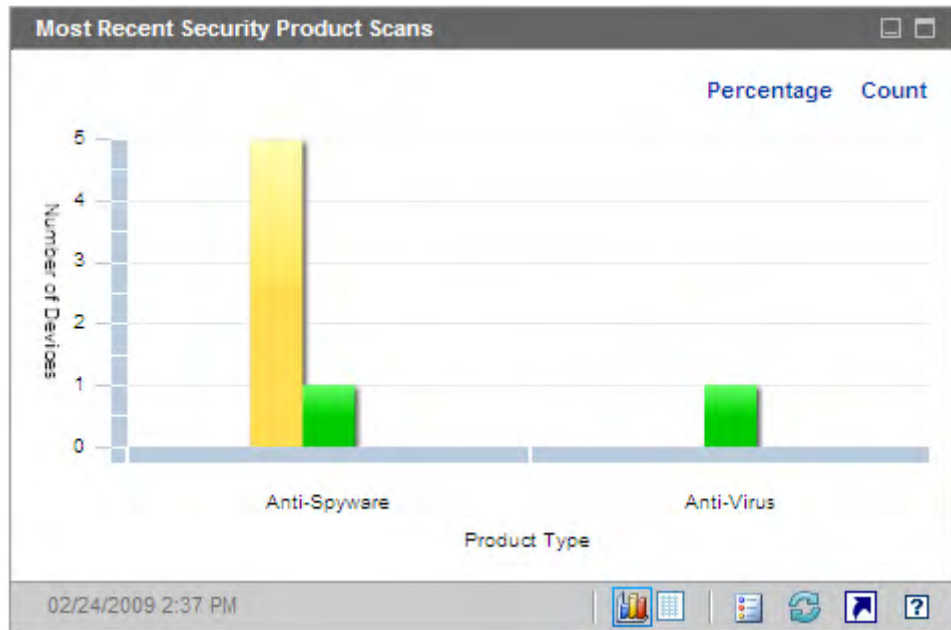
Table 15 Scan Intervals

Color		Interval
	Red	More than 4 weeks
	Yellow	2 – 4 weeks
	Green	Less than 2 weeks
	Gray	Never
	Blue	Scan unknown

When you hover the mouse over a colored bar in the chart, a tool tip appears that shows you the number and percentage of devices that have been scanned during the corresponding time interval.

Because this chart uses a logarithmic scale for the Count view, if a particular time interval contains only one device, no data is shown for that time interval in this view. This is a known limitation of logarithmic scales. The data is visible in the Percentage view, however, as well as the grid view.

Figure 32 Most Recent Security Product Scans



The grid view for this pane shows you the same information in table format. Note that the grid view always uses device counts, not percentages.

If you click one of the colored bars in the chart view, a new browser window opens, and a filtered report is displayed. The report shows you the number of managed client devices that were most recently scanned by the pertinent security tool (anti-virus or anti-spyware) during each time interval.

Related Topics:

[Using the Dashboards](#) on page 83

[Security Tools Management Dashboard](#) on page 125

[Security and Compliance Management](#) on page 43

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 134
- [Device Compliance by Bulletin](#) on page 136

The Operational View includes three information panes:

- [Device Compliance by Status \(Operational View\)](#) on page 138
- [Microsoft Security Bulletins](#) on page 139
- [Most Vulnerable Products](#) on page 140

You can configure the dashboard to show or hide any of these panes. See [Dashboards](#) on page 318.



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:

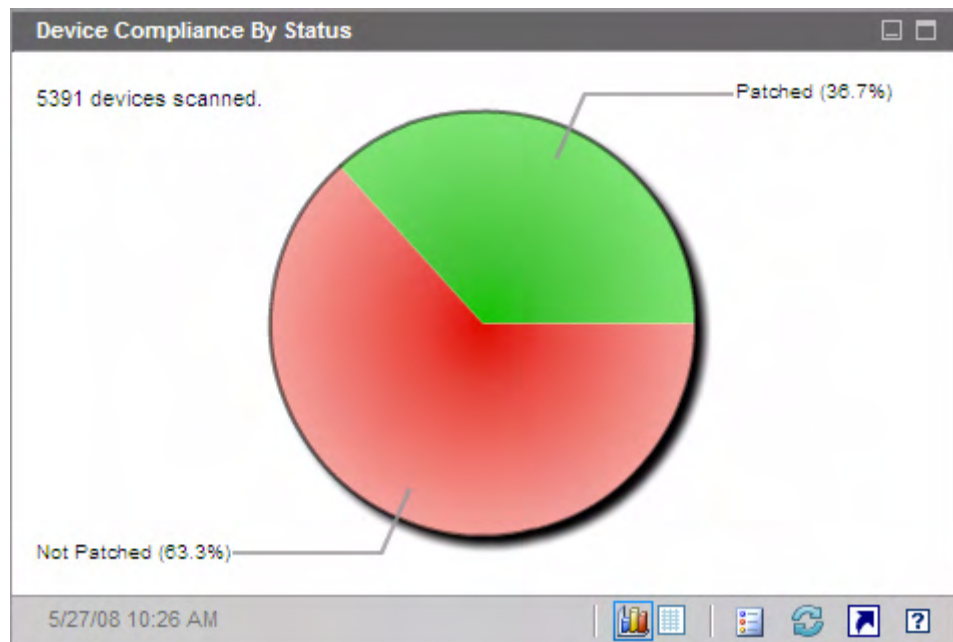
- Patched (green)
- Not patched (red)

The [Device Compliance by Status \(Operational View\)](#) on page 138 is similar but has finer-grained detail:

Table 16 Device Compliance By Status Views

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

Figure 33 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

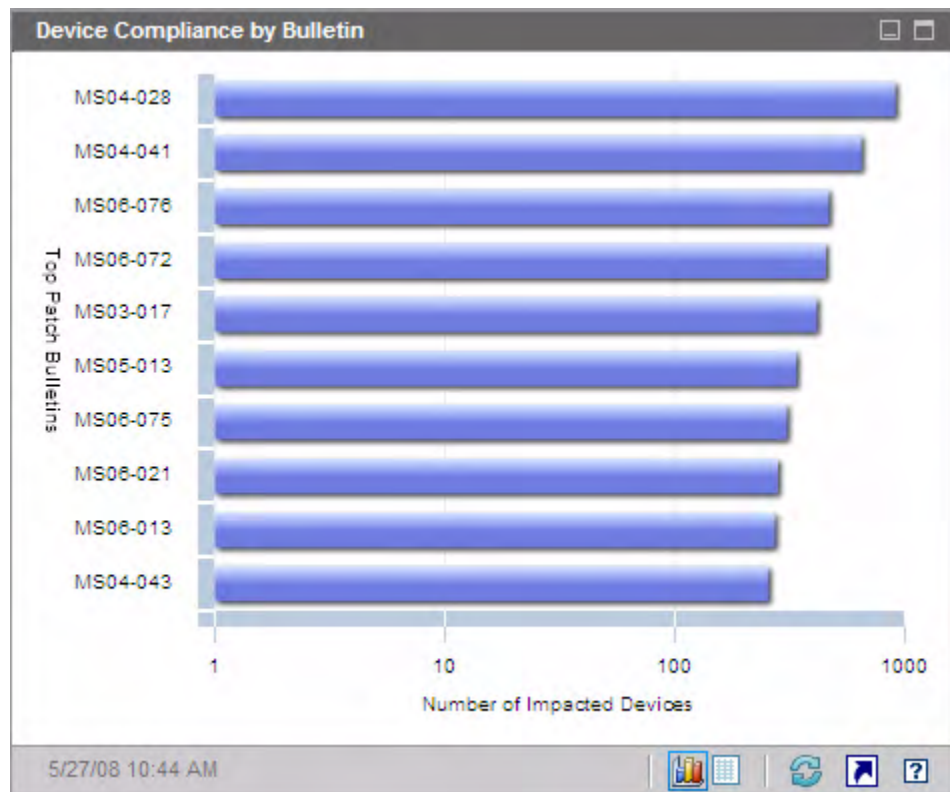
The chart view of this pane shows you the ten patch vulnerabilities that affect the greatest number of devices in your network. The vertical axis lists the patch bulletin numbers for these vulnerabilities. The horizontal axis represents the number of devices affected and uses a logarithmic scale.



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 34 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.

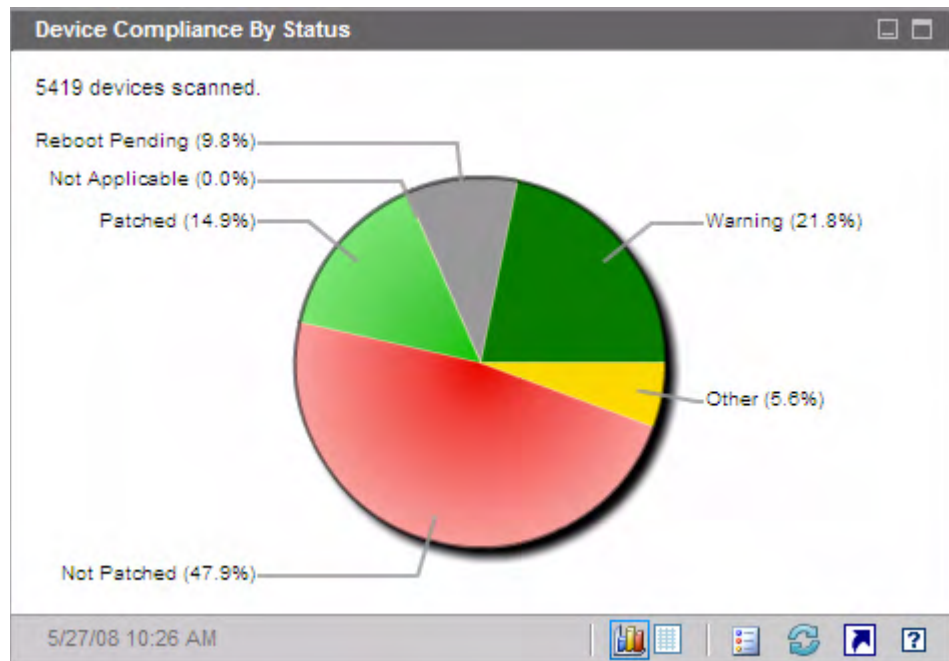
Device Compliance by Status (Operational View)

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 35 Device Compliance by Status (Operational View)



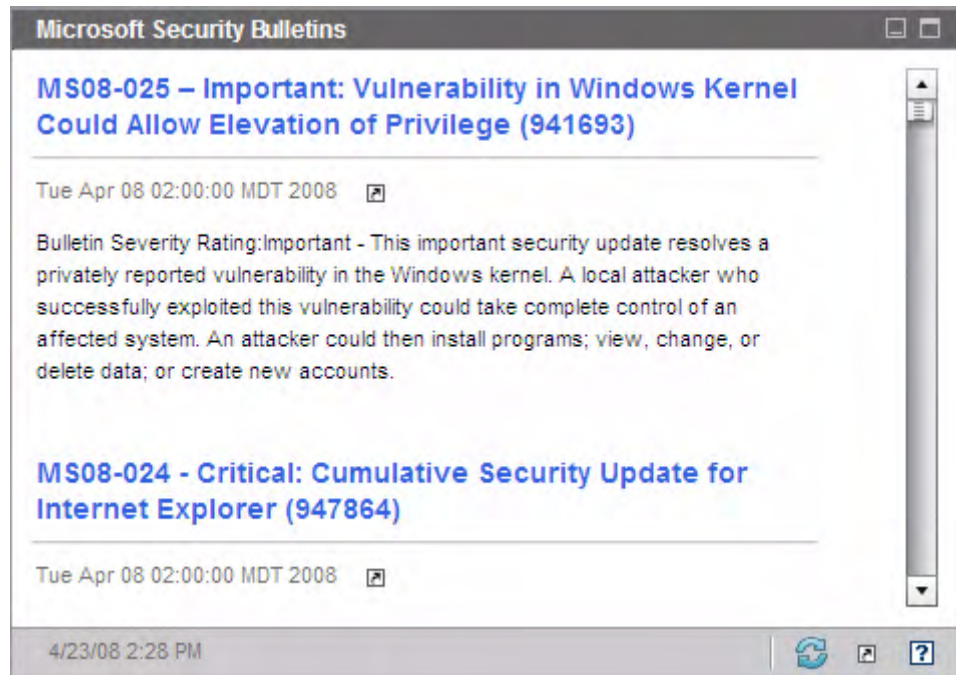
If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.


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 318).

Figure 36 Microsoft Security Bulletins



To view detailed information about a particular bulletin, click the  icon just below the bulletin name.

This pane does not have a chart view.

Most Vulnerable Products

This pane is disabled by default. To enable it, see [Dashboards](#) on page 318.

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

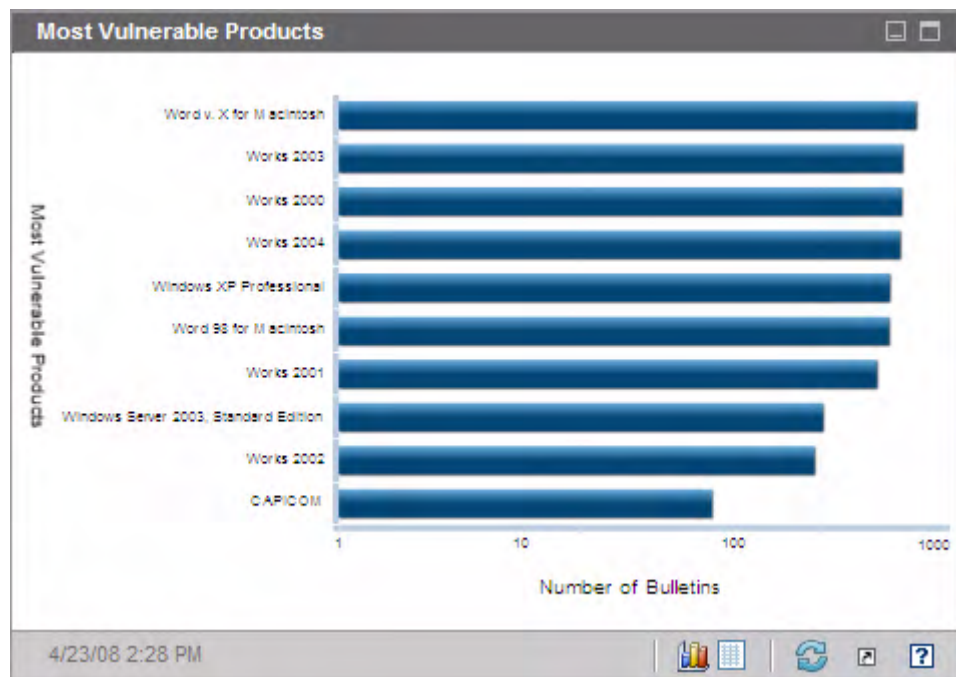
- 20 managed devices require 3 of these patches
- 50 managed devices only require 1 of the patches

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

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 37 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.

5 Managing the Enterprise

The Management area contains the tools you use to manage the client devices in your environment.. This chapter includes the following topics:

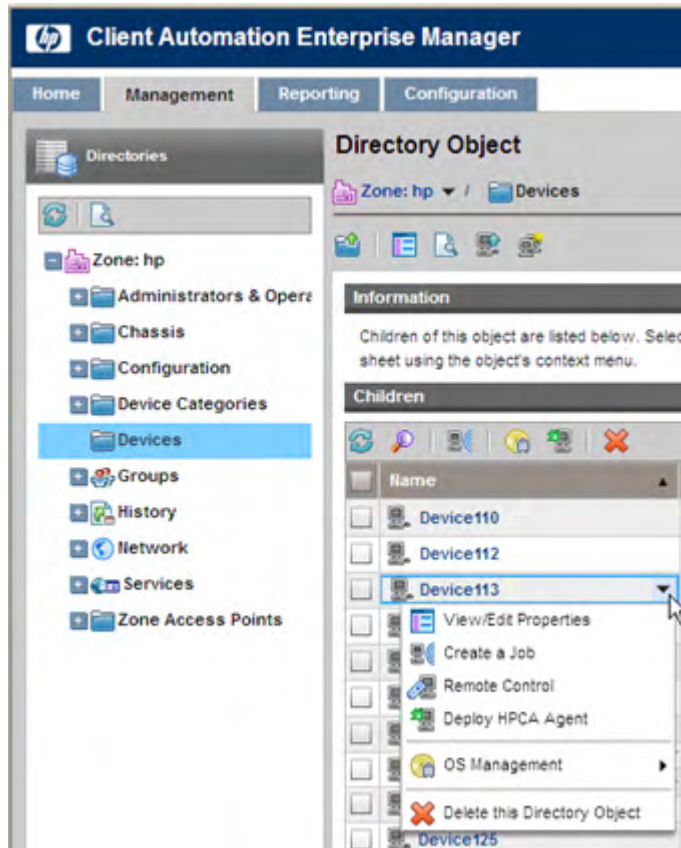
- [Managing Directory Policies](#) on page 144
- [Service Information](#) on page 153
- [Managing Groups](#) on page 154
- [Deploying the HPCA Agent](#) on page 156
- [Importing Devices](#) on page 153
- [Managing Jobs](#) on page 158
- [Creating Satellite Synchronization Jobs](#) on page 171
- [Removal of Old Job Execution Records](#) on page 170
- [Managing Virtual Machines](#) on page 173
- [Controlling Devices Remotely](#) on page 180
- [Managing Operating Systems](#) on page 186
- [Viewing Out Of Band Details](#) on page 200

Managing Directory Policies

From the Directories tree on the Management tab, you can view the objects in your configured directory services. See [Directory Services](#) on page 267. You can view the properties of an object, create its policies, and view its entitlements.








When you click a directory object in the left navigation tree, you see a list of its children in the content pane. When you rest the cursor over the name of a child object in the list, a drop-down menu becomes available – click the down-arrow to display the menu. The options available in the menu vary depending on the hierarchical context in which the object exists and the HPCA features that are currently enabled.

Figure 38 Directory Object View



The following table summarizes the actions that you can take from the drop-down menu for a child object.

Table 17 Actions Available from the Drop-Down Menu

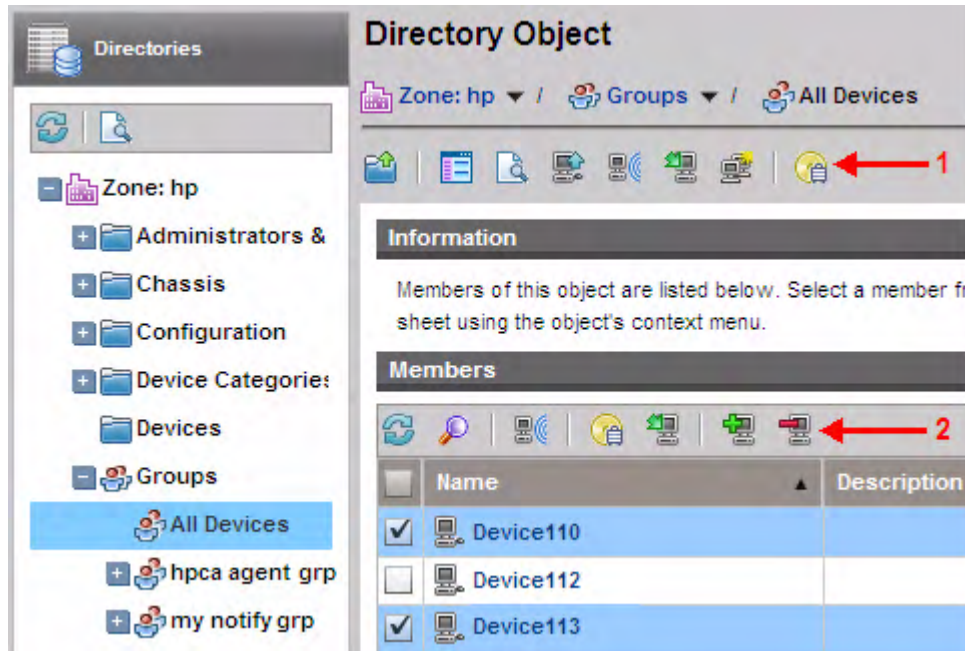
Icon	Action	Description
	View/Edit Properties	View or edit the properties of this child object in a new browser window. See Directory Object View on page 144.
	Create a Job	Create a Notify or DTM job for this object. See Managing Jobs on page 158.
	Remote Control	Access a managed device remotely. See Controlling Devices Remotely on page 180
	Deploy HPCA Agent	Deploy the HPCA Agent to this device so that it can be managed by HPCA. See Deploying the HPCA Agent on page 156.
	OS Management	Deploy an operating system, or perform a one-time hardware maintenance operation. See Managing Operating Systems on page 186.
	View Out of Band Details	View the Out of Band details for a device with Intel vPro or DASH-enabled devices. See Viewing Out Of Band Details on page 200.
	Delete this Directory Object	Delete this object from the HPCA database. See Importing Devices on page 153.

In the Directory Object view, there are two toolbars:

- The upper toolbar pertains to the object selected in the Directories tree.
- The lower toolbar pertains to the selected child objects in the grid.

In the example shown in [Figure 39](#) on page 146, the All Devices group is selected.

Figure 39 Directory Object View Toolbars



In this example, the upper toolbar (1) pertains to the All Devices group, and the lower toolbar (2) pertains to the selected Children (or Members) in the grid – in this case, Device110 and Device113.

View an Object's Properties

When you select **View/Edit Properties** for a directory object, the properties of this object are displayed in a new browser window (see [Figure 40](#) on page 147).

Figure 40 Directory Object Properties Window

Directory Object [?]

Zone: HP / Devices / serdar.cnd.hp.com

Zone: HP / Devices / serdar.cnd.hp.com


Properties

- Children
- Policies
- Entitlements
- Jobs
- Job Executions

Information

All properties for this directory object are listed below.

Device Summary



DNS Hostname: Device110.mycompany.com
 Operating System: Windows Vista
 Service Pack: Service Pack 1
 System Manufacturer: Hewlett-Packard
 System Product Name: hp workstation xw8200
 System Serial Number: 132705
 IP Address: 208.77.188.166
 MAC Address:

OS Management

OS State: ✔ Normal

Assigned Operating System:

Assigned Hardware Configuration Objects:

Properties

Name	Value
Common Name	Device110.mycompany.com
Create Time Stamp	Wed Mar 18 14:19:35 GMT-0600 2009
Created By	cn=hp,cn=radia
DNS Hostname	Device110.mycompany.com
Display Name	Device110.mycompany.com
Distinguished Name	cn=Device110.mycompany.com,cn=device,cn=hp,cn=radia

33 of 33 records shown

From here, you can perform the following actions:

- Click **Children** to view the object's children. Click a child object to browse to that object in the content pane.
- Click **Members** to view the object's members. If the object has no members, this link is not present.
- Click **Policies** to view the object's local policy configuration, and to create policies for this object.
- Click **Entitlements** to view all resolved policies for this object.
- Click **Jobs** to view a list of current and past jobs for this object. If there are no jobs for this object, this link is not present.
- Click **Job Executions** to view a list of DTM job executions for this object. See [Jobs and Job Executions](#) on page 160 for more information.
- Click **Virtual Machines** to view a list of the virtual machines that exist on the server. This link is available only if the selected object is a VMware ESX Server. For additional information, see [Managing Virtual Machines](#) on page 173.

Search for an Object


The HPCA Console provides the ability to search for directory objects. This search is contextual. This means that when you initiate a search, the root of that search is the current directory object. You can initiate a search from either the main window or the Directory Object window—both contain a search button.



Directory Objects that contain a large number of children may time out when retrieving a large number of records. Although the console may time out, the background process will continue to retrieve data until it reaches 10,000 records. If this happens, click the **Refresh** button to try the request again.

For directory objects with greater than 5000 child nodes, use the Search interface to navigate to a node within that list. This method will allow you to bypass possible time outs when browsing nodes with a large number of children.

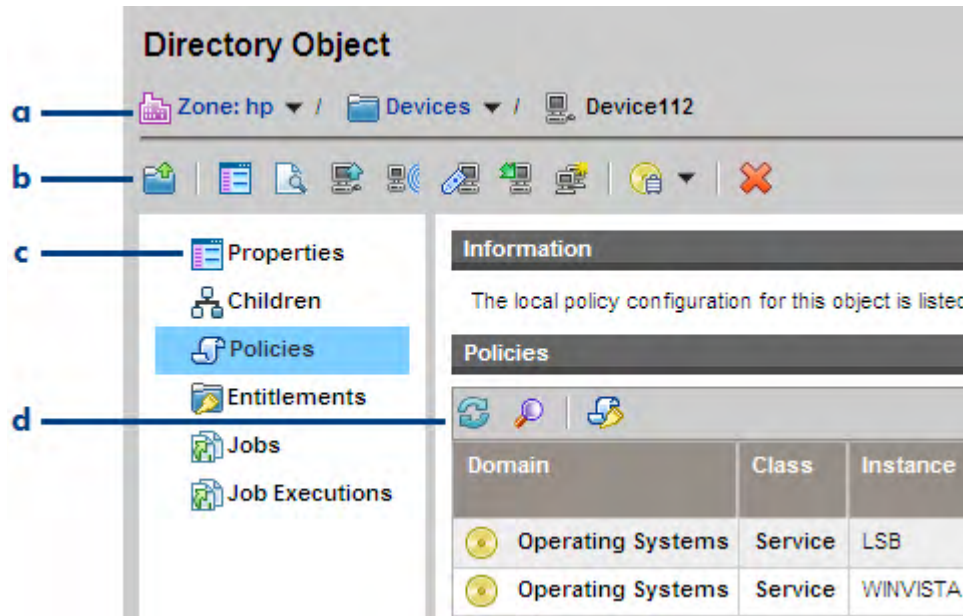
To search for a directory object:

- 1 From the Management tab, **Directories** area, click the Search Directories  button.
- 2 From the Directory Search box, you can define the following parameters:
 - Specify the distinguished name (DN) for the search by selecting an item in the left navigation menu.
 - Select the **Scope** of the search: either the current level or the current level and all levels below it in the directory hierarchy.
 - Create a **Filter** expression by selecting an attribute, an operator, and typing in the criteria to match.
 - ▶ When using the OBJECTCLASS filter, the only valid conditions are Equals or Does Not Equal. Also, certain directories, such as Active Directory, do not support wildcard characters included in the search strings for some attributes.
- 3 Click **Search**. The objects that match the criteria you specified are listed in the Search Results table.
- 4 Click **Reset** to begin a new search.






Manage Policy for Directory Objects


From the Directory Object properties window (see [Figure 40](#) on page 147), you can manage the local policy configuration for an object.


Figure 41 Directory Object Policy Detail





Legend


- a** Path to selected directory object
- b** Directory object toolbar:
 -  Browse to the parent object
 -  View/Edit properties of this object
 -  Search directories
 -  Import devices into the HPCA device repository
 -  Create an HPCA job

 Start a new remote control session

 Deploy the HPCA Agent


 Create a new group


 Perform an OS Management task


 Delete this Directory Object

c Object links (see [View an Object's Properties](#) on page 146)

d Policy Management toolbar:

 Refresh

 Show/Hide filter

 Launch the Policy Management Wizard

To manage policy of directory objects:


- 1 On the **Management** tab, click **Directories**. The list of available directory services expands.
- 2 Click the directory service that you want to expand.
- 3 Click a container or child of that directory service.


To work with a specific directory object, navigate to that object, and select **View/Edit Properties** from the drop-down menu. A new browser window opens for that directory object.

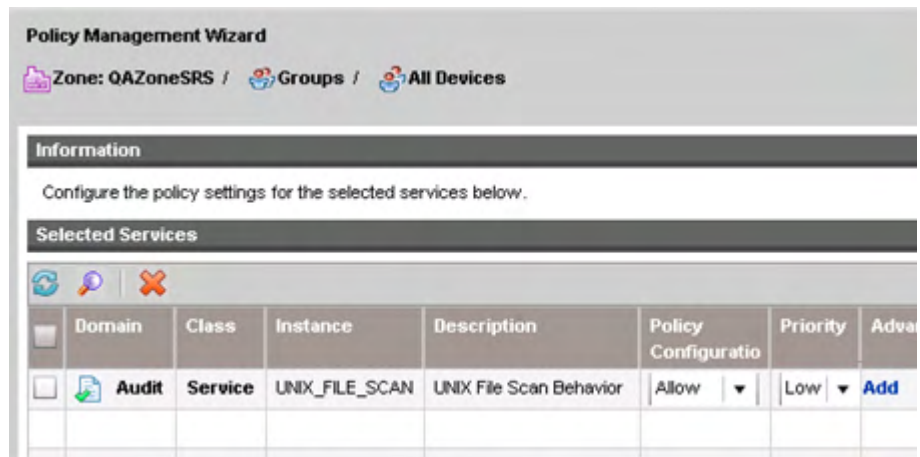
In our example we will create a policy for one device.

[Figure 41](#) on page 150 explains the different sections of the Directory Object window.

- 4 Click the **Policies** link in the left navigation menu..

 When you click the **Policies** link, the HPCA Console checks your permissions. If you do not have write permissions, the Policy Management Wizard button is disabled (gray).

- 5 Click the **Policy Management Wizard**  button.
- 6 In Step 1 of 3: Service Selection, you will select the services that you want to add to the object's policy. Select the Configuration Server Database Domain from which you want to select the Service.
- 7 Select the box to the left of each service that you want to add.
- 8 Click **Add to Selection** to move the service to the tree view on the right side of the wizard's screen.
- 9 Click **Next** when you have added all the services you need.
- 10 In Step 2 of 3: Policy Configuration, set the type of Policy and the Priority for each of the services. The example image below displays one Service from the Audit Domain.



- Set **Policy Configuration** to either Allow or Deny.
- Set **Priority** to Low, Medium, or High.
- Click **Add** in the **Advanced** column to add additional Client Automation attributes and expressions to the criteria for an object. See the *Policy Server Guide*.



The **Advanced** feature should only be used by experienced HPCA Administrators who are extremely familiar with the Configuration Server Database and the HPCA Infrastructure.


- 11 Click **Next** when you have configured the policies.

- 12 In Step 3 of 3: Configuration Summary, check your configuration. Click **Commit** to complete the Policy Management Wizard.
- 13 Click **Close** to acknowledge the dialog.

Service Information

After signing in to the HPCA Console, you can view the services that are available from your Configuration Server. A service is a set of data managed as a unit – for example, an application. Services are created using the CSDB Editor. Refer to the *Administrator Guide* for more information about services.

To view available services:


- 1 On the **Management** tab, click **Services**. The list of available Configuration Server Database Domains opens.
- 2 Click the Domain that contains the Services that you want to see.
- 3 To narrow the list of available services displayed, click the **Show/Hide Filter Input** button  to display the filter options.
- 4 Click a Service to view its details.
 - The **Catalog** tab shows the attributes of the Service from the Configuration Server Database (CSDB).
 - The **Reporting** tab shows summary reports on the Service.


Importing Devices

Before you can deploy the HPCA Agent to a device, you must import that device into HPCA. You must also import any VMware ESX Server that you want to manage using HPCA.


When you import a device, a directory object is created for that device. No attempt is made, however, to verify that you have specified a valid device.

To import devices

- 1 On the **Management** tab, go to the Directories area, and click **Devices**.
- 2 Click the  (Import Device Wizard) button.
- 3 In the **Device IP/Host Name** text box, type or paste a comma-separated list of device host names or IP addresses.
- 4 In the Device Classification drop-down, select the appropriate classification for the group of devices.
 - **No Preset Classification** – Devices are imported with no classification.
 - **VMware ESX Server** – Enables the Virtual Machines link in the Directory Object window for each device imported with this classification. See [Managing Virtual Machines](#) on page 173.
- 5 Click **Add**. Devices are added to the import Devices list.

To remove a device from the list, select the check box to the left of the device and click the  (Remove) button.
- 6 Review the list, and click **Commit**. Devices are imported into the Devices container. They are also added to the All Devices group.
- 7 Click **Close** to acknowledge the dialog.

To remove a device:

To remove a device that was previously imported, browse to the device object page and click the  (Delete this Directory Object) button.

Managing Groups




Groups are used to perform tasks on many devices at once, such as deploying the HPCA Agent or creating a job to notify devices when updated software is available. Devices are added to groups based on search criteria that you define during group creation. The following sections describe the different group management tasks available.

To create an external directory group:


Groups for mounted external directory sources (LDAP or Active Directory, for example) must be created using the tools provided by the directory service. Contact your system administrator for details.

To create an internal directory group:



The following procedure creates groups for internal directories. Groups that you create in the HPCA Console are created in the internal zone under the Groups container.

- 1 On the Management tab tool bar, click **Create a New Group** .
The HPCA Group Creation Wizard opens.
- 2 Type a name and description for the group.
- 3 Click **Add Devices** .
The Add Devices window opens.
- 4 Define Search Parameters and click **Search** to display a list of devices. (Clicking **Search** without defining parameters will return a list of all available devices).
- 5 Select the devices that you want to add, and click **Add**.
When you are finished adding devices, close the Add Devices to a New Group window.
- 6 To remove devices, select the devices in the Members grid, and click **Remove Devices** .
- 7 Click **Submit**. The new group is added to the Groups container within the internal zone.


To modify a group description or devices:

- 1 Use the navigation tree, and select the group that you want to modify.
- 2 Use the tool bar or the group context drop-down menu, and select **View/Edit Properties** .

The group's directory object window opens.

- 3 Click the **Properties** link to view the properties page and to modify the group name or description. Click **Save** to commit any changes.
- 4 Click the **Members** link to view the list of devices that belong to the group.
- 5 Use the **Add Devices**  or **Remove Devices**  tool bar buttons to update group membership.
- 6 When you are finished, close the directory object window.

To remove a group:

- 1 Use the navigation tree, and select the group that you want to remove.
- 2 Click **Delete this Directory Object** .

This removes only the group object. It does not remove the devices in the group.

Deploying the HPCA Agent

The HPCA Agent is used to manage devices in your environment. Deploy the Agent to devices using the Agent Deployment Wizard. For additional information about the HPCA Agent, refer to the *HP Client Automation Application Manager and Application Self-Service Manager Guide*.

You can deploy the Agent to single devices or to devices belonging to a group. Use the directory object tree to locate the devices, then use the Agent Deployment Wizard to create a deployment job.

In order for the Agent to be deployed successfully, the following may be required on the client devices:


- Windows Firewall should be disabled.

- The Agent must be reachable by the server over the network.
- If deploying to Windows XP, Simple File Sharing must be disabled.
- If deploying to Windows Vista, 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 Agent deployment. If the devices are not part of a domain, additional steps are required to allow access for local administrators. See the following link on Microsoft's support web site for detailed steps:

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

After making these changes, reboot the device.

To deploy the HPCA Agent

- 1 From the directory object tree, select the directory object that contains the devices to which you want to deploy the Agent.
- 2 Select the devices from the list and click **Launch the HPCA Agent Deployment Wizard** . The Agent Deployment Wizard opens.
- 3 At **Step 1**:
 - a Specify the credentials to use when deploying the Agent. These credentials should have adequate administrator permissions to perform the installation.
 - b To install the Agent in silent mode, select the **Silent Install** check box. This will prevent an installation user interface from opening on the target device.
- 4 Click **Next**.
- 5 At **Step 2**, enter the schedule information for when the Agent Deployment job should run.
- 6 Click **Next**.
- 7 At **Step 3**, review the summary information for the job.
- 8 Click **Submit**.

When you finish the steps in the wizard, an Agent Deployment job is created. A deployment job is complete when the Agent has been deployed to all devices included in the job. Use the **Jobs** area (see [Managing Jobs](#) on page 158) to view the status of any jobs.

Managing Jobs

Use the Jobs area on the Management tab to view and manage current and past jobs. The Jobs area includes two categories:

- The **All Jobs** category lists jobs submitted by all HPCA Console users.
- The **My Jobs** category lists jobs submitted by the HPCA Console user who is currently signed on.

Each category contains a list of **Current Jobs** that are either running or waiting to run and **Past Jobs** that have finished running.

You can manage three different types of jobs in the HPCA Console:

Table 18 Types of Jobs

Job Type	Description
Notify	The HPCA Console tells the target devices to connect to the Configuration Server in order to perform a certain action. This is a centralized (server-push) method of job management. The HPCA Console uses an internal process engine to manage these types of job.
Distributed Task (DTM)	The target devices periodically synchronize themselves with the HPCA Core and receive instructions to perform a particular action according to a specified schedule. You can configure and manage this schedule in the HPCA Console. This is a distributed (client-pull) method of job management, because jobs can run independently of the HPCA Core.
Deployment (RMP)	These jobs involve Agent or OS deployment. You can view information about RMP jobs in the HPCA Console, but you cannot modify it. Deployment jobs, like Notify jobs, are managed centrally (server-push).

Current and Past Jobs

The Current Jobs page lists jobs that are running or waiting to run. The Past Jobs page lists jobs that have finished running. For each job, the following information is shown:

Job ID – The unique identifier for this job. This ID is assigned by HPCA when the job is created. To see the job details for a particular job, click its Job ID.

Type – Notify, DTM, or RMP.

Display Name – The name specified when the job was created.

State – Enable, Disabled, Running, Completed, or Scheduled. Jobs that are enabled can be scheduled to run on target devices.

Status – The current status of the job: Success, Failure, or Unknown (while the job is either Running or Scheduled).

Description – A text description specified when the job was created.

Schedule – The schedule associated with the job.

Target – The target device or group where the job will run.

Action – The action that is taken when the job runs on the target devices.

Create Time – The date and time when this job was created.

Created By – The HPCA Console user who created the job.

Last Execution Time – The date and time that the job was last run. If the job has never been run before, the date of 12/31/1969 is displayed.

Use the buttons at the top of the Jobs table to perform the following actions:

Table 19 Jobs Table Controls






Icon	Description
	Refresh data
	Show/Hide filter input

Table 19 Jobs Table Controls

Icon	Description
	Delete the selected job (or jobs)
	Enable the selected job (or jobs) – applies to current DTM jobs only
	Disable the selected job (or jobs) – applies to current DTM jobs only

Jobs and Job Executions

A **job** is the framework that defines the parameters for a particular action and target device or group. A job consists of three primary components:

- Target – a device or group of devices on which the job will run
- Action – the command that will be performed
- Schedule – when the action should be executed on the target

When a job is running, waiting to run, or has finished running, a **job execution** represents an instance of that job on a particular device.

Targets

A target is a single device or a group of devices on which a job will run. This is typically an Active Directory group whose members can change over time. The target is specified when the job is created.

The Target Details window provides information about the target devices associated with one or more jobs. The window contains three tabs:

- The **Target Devices** tab contains a list of all the devices associated with this job. To view information about a particular device, select **View/Edit Properties** from the shortcut menu for that device.
- The **Job Executions on Target** tab shows you any job executions that are scheduled to run, are running, or have run for this job on this target (or target group).
- The **All Jobs for Selected Target** tab shows you all the jobs that use this target (or target group).

To access the Target Details window:

- 1 In the Current Jobs or Past Jobs table, click a **Job ID**.
- 2 In the Job Details window, click the **Properties** tab.
- 3 In the Target section, click the target group or device name.

You can also access the Target Details window by selecting a value in the **Target** column in either the Current Jobs or Past Jobs table.

Schedules

You can schedule a DTM task to run once at a particular time or periodically according to the parameters that you specify.

The Schedule Details window enables you to view information about the schedule associated with an existing DTM job. If this job is a current job, you can also modify the schedule.

To access the Schedule Details window:

- 1 In the Current Jobs or Past Jobs table, click a **Job ID** for a DTM job.
- 2 In the Job Details window, click the **Properties** tab.
- 3 In the Schedule section, click **Modify**.

To specify a schedule for a DTM job:

- 1 From the **Begin** task list, select **On a schedule** or **At startup**.
If you select At Startup, you can skip the rest of these steps.
- 2 Select the frequency with which this job should run: once, hourly, daily, weekly, or monthly.
- 3 If you selected a frequency other than “once,” specify the **Every** information to define the recurrence interval for this job.
- 4 Specify the **Start Date** for the job.
- 5 If you want to stop initiating new job executions for this job on a certain date, select the check box to the left of the **End Date** field, and specify the end date.
- 6 Specify the **Start Time** for the job.

- 7 If you want to stop initiating new job executions for this job at a certain time, select the check box to the left of the **End Time** field, and specify the end time.
- 8 If you want the job to start at a randomized time between your Start Time and End Time, select the **Randomize Start Time** box.

See [Create a New DTM or Notify Job](#) on page 166 for more information.

Job Details for DTM Jobs

When you click a Job ID for a DTM job in either the Current Jobs or Past Jobs tables, the Job Details window opens, and the following information is displayed:

- The **Summary** tab displays the ID, name, description, and creation time for the job as well as the job's current state (Enabled, Disabled, or Completed). This tab also includes a pie chart that shows you the status of the job on the target devices (Success, Failure, Warning, or Unknown).

When a job execution for this job is running, the status is Unknown.

A DTM job is moved to the Completed state when an End Date is used in its schedule, and this End Date has passed.

- The **Properties** tab contains information about the job, including the description, action, target, and schedule used to create the job.

For information about the target devices associated with this job, click the target name. See [Targets](#) on page 160

To view or change the schedule for this job, click the **Modify** schedule link. You can only modify the schedule for current jobs. See [Schedules](#) on page 161.

- The **Job Executions** tab shows the job executions that have been scheduled for this job. This includes job execution that have already completed.

To view more information about a particular job execution, click the **Id** for that job execution in the table. The Job Execution Details window opens. See [Job Execution Details](#) on page 164.

The Job Details window contains slightly different information for Notify jobs. See [Job Details for Notify Jobs](#) on page 163.

Job Details for Notify Jobs

When you click a Job ID for a Notify job in either the Current Jobs or Past Jobs tables, the Job Details window opens, and the following information is displayed:

- The **Summary** tab displays the ID, name, description, and creation time for the job as well as the job's current state.

Table 20 Notify Job State Descriptions

State	Description	Example
Scheduled	The job has not yet started running.	A Notify job has been scheduled to run at some point in the future but has not yet started.
Running	The job has not yet reached the end state. Running jobs are included in the Current Jobs list.	A running Notify job is in the process of notifying each device.
Completed	The job has reached its end state, and all steps have been processed. Completed jobs are included in the Past Jobs list	A Notify job is complete when all devices included in the job have been notified.

This tab also includes a pie chart that shows you the status of the job on the target devices (Running, Success, Failure, Warning, or Unknown).

- The **Properties** tab contains information about the job, including the action, target, and schedule used to create the job.

For information about the target devices associated with this job, click the target name. See [Targets](#) on page 160

- The **Job Executions** tab shows the status of the *most recent* job execution on each target. This includes job executions that have already completed.

To view more information about a particular job execution, click the **Id** for that job execution in the table. The Job Execution Details window opens. See [Job Execution Details](#) on page 164.

The Job Details window contains slightly different information for DTM jobs. See [Job Details for DTM Jobs](#) on page 162.

Job Details for RMP Jobs

When you click a Job ID for an RMP job in either the Current Jobs or Past Jobs tables, the Job Details window opens. The information displayed is the same as that displayed for a Notify job (see [Job Details for Notify Jobs](#) on page 163).

Job Execution Details

For DTM jobs, the Job Execution Details tab lists the most recent job execution for each job that is currently running or has finished running on all target devices. For Notify and RMP jobs, this tab lists the most recent job execution for each job that is currently running, is waiting to run, or has finished running on all target devices.

The following information is displayed:

ID – The unique identifier for this job execution. Note that this ID pertains only to this execution (instance) - it is not the same as the Job ID specified in the Jobs table. To see the job details for a particular job execution, click its ID.

Type – Notify, RMP, or DTM (distributed task)

State – Running, Completed, or Waiting to Start (for Notify and RMP jobs). See [Job Execution States](#) on page 165.

Description – A text description specified when the job execution was created.

Summary – A status message pertaining to the job execution.



Start Time – For current jobs, this is the time this job execution is scheduled to start on the target devices. For past jobs, this is the time that the job execution started.

End Time – For current jobs, this is blank. For past jobs, this is the time that this job execution stopped.

Job – The Job ID of the job on which this execution is based.

You can use the buttons at the top of the table to manage existing job executions:

Table 21 Job Executions Actions

Icon	Description
	Refresh data
	Show/Hide filter input

Note that some buttons are only available during certain job states. A job execution that has completed, for example, would not have a Resume, Pause, or Cancel button.

Click the Job ID of any job to open the Job Details window. See [Job Details for Notify Jobs](#) on page 163 or [Job Details for DTM Jobs](#) on page 162 for additional information. See [Job Execution States](#) on page 165 for additional information about the status of each job.

Job Execution States

HPCA Console job executions can include any number of steps, depending on the job type. For example, Notify jobs include a step for each device to be notified. The execution status of those steps determines the current job execution state.

Table 22 Job Execution State Descriptions


State	Description
Running	The job execution has not yet reached the end state. Running job executions are included in the Current Job Executions list.
Completed	The job execution has reached its end state and all steps have been processed. Completed job executions are included in the Past Job Executions list
Waiting to Start	The job execution is based on a job that is in the Scheduled state.

Create a New DTM or Notify Job

You can use the HPCA Job Creation Wizard to create a new DTM or Notify job. To create a new Agent deployment job, see [Deploying the HPCA Agent](#) on page 156. To create a new OS deployment job, see [Managing Operating Systems](#) on page 186.

To create a new DTM or Notify job:

- 1 On the Management tab, go to the Directories area, expand the zone that you want to use.
- 2 Display the list of **Groups** or **Devices** that you want to work with.
- 3 From the drop-down menu for the group or device, select **Create a Job**. The HPCA Job Creation Wizard opens.

Alternatively, you can select one or more groups or devices from the grid and then click the **Launch HPCA Job Creation Wizard**  icon on the toolbar.

- 4 In the **Job Type** list, select **DTM** or **Notify**.

In a DTM job, the agents on the target devices connect to the HPCA Core server to get a list of jobs and then execute those jobs when the job timers expire. A DTM job is most appropriate when you want to execute this job on a regular schedule on these devices.

In a Notify job, the HPCA Core server asks the HPCA Agent to perform the scan. A Notify job is most appropriate when you want certain target devices to execute the job once at a specific time – or immediately.


- 5 Specify a **Name** and **Description** for your job.
- 6 In the **Job Action Template** list, select the Job Action Template that you want to use for this. See [Job Action Templates](#) on page 276 for more information.
- 7 If you want to specify parameters for the job action that are not specified in the Job Action Template, enter those in the **Additional Parameters** box.
- 8 Click **Next**.
- 9 Specify the schedule for this job. See [Schedules](#) on page 161 for details.
- 10 Click **Next**.
- 11 Review the settings you have specified, and click **Submit** when ready.

To view the job, click the Jobs area on the Management tab.



If you modify the schedule for a DTM job, you must refresh that schedule on each of the target devices. See [Removal of Old Job Execution Records](#) on page 170.

Delete a Job

To delete a current or past job, select the job in the Current Jobs or Past Jobs table, and click the **Delete Selected Job**  icon. Please note the following:

- Notify jobs that are currently running cannot be deleted.
- For DTM jobs, the job disappears from the Current Jobs list when you click the icon, but job executions from that job remain visible in the Directory Object view for each target device (select **View/Edit Properties** to display).

After you delete a DTM job, that job is no longer available to be downloaded to target device in subsequent agent synchronizations with the HPCA Core server. Target devices that already have the deleted job can still execute the job until they synchronize with the HPCA Core server.

Refresh DTM Schedules on Targets

If you modify the schedule for a DTM job on the HPCA Core server, you must also refresh that schedule on each target device. You can do this by creating a job using the Refresh DTM Job Schedules sample job action template.

By default, there is a DTM_DAILY_TIMER in the Configuration Server Database (CSDB) that can be entitled to a managed device to instruct its agent to perform a synchronization with its Core server once a day for job information.


A Refresh DTM Schedules job provides another way to schedule the synchronization with the Core server. For example, a Refresh DTM Schedules job can be created to ask agents to synchronize with the Core server every 12

hours for job information. To the agent of a target device, this Refresh DTM Schedules job will be run just as any other agent job – such as a Software Connect – when the job timer expires.



Before you can successfully run a Refresh DTM Schedules job on a client device, the HPCA Agent on that client must have performed a prior connect operation to the HPCA Core server.

To create a Refresh DTM Schedules job:

- 1 In the Management tab, **Directories** area, navigate to the object that contains the target devices for the pertinent DTM job (or jobs).
- 2 Select the target devices that you want to refresh.
- 3 Click the  tool bar icon to launch the **HPCA Job Creation Wizard**.
- 4 To refresh immediately, select **Notify** from the **Job Type** drop-down box. To refresh on a schedule, select **DTM**.

If you select **DTM**, when the target devices synchronize with the Core server, they will acquire this job. It will instruct them to connect back to the Core server for job information based on the schedule settings that you specify.

If you want agents to use the new synchronization schedule sooner, it might be helpful to *also* schedule a **Notify** Refresh DTM Schedule job to instruct the agents on target devices to synchronize with the Core server at a specified time and *then* download the **DTM** Refresh DTM Schedules job.

- 5 Enter a name and description for the refresh job.
- 6 In the **Job Action Template** list, select **Refresh DTM Job Schedules**
- 7 Click **Next**.
- 8 Enter the schedule settings (see [Schedules](#) on page 161), and click **Submit**.

The job is added, and the target devices will refresh their DTM job schedules based on the settings that you defined.

To view the status of the job, click the **Jobs** area on the Management tab.

Device Resolution for Notify Jobs

Devices included in a Notify Job are resolved according to the order defined in the following file:

```
<tomcatDir>\webapps\em\web-inf\console.properties
```

By default, <tomcatDir> is as follows.

```
C:\Program Files\Hewlett-Packard\HPCA\tomcat
```

The default order is:

```
group.target.host.attributes=ipaddress,dnshostname,displayname,cn
```

If necessary, this list can be modified. If you make changes to this file, you must restart the HPCA Tomcat service.

For devices that could not be resolved, a message is displayed in the Job Details window, Details tab. You can open the Job Details window by clicking the Job ID.

Device Resolution for DTM Jobs

Devices included in a DTM job are resolved in the following order:

- 1 ipaddress
- 2 dnshostname
- 3 displayname
- 4 cn

A service periodically runs to resolve target devices for DTM jobs. This service is configurable in the following file:

```
<tomcatDir>/webapps/ope/config/dtm.properties
```

Table 23 Parameters for Device Resolution Service for DTM Jobs

Parameter	Default Value	Comment
enableTargetRefresh	true	Enables or disables this service
rmpProtocol	http:\\	Can be https:\\ for SSL
rmpServer	localhost	HPCA Portal server

Table 23 Parameters for Device Resolution Service for DTM Jobs

Parameter	Default Value	Comment
rmpPort	3466	Portal server port to which to connect
rmpUser	SYSTEM	
rmpPassword		Not shown here for security
userDS	""	User directory to which to connect
targetRefreshInterval	360	Default is 6 minutes (360 seconds)
targetRefreshInitDelay	60	Seconds to wait after startup before DTM starts the target resolution service

Removal of Old Job Execution Records

You can specify how long records of past DTM and Notify job executions are stored in the HPCA database. You can also specify the maximum number of records that should be stored. This is configured in the following file:

```
<tomcatDir>\webapps\ope\config\dtm.properties
```

By default, <tomcatDir> is as follows.

```
C:\Program Files\Hewlett-Packard\HPCA\tomcat
```

Use the following parameters to specify these settings:

```
dtmJobRunKeepDays=30  
opeJobRunKeepDays=30  
dtmJobRunKeepRecords=-1  
opeJobRunKeepRecords=-1
```


The default settings are shown here. for the period of time specified by these parameters. The value of -1 indicates that there is no limit on the number of records that can be stored.

Creating Satellite Synchronization Jobs

Satellite Servers are used to allow for data caching and the distribution of configuration settings to managed devices. Satellites must be synchronized with the Core server in order to make the latest data available to those devices. You can perform a synchronization from the Satellite Console, or this synchronization task can be scheduled by creating a job in the HPCA Console.

- ▶ Before you can synchronize data on a Satellite Server, you must have initially configured your Satellites. Refer to the *HPCA Core and Satellite Getting Started and Concepts Guide* for details.
- ▶ Before you can successfully run a Satellite Synchronization job on a client device, the HPCA Agent on that client must have performed a prior connect operation to the HPCA Core server.

To create a Satellite Synchronization job:

- 1 In the Management tab, **Directories** area, navigate to the object that contains the Satellite device.
- 2 Select the Satellite device and launch the **HPCA Job Creation Wizard** by clicking the  tool bar icon.
 - ▶ If you select a device that is not a Satellite server, the job will fail.
- 3 To synchronize a satellite immediately, select **Notify** from the **Job Type** drop-down box. To synchronize on a schedule, select **DTM**.

If you select **DTM**, this Satellite Synchronization job will be downloaded to the Satellite only *after* the agent on the Satellite device has performed a Refresh DTM Schedule.
- 4 Enter a name and description for the synchronization job.
- 5 Select the **Job Action Template** for the synchronization type you would like to schedule:
 - **Satellite Synchronization (All)**

Select this template to synchronize both configuration settings and data.
 - **Satellite Synchronization (Configuration)**

Use this template to synchronize only configuration settings.

— **Satellite Synchronization (Data)**

This template will synchronize data, only.

6 Click **Next**.

7 Enter the schedule settings (see [Schedules](#) on page 161), and click **Submit**.

The job is added and the Satellite server will synchronize data or configuration settings based on the settings you defined.

To view the status of the job, click the **Jobs** area of the Management tab.

Managing Virtual Machines

The HPCA Console enables you to manage the virtual machines running on your virtual hosting servers. For example, you can create and manage virtual machines on an existing VMware ESX Server in your environment.


To manage your virtual machines:

- 1 On the **Management** tab, expand the zone containing the devices that you want to manage.
- 2 In the left navigation tree, click **Devices**.
- 3 In the list of devices, locate your ESX Server in the list of devices.
- 4 In the drop-down menu for this device, click **View/Edit Properties**. A separate browser window opens, as shown on [Figure 40](#) on page 147.
- 5 In the Directory Object window for your ESX Server, click the **Virtual Machines** link in the left navigation menu.

► The Virtual Machines link is only visible if this device was imported using the **VMware ESX Server** device classification. See [Import Devices](#) in the Configuration chapter for more information.

If this is the first time you have clicked this link for this ESX Server during this HPCA Console session, you will need to provide login credentials:

Virtual Host Server Authentication

 Initialize connection to VirtualHost Server myESXserver succeeded.

Required Fields *

Server URL: *

User ID: *

Password: *

Enter the **User ID** and **Password** for the ESX Server, and click **Sign In**.

A list of the virtual machines hosted by this ESX Server is displayed, as shown in [Figure 43](#) on page 176.

To view the properties for a particular virtual machine, click its name.

Figure 42 Device Properties for a VMware ESX Server

Directory Object ?

Zone: hp / Devices / myESXserver

Properties

- Children
- Policies
- Entitlements
- Jobs
- Job Executions
- Virtual Machines

Information

All properties for this directory object are listed below.

Device Summary

DNS Hostname: myESXserver

Operating System:

Service Pack:

System Manufacturer:

System Product Name:

System Serial Number:

IP Address:

MAC Address:

OS Management

OS State: ✔ Normal

Assigned Operating System: WINVISTA

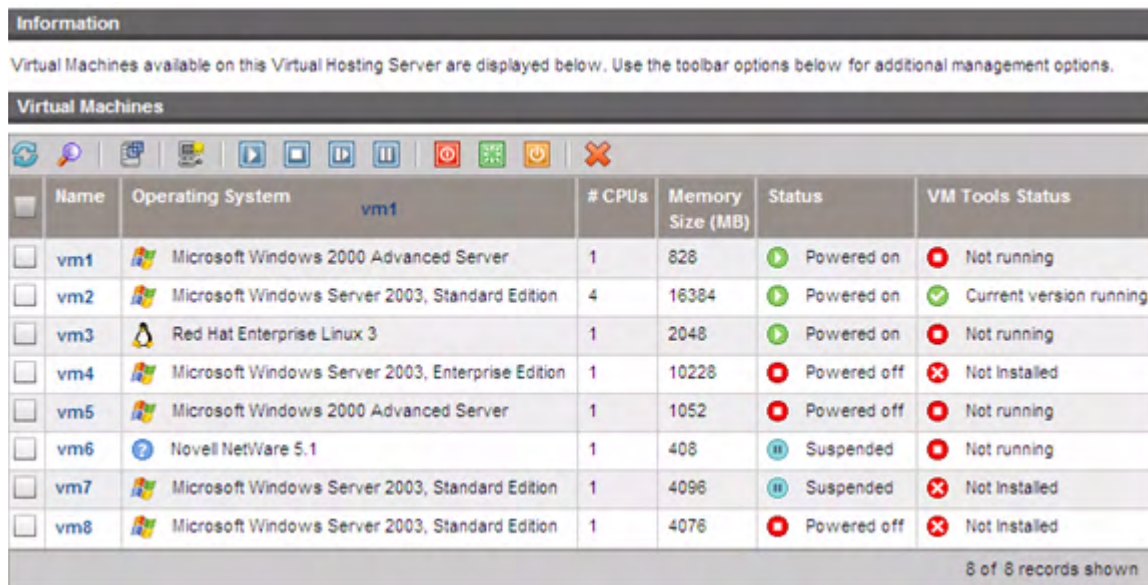
Assigned Hardware Configuration Objects:

Properties

Name	Value
Common Name	myESXserver
Create Time Stamp	Mon Aug 25 08:36:23 GMT-0600 2008
Created By	uid=admin,cn=user,cn=hp,cn=radia
DNS Hostname	myESXserver
Device Category	esxserver
Display Name	myESXserver

17 of 17 records shown

Figure 43 List of Virtual Machines Hosted by an ESX Server



The columns in the Virtual Machines list contain the following information:













Table 24 Virtual Machine List Columns

Column Name	Description
Name	The name of the virtual machine
Operating System	The operating system of the virtual machine
# CPUs	The number of CPUs allocated to the virtual machine
Memory Size	The amount of memory allocated to the virtual machine
Status	The current status of the virtual machine
VM Tools Status	The current status of the VM tools on the virtual machine

Click the name of a virtual machine to open the Virtual Machine Properties window for that machine.

You can use the following controls to create and manage virtual machines on your ESX Server:


Table 25 Virtual Machine Toolbar

Icon	Description
	Refresh Data
	Show/Hide Filter input
	Display VM Host System Properties
	Create New Virtual Machine
	Suspend the Selected Virtual Machines
	Reset the Selected Virtual Machines
	Stop the Selected Virtual Machines
	Start the Selected Virtual Machines
	Standby OS on the Selected Virtual Machines ¹
	Reboot OS on the Selected Virtual Machines ¹
	Shutdown OS on the Selected Virtual Machines ¹
	Delete the Selected Virtual Machines

¹Requires VMWare Tools to be running on the virtual machines.


Select the check box for each virtual machine you want to manage, and then click the appropriate virtual machine control to complete the desired action.

Creating New Virtual Machines

The **Create New Virtual Machine**  control in the Virtual Machines table enables you to create a new virtual machine on the ESX Server by using the Virtual Machine Creation Wizard. This wizard prompts for information

similar to the information requested by the VMware virtual machine creation wizard. You should be familiar with VMware terminology before using this wizard.

To create a new virtual machine:

- 1 Follow steps 1-5 under [Managing Virtual Machines](#) on page 173 to open the Virtual Machines list for your ESX Server.
- 2 Click **Create New Virtual Machine** . The Virtual Machine Creation Wizard opens.
- 3 Provide the following information for the virtual machine you want to create:
 - **Data Center:** Use the drop-down list to select the data center in which to create the new virtual machine.
 - **Host System:** Use the drop-down list to select the host system for the virtual machine.
 - **Name:** Type a name for the virtual machine. Virtual machine names can be up to 80 characters long and can contain alpha-numeric characters, spaces, hyphens, and underscores. Virtual machine names must be unique within each data center and within each folder.
 - **Description:** Type a description of the virtual machine.
- 4 Click **Next**.
- 5 Use the drop-down list to select a **Data Store**. Be sure to select a data store with enough space to store the virtual machine and its virtual disk files.
- 6 Enter the **Disk Size**. Type or use the up and down arrows to enter the Disk Size in megabytes, or use the slider tool to enter the size in gigabytes.
- 7 Click **Next**.
- 8 Select the **Guest Operating System**, and then select the **Version** and **Operating System Policy** to assign to the new virtual machine. Available policies are defined by the HPCA OS Manager.
- 9 Click **Next**.
- 10 Type or use the drop-down list to enter the **Number of Virtual Processors** for the virtual machine. Note that a virtual machine cannot be assigned more processors than the actual number of logical processors on the host device.

- 11 Enter the virtual machine **Memory Size**. Type or use the up and down arrows to enter the memory size in megabytes or use the slider tool to enter the size in gigabytes. Minimum memory size is 4MB.
- 12 Click **Next**.
- 13 Use the drop-down lists to select the **Number of NICs** (Network Interface Cards) and the **NIC #1 Virtual Network** to configure for this virtual machine.
- 14 Select **Connect at Power On** if you want each NIC to connect to the network when the virtual machine is powered on.
- 15 Click **Next**.
- 16 Review the summary information and click **Commit**.
- 17 The virtual machine is created. View the new virtual machine in the Virtual Machines list. Click the virtual machine name to open the properties window.

Controlling Devices Remotely

The HPCA Console provides the capability to remotely access devices in either the internal or external repository using one of three methods:

- Windows Remote Desktop Connection
- Virtual Network Computing (VNC)
- Windows Remote Assistance

The HPCA Console attempts to determine the remote control capabilities of each target device and the best way to communicate with it. When you initiate a remote control connection to a particular target device, you can choose from the connection types that are available on that device.

For VNC and Windows Remote Desktop Connection, you must specify the port on which the remote devices will be listening for the remote connection. It is not necessary to specify a port for Windows Remote Assistance, because Windows Remote Assistance always uses a Distributed Component Object Model (DCOM) interface on port 135.




Your HPCA administrator can enable or disable remote control capability altogether or enable one or more specific remote control tools. See [Configure Remote Control](#) on page 286 for more information.

There are specific requirements that must be satisfied before each type of supported connection can be established. See [Requirements for Remote Connections](#) on page 181 for more information.

To access a device remotely:

- 1 Click the **Management** tab.
- 2 Expand the zone containing the device that you want to access remotely.
- 3 In the left navigation pane, click **Devices**.
- 4 In the right-click shortcut menu for the device that you want to access, click **Remote Control**.

You can also choose **View/Edit Properties** and then click the  (Remote Control) icon in the Directory Object window.

▶ If the HPCA Console cannot connect via Windows Remote Desktop Connection, VNC, or Windows Remote Assistance, an error message will appear when you click Remote Control.

- 5 For a Windows Remote Desktop Connection, specify the following:
 - **Method:** Select Windows Remote Desktop.
 - **Resolution:** Select the size of the Windows Remote Desktop Connection window on your screen.

For a VNC connection, specify the following:

- **Method:** Select VNC (Virtual Network Computing).

For a Windows Remote Assistance Connection, specify the following:

- **Method:** Select Windows Remote Assistance.

- 6 Click **Connect**. A new browser window opens, and your remote connection is established.

For VNC connections, you may first be required to provide a VNC password.

For Windows Remote Assistance connections, the user currently logged onto the target device must accept the connection.

Related Topics:

[Requirements for Remote Connections](#) on page 181

[Configure Remote Control](#) on page 286

[Remote Control Auditing](#) on page 185

Requirements for Remote Connections

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

- The remote device must be powered on.
- If the firewall is enabled, the remote access port on the remote device must be open.

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

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

Requirements for Windows Remote Desktop Connection

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

To use Windows Remote Desktop Connection, you must access the HPCA Console using Internet Explorer (version 6.0 or later). This is because the Console launches a wrapper that uses an ActiveX component when this type of connection is requested.

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

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

Requirements for VNC

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

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

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

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

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

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

You can use an Application Management Profile (AMP) to distribute the UltraVNC, RealVNC, and TightVNC server software to your client systems. AMPs for the preceding applications can be obtained from the AMP Community on the HP Live Network web site. For more information about AMPs, refer to the *Application Management Profiles User Guide*.

Requirements for Windows Remote Assistance

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

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

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

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

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

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

- Both the system where you are accessing the HPCA Console and the target devices must be joined to the same domain.
- The system where you are accessing the HPCA Console (the “Expert” system in the Windows Remote Assistance interaction) must have the following software installed:
 - Java Runtime Environment (JRE) version 5 (or later)

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

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

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

`domain_name\user_name`

`domain_name\groupname`

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

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

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

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

Firewall Considerations

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

Windows Remote Desktop Connection requires TCP port 3389.

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

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

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

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

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

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

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

Remote Control Auditing

Each time that anyone in your HPCA managed environment attempts to remotely connect to a managed device by using the HPCA Console, a remote control audit event is logged. The following information is recorded:

- Who initiated the remote control session and when?
- What was the target device?
- What type of connection was used?

You can view the remote control audit log by opening the Remote Control report in the Administrative Reports view.



The Remote Control report contains the following information:

Time – Date and time when the remote control event occurred

Connect Status – Description of the remote control event

User – HPCA Console User ID of the person who initiated the remote control event

Connection Type – VNC, Remote Desktop, or Remote Assistance

Target Host – Host name or IP address of the device that was accessed via remote control

HPCA Host – Host name or IP address of the system hosting the HPCA Console

You can sort the report based on any of these items by clicking the column heading. The gray arrow indicates the sort order.

Related Topics:

[Controlling Devices Remotely](#) on page 180

[Using Reports](#) on page 203

Managing Operating Systems

You can use the operating system (OS) management features of the HPCA Console to install, replace, update, or repair operating systems on your client devices. You can also use HPCA to perform various low-level tasks that must be completed before you can deploy an OS (for example, BIOS firmware updates, settings, and drive-configuration).

The following topics are covered here:

- [OS Management Terms](#) on page 187
- [Prerequisites for OS Management](#) on page 188
- [Deployment Scenarios](#) on page 189
- [How it Works](#) on page 192
- [Deploy an OS Image](#) on page 193
- [View the Status of OS Management Activities](#) on page 200

For a comprehensive discussion of OS management in HPCA, refer to the *HPCA OS Manager System Administrator User Guide*.

OS Management Terms

The following terms are used throughout this discussion of OS management in HPCA:

bare-metal device

A device that does not have a local OS installed.

HPCA Agent

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

hardware configuration object

An object stored in the HPCA database that contains information about how a target device's hardware must be configured in order for it to be ready for operating system installation.

local service boot (LSB)

LSB is an alternative to PXE that enables HPCA to assume management of the OS on devices that are not booted from the network.

You cannot use LSB in bare-metal or disaster recovery scenarios. You can only use LSB when you are migrating from one working OS to another or for performing low-level management tasks that are not related to drive management.

managed device

A device that is recognized and managed by HPCA.

preboot execution environment (PXE)

Network boot technology that initiates the HPCA Agent over the network.

reference machine

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

Service Operating System (Service OS)

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

target device

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

unmanaged OS

The term “unmanaged OS” applies in both of the following situations:

- A target device has been discovered, but policy has not yet been assigned to the device.
- Policy has been assigned, but you are not ready to overwrite the existing OS.

Prerequisites for OS Management

Before you can deploy an operating system (OS) using the HPCA Console, the following prerequisites must be in place:

- A suitable OS image must be available.
Refer to “[Preparing and Capturing OS Images](#)” in the *HPCA OS Manager System Administrator User Guide* for instructions.
- The OS image must be published to the HPCA Configuration Server Database (CSDB).
Refer to “[Using the Publisher](#)” in the *HPCA OS Manager System Administrator User Guide* for instructions.

In some cases, you may also want to create a suitable hardware configuration object for your target device (or devices). Refer to the *HPCA OS Manager Hardware Configuration Management Guide* for more information.

After these prerequisites are in place, you can use the OS Management Wizard in the HPCA Console to deploy and manage operating systems.

Deployment Scenarios

Deploying an OS 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 26 Deployment Scenarios

Device State	Instructions for deployment
Managed (HPCA Agent installed)	<p>If the device is already managed:</p> <ul style="list-style-type: none">• <i>Optional:</i> Add the device to a group.• Deploy the OS using the OS Management Wizard. <p>Note: If you use LSB during the OS deployment process, you will not need to make preparations for PXE or the ImageDeploy CD.</p>
Un-managed (HPCA Agent not installed)	<p>If the unmanaged device has an OS installed:</p> <ul style="list-style-type: none">• Deploy the HPCA agent to the device.• See instructions for Managed device above. <p>If unmanaged device does <i>not</i> have an OS installed:</p> <ul style="list-style-type: none">• See the instructions below for deploying an OS to a bare-metal device.
Bare-metal (no OS installed)	<p>If the device was previously managed (for hard drive recovery, for example):</p> <ul style="list-style-type: none">• Group membership and any OS entitlement should still be valid. Deploy the OS using either PXE or the ImageDeploy CD. <p>If the device was not previously managed:</p> <ul style="list-style-type: none">• Boot the device using either PXE or the ImageDeploy CD/DVD.• A device object is added to HPCA using a variation on the MAC address as the device name.• Deploy the OS using the OS Management Wizard.• Reboot the device using either PXE or the ImageDeploy CD/DVD. <p>Note: LSB cannot be used for deploying an OS to a bare-metal device.</p>



When you attach an OS to the All Devices group, devices that exist at that time are automatically entitled to that OS. If multiple OSs are attached to All Devices, then a choice of which OS to install is presented. Devices added after the OS is attached to All Devices are not automatically entitled to the OS.

Requirements for Target Devices

A target device is a workstation or server on which you want to install, update, or replace an operating system. A target device must meet the following requirements:

- The device 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.
- The device 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.
- The device must have an English, French, or German keyboard.
- The device must have 128 MB of RAM or more.
- If you are using a network (PXE) boot, the device 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.
 - 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, consider deploying the image on a target machine in a lab environment to confirm success of the deployment.

- The device must have an IDE or SCSI (Adaptec only) boot drive interface.
- The device must match the reference machine's ACPI characteristics (ACPI vs. non-ACPI, which is represented in the HAL) and boot drive interface.
- The device must be compatible with the programmable interrupt controller capabilities represented in the HAL captured on the reference machine. 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.
- The device must support NTFS and FAT32 file systems.
- Windows XPe 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 or Windows CE 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 managing the device. See “Installing the HPCA Agent on Thin Clients” in the *HPCA Core and Satellites Enterprise Edition User Guide* for installation instructions.

How it Works

You can use the OS Management Wizard to deploy an image to a single device, multiple devices that you select at the time, or an established group of devices – including Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) groups.

When you deploy an OS image to multiple devices (not an established group), a new dynamic group is created under Groups in the Directories area on the Management tab. This group contains all the devices that are targets for this OS Deployment. The name of the group begins with “OS Deployment” and includes the name of the OS that will be deployed. For example:

```
OS Deployment of WINXP Service to 2 devices (2009.Mar.11  
06:08:046 PM)
```

Whether you are deploying an OS to a single device or multiple devices, HPCA performs the following actions:

- Assigns selected images as an OS policy on each device.
- Modifies the ROM object under each device based on the specified OS deployment options.
- Creates a job of type RMP to perform a notification. You can check the status of this job on the Current Jobs page (see [Current and Past Jobs](#) on page 159).

View the OS Deployment State

If the OS for a device is being managed by HPCA, the OS deployment state is shown in the OS Management section of the Directory Object view for that device (select **View/Edit Properties** to display this view):

Waiting for OS Deployment – The OS deployment job is scheduled and is waiting to run.

OS Deployment In Progress – The OS deployment job is running.

Normal – The OS deployment job has successfully completed, and the OS is deployed.

Failed – The OS deployment job failed.

Unknown – The state of the OS deployment job cannot be determined.

Deploy an OS Image

Five steps are required to deploy an OS from the HPCA Console:

- 1 Select the target device (or devices) or an established group that contains devices.
- 2 Select the OS image to deploy.
- 3 *Optional:* Select a Hardware Configuration Object to use prior to the OS installation.

Although some target devices may be ready to have the operating system installed out of the box, there may be other situations when you need to identify and apply critical operations before proceeding with the operating system installation. Examples of the types of operations necessary are upgrading the BIOS firmware or configuring a disk array controller (DAC).

- 4 Choose the deployment type: LSB, PXE, or CD/DVD.

For LSB deployments, the HPCA Agent is required. See [Deploying the HPCA Agent](#) on page 156.



- 5 Specify when the deployment should occur.

Each of these steps is explained briefly here. For additional information, refer to the *HPCA OS Manager System Administrator User Guide*.

Before you attempt to deploy an OS image, be sure that the necessary prerequisites are in place. See [Prerequisites for OS Management](#) on page 188 and [Deployment Scenarios](#) on page 189.

To deploy an OS image:

- 1 On the **Management** tab, go to the Directories area, and expand the zone that you want to use.
 - To specify one or more individual target devices, click **Devices**.
 - To specify a group, click **Groups**.

 Groups used for OS deployment should have similar, compatible hardware.
- 2 In the Directory Object table, select the devices (or groups) that you want to use.
- 3 Click the **Deploy/Manage an Operating System**  button. This launches the [OS Management Wizard](#). Follow the instructions in the wizard to configure and launch this OS deployment job.

On the Management tab, monitor the groups under **OS Management** to view the status of the deployment.

OS Management Wizard

After you have selected a device or group for OS deployment, follow these steps to complete the OS Management Wizard:

Step 1 of 5: Operating System Selection

- a Choose one of the following options:
 - **Set new Operating System** – replaces the current OS
 - **Keep existing Operating System unchanged** – does not change the OS
- b Select one of the available OS images.
- c Click **Next**.

Step 2 of 5: Hardware Configuration Object Selection (Optional)

- a If you want to use a hardware configuration object, select **Use Hardware Configuration Management**. If you do not want to use a hardware configuration object, skip to [Step d](#).

See the *HPCA OS Manager Hardware Configuration Management Guide* for more information.

- b Choose one of the following options:
 - **Set new Hardware Configuration Option**
 - **Keep existing Hardware Configuration Option**
- c Select one of the available Hardware Configuration Options.
- d Click **Next**.

Step 3 of 5: Additional Options

- a Select the OS deployment method you will use:
 - **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. See [Using LSB](#) on page 196.
 - **Network Boot (PXE)**: Select this option if you will be using a PXE Server to install the operating system on your devices. See [Using Network Boot](#) on page 196.
 - **CD/DVD**: Select this option if you will be using an ImageDeploy CD or DVD to install the operating system on your devices. See [Using an ImageDeploy CD or DVD](#) on page 197.
- b Select **Emergency Mode** if you want to install (or re-install) the OS without attempting to capture and preserve any existing data – for example, in a disaster recovery scenario.

This option enables the client device to sense the need for management activity. If this option is not enabled, the client device requires an existing and bootable operating system, a working HPCA Agent, and good general integrity (for example, no viruses) in order to sense this.

Refer to “Defining Drive Layouts” in the *HPCA OS Manager System Administrator Guide* for information about capturing and preserving data if **Emergency Mode** is not used.

- c Select **Wake on Lan** if you want HPCA to trigger management operations on a machine that is currently turned off.
- d Click **Next**.

Step 4 of 5: Schedule

- a Specify the **Start Date** and **Start Time** that this OS deployment job should start.
- b Click **Next**.

Step 5 of 5: Summary

The Summary page in the wizard enables you to view all the settings you have specified for this OS deployment job, including the list of target devices. Click **Submit** to create the job. A new RMP type job should appear under **Current Jobs** on the Management tab (see [Managing Jobs](#) on page 158).

Using LSB

The Local Service Boot (LSB) option enables HPCA to assume management of the OS on devices that are not booted from the network.

When using LSB, 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 189 for prerequisite instructions for OS deployment.

Using Network Boot

The PXE-based environment enables HPCA to assume management of the OS on target devices that are booted from the network. See [Deployment Scenarios](#) on page 189 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 that your target devices boot from the network or have PXE-enabled as the primary boot device. Make the necessary configuration adjustments to ensure that this will happen (for example, with some BIOS versions, you can hit **ESC** during the reboot process and change the boot order in the configuration settings).

When you deploy an OS image using Network Boot, the target devices are rebooted using the settings that 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.

Using an ImageDeploy CD or DVD

An ImageDeploy CD/DVD is used to locally boot a target device that does not already have an operating system installed (a bare-metal machine). The ImageDeploy CD/DVD must be available locally at the target device.

Use the `ImageDeploy.iso` file provided with HPCA to create your CD or DVD. This file is located here on the HPCA media:

```
\Media\iso\roms\ImageDeploy.iso
```

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

See [Deployment Scenarios](#) on page 189 for prerequisite instructions for OS deployment.

To deploy an OS image using the ImageDeploy CD:

- 1 Perform the following steps on the target device:
 - a Insert the ImageDeploy CD (or DVD) in the target device, and boot off of the CD (or DVD).
 - b Specify which SOS to boot (**Linux** or **WinPE**).

- c From the boot source menu, select **Install from network**.
- d When prompted, enter your HPCA server IP address or host name and port number. For example,

`HPCA.acmecorp.com:3466` or `192.168.1.100:3466`

Note that port 3466 is reserved for OS imaging and deployment in an HPCA Core and Satellite installation. In a traditional CAE installation, port 3469 is reserved for this purpose.

- e Press **Enter** to continue.

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 ImageDeploy CD connects to the HPCA server, the following messages are displayed:

```
This machine has no local OS or the OS is invalid.
```

```
The machine cannot be used and will be shut down until an administrator specifies Policy and performs a Wake on LAN.
```

- 2 Perform the following steps in the HPCA Console:
 - a On the Management tab, follow the instructions for [Deploy an OS Image](#) on page 193
 - b For the deployment method, select **CD/DVD**.
- 3 After the wizard completes, reboot the target device again using the ImageDeploy 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.

When the image is finished deploying, the target device reboots and starts Windows. The Sysprep process will start and initialize the new image.

Perform a One-Time Hardware Maintenance Operation

Using the HPCA Console, you can create a job that uses a Hardware Configuration Element to perform special hardware maintenance operations on a client device. This may be necessary before you can install, update, or

repair the OS on certain devices – for example, if you need to trigger a RAID (redundant array of independent disks) verify or re-synch after an active hot spare (AHS) been changed.



For more routine low-level operations – such as a BIOS firmware upgrade or disk array controller (DAC) configuration – you should use the normal LDS/LME management process.

For additional information, refer to the *HPCA OS Manager Hardware Configuration Management Guide*.

To perform a One-Time Hardware Maintenance Operation:

- 1 On the **Management** tab, go to the Directories area, and expand the zone that you want to use.
 - To specify one or more individual target devices, click **Devices**.
 - To specify a group, click **Groups**.
- 2 In the Directory Object table, select the devices (or groups) that you want to work with.
- 3 In the drop-down menu for one of the selected devices (or groups), select the **Perform a one-time Hardware Maintenance** item in the OS Management submenu.

This launches the Hardware Maintenance Wizard.

- 4 Select **Emergency Mode** if you want to install (or re-install) the OS without attempting to capture and preserve any existing data – for example, in a disaster recovery scenario.
- 5 Select **Wake on Lan** if you want HPCA to trigger management operations on a machine that is currently turned off.
- 6 From the Available Maintenance Options list, select the hardware configuration element that you would like to use.
- 7 Specify the **Start Date** and **Start Time** that this OS deployment job should start.
- 8 Click **Next**.

The Summary page opens. This page enables you to view all the settings that you have specified for this hardware maintenance job, including the list of target devices.

- 9 Click **Submit** to create the job.

A new RMP type job should appear under **Current Jobs** on the Management tab (see [Managing Jobs](#) on page 158).

View the Status of OS Management Activities

After you click **Submit** in the OS Management Wizard, an RPM job is created and appears in the **Current Jobs** list (see [Current and Past Jobs](#) on page 159).

After the OS deployment job is finished, it moves to the **Past Jobs** list.

If the OS for a device is being managed by HPCA, the OS deployment state is shown in the OS Management section of the Directory Object view for that device (select **View/Edit Properties** to display this view). See [View the OS Deployment State](#) on page 193.

Viewing Out Of Band Details

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.


This option is only available when Out of Band Management is enabled. See [Out of Band Management](#) on page 314 for instructions. For more detailed information, refer to the *HP Client Automation Out of Band Management Guide*.

To view Out of Band details for a device:

- 1 On the Management tab, go to the Directories area, expand the zone that you want to use, and click **Devices** (or **Groups**).
- 2 From the shortcut menu for the device that you want to work with, select **Out of Band Device Details**.

The Out of Band Device Details window opens for the selected device—provided that the device is DASH or vPro equipped, and OOBM is enabled and properly configured.



You can also click the Out of Band Device Details  icon to view the OOB details for a particular device.

When Out of Band Management is enabled, this icon appears on the toolbar in the Directory Object view for any device.

6 Using Reports

The Reporting area contains summary and detailed reports of many kinds. The specific reports available to you depends on the type of HPCA license that you have. The following topics are discussed in this chapter:

- [Reports Overview](#) on page 204
- [Navigating the Reports](#) on page 206
- [Types of Reports](#) on page 208
 - [HPCA Management Reports](#) on page 209
 - [Compliance Management Reports](#) on page 213
 - [Inventory Management Reports](#) on page 209
 - [Patch Management Reports](#) on page 210
 - [Vulnerability Management Reports](#) on page 211
 - [Security Tools Management Reports](#) on page 215
- [Filtering Reports](#) on page 219

Reports Overview

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

- HPCA Management reports
- Compliance Management reports
- Inventory Management reports
- Patch Management reports
- Vulnerability Management reports
- Security Tools 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

The following reports are available only in HPCA Enterprise:

Report Pack	Report Type	Description
vm.kit	Vulnerability Management	Security vulnerability information, including vulnerability definitions and the results of client device scans
compliance.kit	Compliance Management	Compliance management information, including Secure Content Automation Protocol (SCAP) compliance rules and the results of compliance scans on managed client devices
stm.kit	Security Tools Management	Security tools management information, including anti-virus, anti-spyware, and software firewall installation and configuration.
hpc.kit	HPCA Management	Audit reports



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 to compliance management, vulnerability management, security tools management, inventory management, and patch management (if installed and enabled).

The screenshot displays a web browser window with the title "Current Reporting View: Reporting Home Page". The dashboard is organized into six main sections:

- Compliance Management Information:** Shows SCAP Rules Imported: 1354, SCAP Scanned Devices: 225 out of 262, Last Scan Date: 2009-03-02 09:03:38, and Last Acquisition Date: 2009-03-19 10:10:02. Includes Report Quicklinks: View SCAP Rules, View Scanned Devices, and View Top Failed SCAP Rules.
- Inventory Information:** Shows Managed Devices: 262, Managed Services: 14, and Devices Connected Today: 0. Includes Report Quicklinks: View Managed Devices, View Managed Services, and View Device Summary.
- Quick Search:** Features two search boxes. The first is for "Inventory Information" with a dropdown set to "Name" and fields for "Find a Device by" and "Find a Service". Both have "Apply" and "Reset" buttons.
- Security Tools Management Information:** Shows STM Scanned Devices: 9 out of 262, Last Scan Date: 2009-03-02 09:03:18, and Last Acquisition Date: 2009-03-19 10:10:02. Includes Report Quicklinks: View Scanned Devices and View Product Inventory.
- Vulnerability Management Information:** Shows Vulnerabilities Imported: 1513, Scanned Devices: 254 out of 262, Last Scan Date: 2009-03-02 09:13:00, and Last Acquisition Date: 2009-03-19 10:10:01. Includes Report Quicklinks: View OVAL Definitions, View Scanned Devices, and View Top Vulnerabilities.
- Patch Information:** Shows Compliance Summary: Managed Devices: 0, Managed Bulletins: 1, and Last Acquisition: 2009-01-29 14:22:56. Includes Report Quicklinks: View Device Compliance, View Bulletin Compliance, and 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 – and does not apply to vulnerability management reports or compliance management reports.
- 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 27 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 27 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:

- [HPCA Management Reports](#) on page 209
- [Compliance Management Reports](#) on page 213
- [Inventory Management Reports](#) on page 209
- [Patch Management Reports](#) on page 210
- [Vulnerability Management Reports](#) on page 211
- [Security Tools Management Reports](#) on page 215

Each is briefly described here.

HPCA Management Reports

This view contains audit reports for various HPCA functions. For example, the Remote Control audit report contains an entry for each remote control session attempted from the HPCA Console to a managed client device.

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 284 for configuration details.

A typical Managed Devices report includes the following table headings:

- **Details** – opens a Device Summary page for this device.
- **Last Connect** – when the device last connected.
- **HPCA Agent ID** – device name.
- **HPCA Agent Version** – the currently installed Management Agent version.
- **Device** – device name.

- **Last Logged on User** – the last user account used to log on to the device. If multiple users are logged on, only the last to log on is recorded—switching between currently logged on users does not affect this.
- **IP Address** – device IP address.
- **MAC Address** – device MAC address.
- **Operating System** – operating system installed on the device.
- **OS Level** – current operating system level (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 the *HPCA Enterprise Patch Manager Installation and Configuration Guide*.

Vulnerability Management Reports

The Vulnerability Management reports are organized in three groups:

- **Executive Summaries** – These reports provide a snapshot of vulnerability management activities and trends in your environment.
- **Vulnerability Reports** – These reports contain vulnerability definitions and detailed information about vulnerabilities detected in your environment.
- **Device Reports** – These reports contain information about vulnerabilities detected on specific devices in your environment.

You can filter many of these reports or drill down for additional detail. In any report that lists vulnerabilities, for example, you can drill down using the OVAL identifier or CVE identifier for a particular vulnerability to access a link to the pertinent vendor bulletin (if available). Vendor bulletins typically contain remediation information and sometimes include software patches.



When you drill down into a report for more detailed information, the data may be filtered in a different way than the data displayed in a summary level report. See [Filtering Reports](#) on page 219 for more information.

Table 28 Executive Summaries

Report Name	Description
Top Vulnerabilities	The ten vulnerabilities detected on the largest number of managed client devices in the enterprise
Top Vulnerable Subnets	List of the most vulnerable subnets based on the number of managed client devices with vulnerabilities and the severity category for each device
Top Vulnerable Devices	List of the ten client devices in your network with the largest number of vulnerabilities.
Vulnerability Impact by Severity	The outcomes of all vulnerability scans performed over the last year, including the number of managed client devices in each severity category at the time
Historical Vulnerability Assessment	The outcomes of all vulnerability scans performed over the last year, including the number of managed client devices in each severity category at the time

Table 29 Vulnerability Reports

Report Name	Description
OVAL Definitions	List of all the vulnerabilities included in the current vulnerability scan, by OVAL identifier
Application Vulnerabilities	List of all software application vulnerabilities for which HPCA currently scans
Operating System Vulnerabilities	List of all operating system application vulnerabilities for which HPCA currently scans

Table 29 Vulnerability Reports

Report Name	Description
Vulnerabilities by Impacted Devices	List of vulnerabilities detected on managed client devices sorted by the number of impacted devices
Acquisition History	History of HP Live Network content updates performed, including the number of High, Medium, and Low vulnerabilities in each update

Table 30 Device Reports

Report Name	Description
Scanned Devices	List of the managed client devices that have been scanned and the number of vulnerabilities found on each device
Devices Not Scanned	List of the managed client devices that have not been scanned

These reports are displayed on the Reporting tab. Some of the reports are also available from the [Vulnerability Management Dashboard](#).

Compliance Management Reports

The Compliance Management reports are organized in three groups:

- **Executive Summaries** – These reports provide a snapshot of your environment from the compliance management perspective. Use these reports to quickly assess the following:
 - How many client devices are in or out of compliance
 - Which compliance rules are most frequently violated
 - Which client devices are the most noncompliant
- **SCAP Reports** – These reports show you how many client devices are currently in or out of compliance with each Secure Content Automation Protocol (SCAP) benchmark included in your scans.

- **Device Reports** – These reports show you the results of the most recent compliance scan for each scanned client device. They also show you which client devices were not scanned.

You can filter many of these reports or drill down for additional detail. See [Find Information about Compliance Failures](#) on page 67 for more information.



When you drill down into a report for more detailed information, the data may be filtered in a different way than the data displayed in a summary level report. See [Filtering Reports](#) on page 219 for more information.

Table 31 Executive Summaries

Report Name	Description
Compliance Status	Total number of compliant and noncompliant scanned client devices in the enterprise.
Top SCAP Noncompliant Devices	The ten most noncompliant scanned client devices in the enterprise—in other words, the devices that comply with the fewest number of SCAP rules.
Top Failed SCAP Rules	The ten SCAP rules that failed on the largest number of scanned client devices.
Historical Compliance Assessment	The average default score for applicable devices that were scanned against each benchmark over a one year period (also shows the number of compliant and noncompliant devices)

Table 32 SCAP Reports

Report Name	Description
Compliance Summary	List of all the SCAP benchmarks included in the current compliance scan and the number of scanned client devices that are in and out of compliance with each.
Compliance Rules	List of all the SCAP rules included in the current compliance scan and the number of scanned client devices that passed or failed each rule.
Acquisition History	History of HP Live Network compliance content updates performed, including the source of the update, whether or not the scanner was downloaded, and the benchmark ID and version for each benchmark downloaded.

Table 33 Device Reports

Report Name	Description
Scanned Devices	Compliance scan results for managed client devices that have been scanned. For each device, this includes compliance status, default score, date of the most recent compliance scan, number of rules that passed, and number of rules that failed.
Devices Not Scanned	List of managed client devices that have not been scanned for compliance with SCAP benchmarks.

These reports are displayed on the Reporting tab. Some of these reports are also available from the [Compliance Management Dashboard](#).

Security Tools Management Reports

The Security Tools Management reports are organized in three groups:

- **Executive Summaries** – These reports tell you when your anti-virus and anti-spyware definitions were last updated on your managed client devices and when these devices were last scanned for viruses and spyware.
- **Product Reports** – These reports contain information about the anti-virus, anti-spyware, and firewall products detected on your client devices.
 - For each type of product, you can view a list of all products detected and a list of devices where these products were found.
 - For anti-virus and anti-spyware tools, you can view the date of the last definition update and scan for each pertinent device.
 - For firewall products, you can view a list of the firewall rules.
- **Device Reports** – These reports tell you whether each type of security tool is installed, enabled, or both on each client device.

The Security Tools Management reports are displayed on the Reporting tab. Some of the reports are also available from the Security Tools Management dashboard.

You can filter many of these reports or drill down for additional detail. See [Find Information About Security Tools](#) on page 69 for more information.



When you drill down into a report for more detailed information, the data may be filtered in a different way than the data displayed in a summary level report. See [Filtering Reports](#) on page 219 for more information.

Table 34 Executive Summaries

Report Name	Description
Last Definition Update Summary	When the anti-spyware and anti-virus definitions were most recently updated on your managed client devices
Last Scan Date Summary	When your managed client devices were most recently scanned for spyware and viruses

Table 34 Executive Summaries

Report Name	Description
Product Summary	List of all anti-spyware, anti-virus, and software firewall products detected and the number of client devices that have each product installed
Product Status Summary	Number of devices where each type of security tool was detected and enabled, detected and disabled, not detected, or unknown

Table 35 Product Reports

Report Name	Description
Anti-Spyware	
Discovered Anti-Spyware Products	List of anti-spyware tools detected on the managed client devices in your enterprise
Devices with Anti-Spyware Products	Date of the last spyware definition update and spyware scan for each pertinent device
Anti-Virus	
Discovered Anti-Virus Products	List of anti-virus tools detected on the managed client devices in your enterprise
Devices with Anti-Virus Products	Date of the last virus definition update and virus scan for each pertinent device
Firewall	
Discovered Firewall Products	List of software firewall tools detected on the managed client devices in your enterprise

Table 35 Product Reports

Report Name	Description
Devices with Firewall Products	List of the devices with software firewall products, including whether real-time protection is enabled and binaries are authenticated
Firewall Rules	For each software firewall product detected, the list of rules currently enforced
All Products	
Discovered Products	List of all anti-spyware, anti-virus, and software firewall products detected on the managed client devices in your enterprise
Acquisition History	Date and status of security tools management content updates from HP Live Network

Table 36 Device Reports

Report Name	Description
Scanned Devices	List of the security tools that are installed, enabled, or both on each managed client device that was scanned for the presence of security tools
Devices Not Scanned	List of the managed client devices that have not been scanned for the presence of security tools



These reports are displayed on the Reporting tab. Some of these reports are also available from the [Security Tools Management Dashboard](#).

The following reports include summary statistics regarding the state of the security tools on your managed client devices:

- Product Summary (under Executive Summaries)


- Discovered Products (under Product Reports > All Products)
- Devices Scanned (under Device Reports > Scanned Devices)

These statistics are also displayed when you expand the **Discovered Security Product Statistics** banner in the Device Detailed View for a particular scanned device. To display this view, follow these steps:

- 1 Open the Device Reports > Scanned Devices report.
- 2 Click the **Details**  icon for a particular device.
- 3 In the Device Details section, click the **Details**  icon again.

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.

See also:

- [Find Vulnerability Remediation Information](#) on page 65
- [Find Information about Compliance Failures](#) on page 67
- [Find Information About Security Tools](#) on page 69

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:

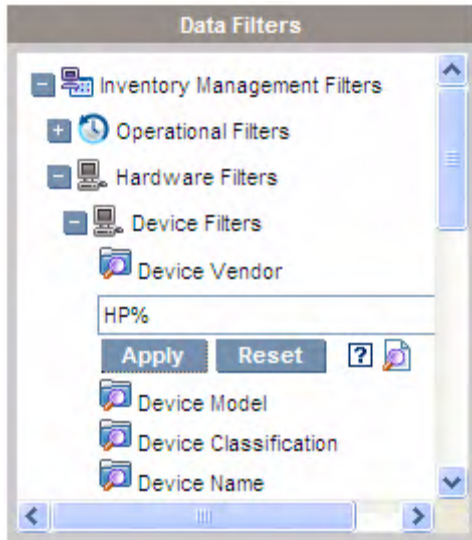
- 1 In the Data Filters section of the left navigation tree, expand the filter group that you want to use.
- 2 *Optional:* For the specific filter that you want to apply, click the  (show/hide) button to show the filter controls:
- 3 Specify the filter criteria in the text box, or click the  (criteria) 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 37 Special Characters and Wildcards

Character	Function	Device Vendor Filter Example	Records Matched
* or %	Matches all records containing a specific text string	HP*	All records that begin with “HP”
		%HP%	All records that contain “HP”
? or _	Matches any single character	Not?book	All records that begin with “Not” and end with “book”
		Note_ook	All records that begin with “Note” and end with “ook”
!	Negates a filter	!HP*	All records that do not start with “HP”


For example, if you specify HP% in the text box for a device related filter, the filter will match all devices whose Vendor names contain HP.




- 4 Click the **Apply** button. The report will refresh. To remove the filter, click the **Reset** button.

When you apply a filter to a report, the filter is listed in the report header:



If you apply a filter, that filter will remain in effect until you explicitly remove it. You can click the  (Remove button) to the left of the filter name to remove a filter from the current report.



You can also create an “in-line” filter by clicking a data field in the report currently displayed. For example, if you were viewing a Vulnerability Definitions report, and you wanted to see only those vulnerabilities with High severity, you would click the  (High Severity) icon in the Severity column.

Vulnerability Management Filters

The following table summarizes how the vulnerability management filters correspond to the pertinent reports.

Table 38 Vulnerability Management Filters

Reports	Applicable Filters
OVAL Definitions Vulnerabilities by Impacted Devices	OVAL Definition ID CVE ID Severity
Application Vulnerabilities	OVAL Definition ID CVE ID Severity Application Vendor ^a
Operating System Vulnerabilities	OVAL Definition ID CVE ID Severity Operating System ^c Vendor ^a
Top Vulnerable Devices	Device Name ^b Maximum Risk
Vulnerability Impact by Severity	Device Name ^b Maximum Risk Operating System ^c
Acquisition History	Vulnerability Acquisition Source

Table 38 Vulnerability Management Filters

Reports	Applicable Filters
Scanned Devices	Device Name ^b Maximum Risk Hardware Vendor ^b Hardware Model ^b Hardware Class ^b
Devices Not Scanned	Device Name ^b Hardware Vendor ^b Hardware Model ^b Hardware Class ^b

a The Vendor filter is also applicable when you drill down through the Scanned Devices report. See [Find Vulnerability Remediation Information](#) on page 65.

b Located in Inventory Management Filters > Hardware Filters > Device Filters.

c Located in Inventory Management Filters > OS Filters.

Compliance Management Filters

The following table summarizes how the compliance management filters correspond to the pertinent reports.

Table 39 Compliance Management Filters

Reports	Applicable Filters
Top SCAP Noncompliant Devices	Benchmark Benchmark Version Benchmark Profile
Historical Compliance Assessment	Benchmark Benchmark Version

Table 39 Compliance Management Filters

Reports	Applicable Filters
Compliance Summary	Device Name ^a Device Compliance Status Hardware Vendor ^a Hardware Model ^a Hardware Class ^a Benchmark Benchmark Version Benchmark Profile
Compliance Rules	Benchmark Benchmark Version Benchmark Profile Rules CCE ID
Acquisition History	Acquisition Source Benchmark Benchmark Version Benchmark Profile
Scanned Devices	Device Name ^a Device Compliance Status Hardware Vendor ^a Hardware Model ^a Hardware Class ^a Benchmark Benchmark Version Benchmark Profile

Table 39 Compliance Management Filters

Reports	Applicable Filters
Devices Not Scanned	Device Name ^a Hardware Vendor ^a Hardware Model ^a Hardware Class ^a Operating System ^b Operating System Level ^b

a Located in Inventory Management Filters > Hardware Filters > Device Filters.

b Located in Inventory Management Filters > OS Filters.

Security Tools Management Filters

The following table summarizes how the security tools management filters correspond to the pertinent reports.

Reports	Applicable Filters
Discovered Products	Product Type
Discovered Anti-Spyware Products	Product Name
Discovered Anti-Virus Products	Product Version
Discovered Firewall Products	Product Vendor
Discovered Products	

Reports	Applicable Filters
Devices with Anti-Spyware Products Devices with Anti-Virus Products Devices with Anti-Firewall Products Scanned Devices Devices Not Scanned	Device Name ^a Hardware Vendor ^a Hardware Model ^a Hardware Class ^a Operating System ^b Operating System Level ^b
Firewall Rules	Firewall Rule Name Firewall Rule Type Firewall Rule Protocol

a Located in Inventory Management Filters > Hardware Filters > Device Filters.

b Located in Inventory Management Filters > OS Filters.

7 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 230
- [Out of Band Management](#) on page 237
- [Patch Management](#) on page 241
- [OS Management](#) on page 252

The Satellite Console Operations tab provides Server Status and Support information as described in the following sections.

- [Server Status](#) on page 230
- [Support](#) on page 231

Infrastructure Management

Infrastructure Management operations are described in the following sections:

- [Server Status](#) on page 230
- [Support](#) on page 231
- [Live Network](#) on page 232

Server Status

Server Status displays the currently installed license information as well as a list of the component services that are controlled by the HPCA server. These component services handle different aspects of HPCA processing. The Server Status **Summary** table allows you to see which of these services are enabled.

[To review the status of component services](#)

- 1 On the HPCA Console, go to the Operations tab and click **Service Status**.
- 2 View the Summary table that lists the component services and whether they are enabled.

The Satellite Console Server Status page displays additional properties.

- Upstream Server
- Data cache usage
- Data cache capacity
- Synchronization status

The Satellite Console's Server Status page includes a **Tasks** area that enables you to update the data cache.

Synchronize Satellite Now

The Satellite server's contents (software services, patches, and operating system images) must be synchronized with an upstream host.



Before you can cache and synchronize data on a Satellite Server, you must have initially configured your Satellites. Refer to the *HPCA Core and Satellite Getting Started and Concepts Guide* for details.

Running the synchronization will synchronize the content that is used by the services that are enabled on the Satellite. For example, if the Satellite is fully enabled, it will synchronize:

- HPCA agent maintenance
- Configuration metadata
- Data cache resources for software and patches (requires Data Cache be enabled)
- Operating system images (requires Operating Systems service be enabled)

Satellite server synchronization can be scheduled to by creating a job on the Core server. See [Creating Satellite Synchronization Jobs](#) on page 171 for additional information.

Flush Data Cache

If there are critical new resources to download from an upstream server and the current data cache usage is close to capacity, or the data cache contains outdated or corrupt files, you can flush the resource cache to make room for a quick loading of new resources.



Take care when using this option because it flushes the entire cache—dynamic and preloaded.

This action could result in the accidental deletion of important files.

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 232, 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 logfile.zip**.
- 3 When prompted, click **Save** to store the compressed file on your computer.
- 4 Specify a location to store the file and click **OK**.
- 5 The log files are downloaded to your computer and saved in a single ZIP formatted file.

 Internet Explorer security settings may prevent these files from being downloaded. HP recommends adding the HPCA console URL to your trusted sites or modifying your Internet Explorer settings to not prompt for file downloads.

Live Network

Use the Live Network settings to specify how and when the HP Live Network security and compliance management content is updated. You can set up a schedule for automatic updates or initiate an immediate update. You should always perform an update after you install or upgrade your HPCA software to ensure that you have the most recent security and compliance scanner and data.

 When HPCA updates your content from the HP Live Network site (or from the file system), it uses a tool called the HP Live Network Connector (LNC). This tool is installed by HPCA and is self-updating. In certain circumstances, you may want to install a new copy of the LNC. See [Download the HP Live Network Connector](#) on page 236 for more information.

Whether you choose to schedule automatic updates or initiate an immediate update, you must specify the content source for the update. You have three choices:

- **From the HP Live Network**

The security and compliance scanners and data are retrieved from the HP Live Network content server and published to the HPCA infrastructure. By default, this path is:

```
<InstallDir>\LiveNetwork\lnc\bin\live-network-connector.bat
```

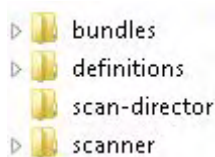
This path is configured automatically by HPCA. You do not need to specify this path unless you have downloaded a new copy of the HP Live Network Connector and installed it in a different location.

To use this option, you must have an active HP Live Network subscription. This is not included in your HPCA software. See your HP representative for details.

- **From the File System**

A copy of the vulnerability and compliance scanner and data are published from a location in the file system on the system where the HPCA Console is installed. You must specify the path name of the folder that contains the scanners and data, and you must manually download these items from the HP Live Network content server before you can initiate an update.

The folder structure from the file system location specified must exactly match the folder structure that is created when the HP Live Network Connector downloads content, as shown here:



The subdirectories under each of these folders must also match exactly.

In some cases, HP Live Network updates only a subset of the security and compliance management content. In this case, some of these directories may not be delivered during a Live Network update.

For more information about using this option, see [Run the HP Live Network Connector Manually](#) on page 76.

- **From the Configuration Server Database**

Vulnerability definitions previously published to the CSDB are loaded into the Reporting database.

See [Move HP Live Network Content from a Test Environment to a Production Environment](#) on page 78.

Schedule Automatic Live Network Updates

Use the following procedure to establish a schedule for automatic HP Live Network updates from the content source of your choice.


To schedule automatic HP Live Network content updates:

- 1 On the Operations tab, expand the Infrastructure Management area, and click **Live Network**.
- 2 Click the **Schedule Updates** tab.
- 3 In the Updates section, select the content source.
- 4 Specify the schedule for automatic updates:

- a **Schedule**—Select Once, Hourly, Daily, Weekly, or None

None is what the HPCA Console shows when nothing is currently scheduled to execute—for example, when a previously scheduled Once task has already completed. You can specify None if you do not want to schedule anything new or if you want to stop an existing schedule. If there is a recurring schedule, the most recently saved schedule is shown (for example, Hourly, Daily, or Weekly).

- b **Start Time**—Time of day to start the updates.

- c **Start Date**—Date to start the automatic updates. Click the  (calendar) button, and select the date.

When the **Schedule Updates** tab is displayed, the time and date fields show the time and date of the last saved schedule. For example, if a previously scheduled Once update has already completed, the Schedule will be set to None, and you can see the time and date of the last update in the Start Time and Start Date fields.

- d If you selected Hourly, Daily or Weekly for the **Schedule**, specify the update interval in the **Every** box.

For example, if you select Daily, with an **Every** interval of two, this will run an update every two days.

5 Click **Save** to implement your changes.

▶ If you leave this tab, any information that you entered prior to clicking **Save** will be lost. Be sure to click **Save** if you want to keep this information.

▶ You can use the **Reset** button to restore the most recently saved settings.

Update the HP Live Network Content Now

Use the following procedure to update your HP Live Network content now. This does not affect any schedule that you have established for automatic updates.

To update the HP Live Network content immediately:

- 1 On the Operations tab, expand the Infrastructure Management area, and click **Live Network**.
- 2 Click the **Update Now** tab.
- 3 Select the content source for this update. This will not affect any automatic updates that are currently scheduled.
- 4 Click the **Update Now** button. A request is issued to update the scanner and data from the content source that you specified.

An update is an asynchronous process that requires some time to complete. You can use the acquisition reports to view the results of an update or check its status.

View the Results or Status of an Update

You can use the HPCA reports to check on the status of an HP Live Network content update.

To view the results or status of an update:

- 1 Click the **Reporting** tab.
- 2 To view the status of the content updates, open the **Acquisition History** report in each of the following reporting views:

Vulnerability Management > Vulnerability Reports

Compliance Management > SCAP Reports



If the configuration information related to HP Live Network is incomplete or incorrect, the update will fail. This will be reflected in both the report and the log file:

```
<InstallDir>\HPCA\VulnerabilityServer\logs\vms-server.log
```

There will be no other indication in the HPCA Console that the update has failed, however.

Download the HP Live Network Connector

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

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

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

- 1 On the Configuration tab, expand the Infrastructure Management area, and click **Live Network**.
- 2 Click the **Download** link to the right of the HP Live Network Connector box. A new browser window will open to the HP Live Network site. From there you can download the LNC executable. You will need your HP Live Network subscription user name and password to log in.

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



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

CAE installation:

```
<InstallDir>\LiveNetwork\lnc\bin\live-network-connector.bat
```

HPCA Core server in a Core and Satellite installation:

```
<InstallDir>\HPCA\LiveNetwork\lnc\bin\live-network-connector.bat
```

Out of Band Management

Out of Band (OOB) Management is enabled using the Configuration tab. See [Configuration](#) on page 253 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 237
- [Device Management](#) on page 239
- [Group Management](#) on page 240
- [Alert Notifications](#) on page 241

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:

- [Start Acquisition](#) on page 241
- [Perform Synchronization](#) on page 243
- [View Agent Updates](#) on page 244
- [View Acquisition History](#) on page 247
- [View Logs](#) on page 247
- [Delete Devices](#) on page 247
- [Gateway Settings](#) on page 248

Start Acquisition

- 1 From Operations, expand **Patch Management** and click **Start Acquisition**.
- 2 Select a file by clicking on its name.

- 3 Confirm the settings for this acquisition.

Acquisition Settings for MS04 ()

Bulletins	MS04*
Mode	Both
Force	NO
Replace	NO

Microsoft Settings

Languages	English
------------------	---------

Report Acquisition Status

Report Acquisition Status

Report Acquisition Status	Periodically	▼
Update Acquisition Status every	1	Minutes

- **Report Acquisition Status:** In addition to the acquisition log, you can specify how frequently you want to update the current acquisition status that is displayed when you View Acquisition Jobs, as discussed on
 - **Update Status Information every:** If you specified **Periodically** in the Report Acquisition Status field, select how frequently you want to update the status file.
- 4 Read the notice on your agent update settings, and click **Submit** to begin your acquisition.

To check the status of the acquisitions:

- Use the Reporting tab to look at the Patch Acquisition Reports.
- Use the Operations tab, Patch Management area to **View Acquisition Jobs**.
- Also use the Operations tab, Patch Management area to access the **View Logs** page and select the `patch-acquire.log`.

Perform Synchronization

The patch information that has been sent to the HPCA Configuration Server DB must be synchronized with the Patch SQL database for assessment and analysis. The HPCA Configuration Server DB and the Patch SQL database house identical information for the set of classes and instances that are synchronized.

- Each class in the PATCHMGR Domain becomes a table in the Patch SQL database. The corresponding table is named `nvd_classname`.
- Each attribute in each class becomes a column in its table. The corresponding column name is `nvd_attributename`. Expressions and connection variables are not replicated.
- Each instance in the class becomes a record in the corresponding table.

This synchronization occurs automatically after a patch acquisition and in normal HPCA operations.

However, there may be times when you need to run the synchronization manually. For example, synchronize the databases manually after an import of patch information from a different HPCA server. Also, synchronize the databases manually if you switch the SQL database configured for Patch Management after some acquisitions have taken place.

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 Agent Updates

When you run a patch acquisition, you can also download the latest Version and updates to the Patch Agent files. The Patch Agent files include the scripts to perform product discovery and management. These files are received from the Patch Update web site provided by HP. After download, the files are published to the PATCHMGR Domain and connected to the DISCOVER_PATCH Service instance.

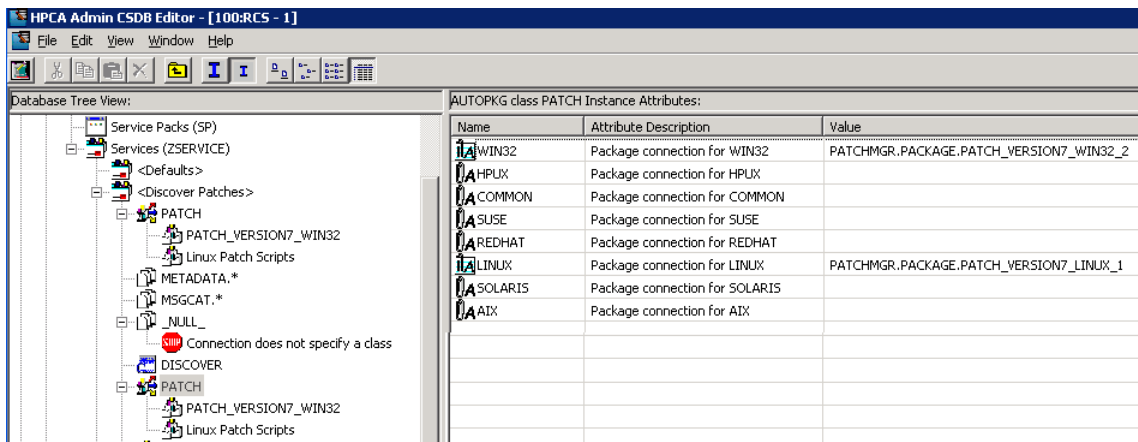
Use the View Agent Updates task to determine the status of updates; View Agent Updates is accessed from Operations tab, Patch Management area on the HPCA Core Console. To do this, click **View Agent Updates**.

Figure 44 View agent updates

Agent Updates			
Package Name	Package	Release	Date Published
Windows Update Agent Media	WUA_MEDIA_X86	7.2.6001.788	2009-03-18 16:13:49
Windows Patch Scripts	PATCH_VERSION7_WIN32_3	7.2	2009-03-18 15:24:46
Windows Update Agent - Scan Data	WUA_MEDIA_SCANDATA	7.2.6001.788	2009-03-14 16:13:45
Windows Patch Scripts	PATCH_VERSION7_WIN32_1_	7.2	2009-03-14 16:13:28
Linux Patch Scripts	PATCH_VERSION7_LINUX_1	7.2	2009-03-14 16:13:19

Agent files are distributed when the DISCOVER_PATCH Service is processed on the Patch Manager target device. This is accomplished through a connection in the DISCOVER_PATCH Service to the PATCH Instance in the AUTOPKG Class. In turn, the AUTOPKG.PATCH Instance connects to the agent maintenance packages created when you selected **Publish** or **Publish and Distribute**. If you have selected to publish only (not to distribute), you will need to create connections from the appropriate instance in the PACKAGE Class to the AUTOPKG.PATCH Instance. Use the Admin CSDB Editor to do this. An example is shown below.

Figure 45 Create connections to the published package



➤ AIX, HP-UX and Solaris are not currently supported.

Agent Updates has the following values:

- **None:** The agent updates will not be published to the PATCHMGR Domain.
- **Publish, Distribute:** This is the default value. Publish the updates to the PATCHMGR Domain and connect them to the DISCOVER_PATCH Instance to distribute the updates to your Patch Manager-managed devices.
- **Publish:** The updates will be published to the PATCHMGR Domain, but will not be connected for distribution to Patch Manager-managed devices. You will need to create these connections.

There are two parameters that control which agent updates you download.

- **Operating System:** Specify which operating systems to acquire the agent updates for. The default is to download all operating systems.. Valid values are **Windows** and **Linux**.

- **Version:** Select the Patch Manager version for which you would like to acquire the agent updates. You can publish only one version to a Configuration Server; one Configuration Server cannot host multiple versions of the agent. If piloting, create a separate Configuration Server for the other version.



Never choose an agent version that is lower than the version of Patch Manager that is first installed or currently implemented in your enterprise.

To update to the current version, specify **Version 7**. This is the default for new Patch Manager 7.50 installations.

Migrating customers are advised to set the “**Publish and Distribute**” option and set the Agent Updates Version to **Version 7**. This will ensure the successful migration of Windows and Linux Patch Agents to Version 7.50. This is needed to continue management of Microsoft security patches when Microsoft discontinues updates to `MSSecure.xml`, in favor of the new Microsoft Update Catalog feed.

Note that when patches are acquired from Microsoft Update, the Source column in the report will show “Microsoft Update” instead of “Microsoft.”



To accommodate Microsoft Update technologies, your target devices must have the Windows Update Agent installed. The Patch Manager acquisition process automatically acquires the latest Windows Update Agent required to perform vulnerability scans and patching when leveraging Microsoft Update Catalog technologies. The `DISCOVER_PATCH` Service will automatically apply the current Windows Update Agent to the managed device on the next agent connection.



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

View Acquisition History

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

View Logs

The Patch Manager Server logs can be used to review and troubleshoot the patch management environment. These logs are available online from the Console using the Operations tab and the Patch Management area.

From the console, click the **Operations** tab and expand the **Patch Management** tasks. Click **View Logs**.

Select a Log File from those listed to open and review it online, or to save it locally and review it with HP support.

- **HPCA-PATCH-3467.log** Log for the Patch Manager Server.
- **patch_acquire.log** Log for patch acquisitions.
- **patch-sync.log** Log of synchronizations between the Patch Manager Database and the Configuration Server Database.
- **httpd-3467.yy.mm.dd.log** Web server access log for Patch Manager Server. This log shows who is accessing the server, either through the web services or through the console interface, and how many accesses were made.

These logs are located in the `\logs` folder of the Patch Manager Server installation directory.

Delete Devices

You can delete Patch Manager compliance data for specific devices using the Operations tab of the console.

To remove compliance data from the Patch Manager ODBC database

- 1 Click the **Operations** tab and expand the **Patch Management** tasks.

- 2 Click **Delete Devices**.

Specify the device criteria below

? Device Name(s):

? Days since last scan:

Next >

- 3 Specify device-selection criteria for the devices to remove. You may:
 - Specify a single device or multiple devices in a comma-separated list.
 - Use wildcards.
 - Specify the number of days since the last vulnerability scan was performed on the device. This may be used to remove compliance information for devices who are no longer reporting compliance data to the Patch Manager Infrastructure components.
- 4 Click **Next**. The console allows you to preview the devices that match the selection filters before removing them from the database.
- 5 Click **Delete** to remove the devices from the Patch Manager ODBC database.



Take care when removing devices from this database; this operation cannot be undone.

Gateway Settings

The Patch Manager Gateway is used to obtain and cache the patch binary files when the **Patch Metadata Download** option is enabled on the **Patch Management > Distribution Settings** page. The Patch Metadata Download option is only available when patching Microsoft devices using Microsoft Update Catalog data feed.

The Patch Management > Gateway Settings area of the Operations tab allows you to review and manage the cache of patch files stored on the Gateway.

Preload Gateway option

- If the Preload Gateway option is turned off, the Gateway caches the patch files as they are requested by Agents. This is the default and recommended setting.
- If the Preload Gateway option is turned on, the Gateway caches the patch files when the patches are acquired.

The following Gateway Operations are available from the area of the Console:

- [View Cache Statistics](#) on page 249
- [Cache Content Details](#) on page 250
- [Export URL Requests](#) on page 250
- [Import URL Requests](#) on page 251

View Cache Statistics

Use the View Cache Statistics page to see statistics on the patch files currently cached on the Gateway, as well as hit, miss and error information that lets you gauge how well the Gateway is satisfying the patch requests of the Agents. The counters for the hit, miss and error information can be reset.

To access the View Cache Statistics page:

- From the Console **Operations** tab, select **Patch Management > Gateway Settings > View Cache Statistics**.

Gateway Cache Statistics

- **Total cache size:** Total size in megabytes of all patches in the Gateway cache.

When the cache size exceeds the Maximum Cache Size configured for the Patch Gateway Operations on the Patch Distribution Settings page, the patches that are older and least used will be deleted.
- **Number of files:** The number of active files in the patch gateway cache available for download.
- **Cache Hits:** The number of requests that have been fulfilled since the last counter reset.
- **Cache Misses:** The number of requests that required a download from the Vendor since the last counter reset.

- **Cache Download Errors:** The number of download errors the gateway encountered since last counter reset. The error can be found in the HPCA-PATCH-3467.log file.
- **Hit Ratio:** The ratio between requests fulfilled from cache, and the total number of requests.
- **Cache Counter Reset On:** The date and time when the cache counter statistics were reset.
- **Reset Cache Counter Statistics:** Click this entry to reset the counters for cache hits, misses and download errors.

Cache Content Details

Use the Cache Content Details page to view the current set of patch binary files cached on the Gateway, by Bulletin number.

To access the View Cache Statistics page:

- From the Console **Operations** tab, select **Patch Management > Gateway Settings > Cache File Statistics**.

Viewing the Cache Content Details

The Cache Content Details page displays the cached bulletins by number. Click on a Bulletin Number to see the list of binaries cached for that bulletin. Double-click a binary file to see more details.

Export URL Requests

If the Gateway server cannot connect to the Vendor download site, these unfulfilled agent request files can be exported and then imported into another Gateway Server with internet-connectivity.

The Export URL Requests operation allows you to see and filter the list of unfulfilled URL requests and import the list into another patch server.

When you export the URL you are prompted to save the contents as XML file with a name of your choice. The XML file contains the patch URLs selected during the export.

To access the Export URL Requests page:

- From the Console **Operations** tab, select **Patch Management > Gateway Settings > Export URL Requests**.

To export a list of unfulfilled URL requests:

- 1 Use the List Display Settings area to filter the unfulfilled list into the ones you want to export.

List Display Settings

Enter a **URL Filter Expression** to filter the list of all unfulfilled patch requests by URL name. Wildcards are accepted. Click **Apply** to apply the filter.

Use the **Page Count** drop-down to set the desired number of URL listings to include on a single page.

To return to the full list of URLs, reset the entry to * and click **Apply**.

If there are unfulfilled URL Requests listed on this page, click Submit to download an export file of these current unfulfilled requests.

Import URL Requests

The URLs exported from the **Export URL Request** operation can be imported into a different Patch Gateway Server using the Import URL Requests page. The imported files will be stored in the Patch Gateway and can only be used only by that Gateway server.

To access the Export URL Requests page:

- From the Console **Operations** tab, select **Patch Management > Gateway Settings > Import URL Requests**

To import URL requests:

- 1 Copy the file saved after using the Export URL Requests task to the local drive of the gateway where you want to import the URL requests.
- 2 In the **Request file to import** area, click **Browse** to locate the xml file that was saved from the Export URL Requests tasks.
- 3 Click **Submit** to start importing the unfulfilled requests in the specified file

The Gateway URL Request Import page displays the URLs being imported, their completion status, and the % completion.

OS Management

Use the OS Management, [CD Deployment](#) area to download images that can be burned to a CD or DVD for operating system deployment.

CD Deployment

You can use the CD Deployment feature to download images that can be burned to a CD or DVD for operating system deployment.

The OS Library list displays all operating system images that have been published to the CA server.

To download services for CD deployment

- 1 On the Operations tab, go to **OS Management > CD Deployment**.
- 2 From the OS Library list, select the services to download.
- 3 Click **Create CD Deployment Media** icon to launch the CD Deployment Wizard.
- 4 Review the summary information and click **Download**. The services begin to download in the background.
- 5 Click **Close**.
- 6 View the download progress in the OS Library list. Click the **Refresh** icon to see the current status of each service in the CD Creation Status column.

When complete, the services are stored by default in:

```
C:\Program Files\Hewlett-Packard\HPCA\Data\ServiceDecks\CDDeployment
```

When this directory is empty, the CD Creation Status is blank for all services listed.



This feature is intended for use with DVDs, typically to store multiple images. Do not span your resources over multiple CD-ROMs or DVD-ROMs.



Your CD-ROM or DVD-ROM must be in Joliet format.

8 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 Enterprise license users with Zone accounts 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 254
- [Core Console Access Control](#) on page 255
- [Infrastructure Management](#) on page 263
- [Device Management](#) on page 284
- [Patch Management](#) on page 287
- [Out of Band Management](#) on page 314
- [OS Management](#) on page 317
- [Dashboards](#) on page 318

Satellite Configuration Options

- [Licensing](#) on page 254
- [Upstream Host](#) on page 254
- [SSL](#) on page 264
- [Satellite Console Access Control](#) on page 259
- [Configuration](#) on page 261

- [Data Cache](#) on page 261
- [Policy](#) on page 265
- [OS Management](#) on page 317
- [Thin Clients](#) on page 285
- [Multicast](#) on page 280

Licensing

A functional HPCA environment requires a valid HP-issued license. This area of the Console stores your license file and displays the license edition (Starter, Standard, or Enterprise) that is installed. You can use this section to review and update your HPCA license.

To apply a new license

- 1 Copy and paste the license information from your new `license.nvd` file into the **License Data** text box.
 - ▶ When copying the license information from your license file, do not include the text that precedes the line `[MGR_LICENSE]` because this will result in the license information not being “readable” to the Console.
- 2 Click **Save**. Updated license information is displayed after **Current License**.

Upstream Host

On a Satellite console, use the Configuration tab **Upstream Host** area to edit the upstream host server information. The upstream server is the server this Satellite will synchronize with, as well as fetch information for requests if a service is disabled or a resource is unavailable. You may use SSL for this inter-server communication, this requires the upstream server is capable of receiving SSL requests.

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 255.
- Access Control on the Satellite Console allows HPCA administrators to select and configure an authentication method. See [Satellite Console Access Control](#) on page 259.

Core Console Access Control

Use the Access Control section to create instances of Console **users** (see [Users Panel](#) on page 255) with unique, custom IDs and passwords. Then, assign **roles** (see [Roles Panel](#) on page 258) 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 **jd~~oe~~/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 258).


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 258).

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.

Satellite Console Access Control

The Access Control section of the Satellite Console allows an HPCA administrator to select a Console-access authentication method (**Local Accounts** or **Directory Service Accounts**) and to configure its settings.

The Summary area of the Access Control section displays the Authentication Method that is currently enabled. The default (Local Accounts) is displayed.

To select and configure an authentication method

- 1 Click **Configure Authentication**. The Authentication Wizard opens.
- 2 In the Set Server Authentication Type area, use the Authentication Method drop-down to select either:
 - **Local Accounts** – This method allows an administrator to set *administrator* and *operator* log-on credentials for the Satellite Console; these credentials restrict access to various parts of the Console. This is the default. See the section, [To use Local Accounts](#) on page 259, for configuration information.
 - **Directory Service Accounts** – This method allows administrator authentication using Directory Service Accounts (such as Active Directory) that are in place in the environment. For configuration information, see [To use Directory Service Accounts](#) on page 260.
- 3 Click **Next** to proceed to the Configuration area and specify the settings for the access method you have chosen.

To use Local Accounts

If you are using Local Accounts to secure access to the Satellite Console, change the password immediately after installing the Satellite server.



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.
- α Configure Console access for administrators and operators in the appropriate areas.

- **Administrator** permissions allow the user to access all areas of the Console.
 - **Operator** permissions restrict the user’s access to only the Operations area of the Console.
- b Click **Next**.
- c When the configuration is complete, click **Close**.

The next time you log in to the Satellite Console using a Local Account, use the new password.

To use Directory Service Accounts

An external Directory Service Account can be used to authenticate a user’s access to the Satellite Console.

- a In the Directory Service Settings area, specify the configuration parameters as described below.
- **Directory Host:** The hostname or IP address of the external directory server that will be used for authentication.
 - **Directory Port:** The port that will be used to access the external directory server. The default is 389.
 - **Base DN:** The base object in your directory at which to start searching when querying for the users.

For example, **dc=europe, dc=acme, dc=com**.
 - **Access Group DN:** The Group DN that contains all members who are entitled to access the Core Console with administrative rights.
 - **Directory User ID:** A valid user ID that can access the directory server in order to verify that a person logging on to the Core is a member of the above-named Group DN. The default is administrator.
 - **Directory Password:** The password that is associated with the above-listed user ID.

- b In the Test LDAP Group User area, supply the credentials of a “test user.”



The test user must be a member of the Access Group DN that was specified above.

This test will ensure that you can access this server after the Directory Service Account configuration is complete.

- **Username:** The user name of an existing Access Group DN user.
- **Password:** The password that is associated with the above-listed user name.

- c Click **Next**.

- d When the configuration is complete, click **Close**.

Administrators can now sign in to the Satellite Console using their Directory Service Account credentials.

Configuration

The Configuration area is available on Satellite Consoles, only.

Configuration services supply “model” and service information to the HPCA agents, based on their entitlements. The agents connect to the server in order to obtain this information and to satisfy changes. When this service is disabled on the Satellite server, HPCA agents will have to use a different server in order to obtain the requested information. This “fallback server” designation should be built in to your infrastructure model (as configured in the CLIENT.SAP Instances of the Configuration Server Database).

- To enable the configuration services, select the **Enable** check box and click **Save**.

Data Cache

The Data Cache area is available on Satellite Consoles, only.

Data Cache services control the underlying HPCA cache-management service that is used to bring down data (such as software, patch, security, and audit) from an upstream host with which the Satellite is synchronized. This page allows you to:

- Enable and disable data cache services on this Satellite.
- Set a resource data cache limit, in megabytes.

▶ Before you can cache and synchronize data on a Satellite server, you must have initially configured your Satellites. Refer to the *HPCA Core and Satellite Getting Started and Concepts Guide*, for details.

To configure Data Cache

- 1 On the Configuration tab, click **Data Cache**.
- 2 Set the following options.
 - **Enable** (Box checked) Indicates that data services are enabled for this Satellite. This is the default and allows HPCA agents that are connecting to this Satellite to receive their software and patches from it.
 - **Enable** (Box unchecked; effectively, **Disabled**) Indicates that data services are disabled for this Satellite.
 - A synchronization with the upstream host will not bring down to this Satellite the software and patch data cache.
 - Any HPCA agents that connect to this Satellite will have their data requests passed to the upstream host.
 - Set **Data cache limit (MB)** to set a maximum size (in megabytes) of the resource cache. The default is 40000 MB.
- 3 Click **Save** to implement your changes.

When the Operations tab is refreshed, the status of this service is shown under Summary.

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 263
- [SSL](#) on page 264
- [Policy](#) on page 265
- [Database Settings](#) on page 267
- [Directory Services](#) on page 267
- [Job Action Templates](#) on page 276
- [Multicast](#) on page 280
- [Live Network](#) on page 281

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 264
- [SSL Client](#) on page 265

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**.

Policy

Policy must be enabled in order for the HPCA server to be able to connect to a directory service that contains entitlement information. When this is disabled, the requested information is obtained from an upstream server.




When Policy is configured in this panel, a directory service instance (that contains the configuration settings) is automatically created in the HPCA list of directory services, which are accessible in the Console's Directory Services panel.

This instance in Directory Services can be modified for additional features—such as authentication—but it is not necessary to create a directory service for policy.

To enable and configure Policy

- 1 In the Policy Settings area, select **Enable** (this will start the Policy Server service).
- 2 Specify the configuration parameters, which are described below.

Directory Host: Specify the fully qualified machine hostname or IP address of the external directory server that will be used for authentication.

 If you are using SSL, do not specify an IP address in this field. SSL does not validate IP addresses.

Base DN: Specify the Group DN that contains all members who have administrative rights to access the Core Console.

Directory Port: Specify the port that that will be used to access the external directory server. The default is 389.

Directory Username: Specify a valid user name that can access the directory server in order to verify that the person logging on to the Core is a member of the above-named Group DN. The default is Administrator.

Directory Password: Specify the password that is associated with the above-listed user name.

3 Click **Save**.

The Core server automatically tests the connection to the external directory service.

If the LDAP connection test is successful, the Core server creates a mount point for the Portal to connect to this directory service and enables it to be used for policy.

4 After a successful connection to the external directory, at the bottom of the Policy page click **Generate LDIF**.

Generate LDIF

In this area, you can choose to generate an LDIF (LDAP Data Interchange Format) file that can be used to update a directory schema with HPCA policy settings.

Clicking this option will allow you to save an LDIF file that is customized with the policy settings that were specified on the Policy page.

 Make sure that the above-listed policy settings are saved before generating an LDIF file.

1 Click **Generate LDIF**.

This creates a file that contains the customized schema changes that are necessary in order for HPCA to use your external LDAP directory.

- 2 When prompted, save the generated LDIF file to a location of your choice.
- 3 Follow the steps in the section [Implementing an External Policy Store](#) on page 28 to use the LDIF file to make the schema changes to your external LDAP directory.

Database Settings

Use Database Settings to configure the ODBC connections to your SQL and Oracle databases for the Core server objects.

Prerequisites

The Core database must be created and an ODBC connection defined for it. Refer to the installation instructions in the product manual for details.

To configure Messaging

- 1 On the Configuration tab, click **Infrastructure Management** then **Database Settings**.
- 2 Set the following options.
 - **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**.

Directory Services

Directory Services are used for many things, including the following:

- Running reports based on Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) containers & groups
- Enabling external AD/LDAP sources for authentication to the HPCA Console

- Policy assignment – a policy is a designation of the services to which a user, an agent computer, or a managed device is entitled
- OS Management operations
- Agent Notification based on AD/LDAP sources

HP Client Automation supports two basic policy usage patterns:

- The **normal** pattern enables you to administer policy (for software and patches, for example) stored in an external LDAP directory—such as Active Directory—that you supply. This policy source is used by the Policy Server to drive resolution in the Configuration Server. Policies in the directory are administered by the HPCA Console.

In order to perform policy management on an external directory service, you must first update the Schema. See the *HP Client Automation Policy Server Installation and Configuration Guide (Policy Server Guide)* for additional information about configuring your environment to use external directories for policy.

➤ This type of policy is not supported in the internal directory of the Portal. See the *HP Client Automation Portal Installation and Configuration Guide (Portal Guide)* for more information.

- The other policy usage pattern supported pertains to **operating system (OS) management**. OS management policies are stored internally in the HPCA Management Portal (Portal). In this case, the Portal provides the operational interface to the Configuration Server to support OS resolutions. Policy administration is done using the OS Management features in the HPCA Console. See the *HP Client Automation OS Manager System Administrator Guide (OS Manager Guide)* for additional details.

➤ OS Management policy is now supported for external LDAP directories.

Related Topics:

[Navigate the Directory Services Page](#) on page 269

[Configure a Connection to the Configuration Server Directory Service](#) on page 272

[Configure Connections to External Directory Services](#) on page 273








Navigate the Directory Services Page

Before you can use LDAP policy management, you must first define the LDAP environment to which you are connecting. To do this, you must create and configure a Directory Services object.

To access the Directory Service page, click the **Directory Services** link in the left navigation menu on the Configuration tab.

The following table describes the toolbar buttons available on the Directory Services page. Use these toolbar buttons to manage any existing Directory Services or create new Directory Services.

Table 40 Directory Services Toolbar Buttons

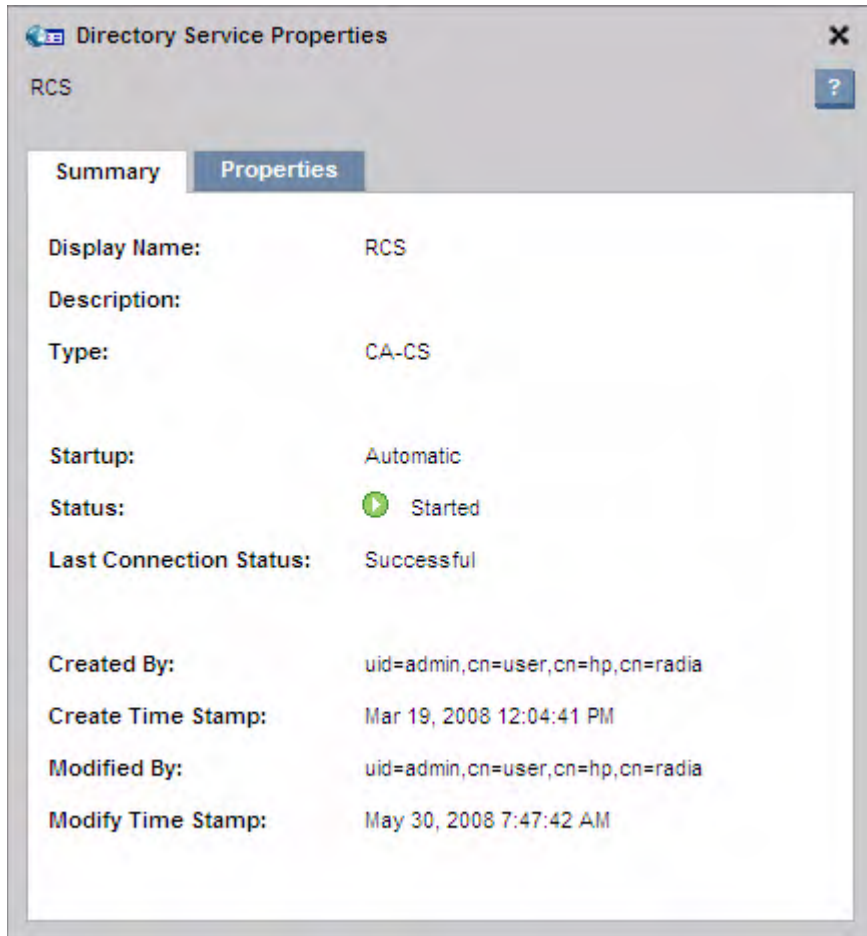
Icon	Toolbar Button Name	Description
	Refresh Data	Refreshes the Directory Services list.
	Show/Hide Filter Input	Use to show or hide the filter toolbar. You can filter Directory Services data by using a text string and narrow the search by selecting individual Directory Services columns to include in the search.
	New Directory Services	Launches the Directory Services Creation Wizard.
	Start the Selected Directory Services	Use to start an existing Directory Service that is stopped.
	Stop the Selected Directory Services	Use to stop an existing Directory Service that was previously started.
	Restart the Selected Directory Services	Use to restart an existing Directory Service.
	Delete the Selected Directory Services	Deletes a Directory Service from the list.

View Directory Service Details

You can view information about any Directory Services objects that have been defined.

To view Directory Service details:

- 1 From the Configuration tab, click **Directory Services** in the left pane.
- 2 Click the name of the directory service for which you want to view details or change options. The following shows a sample Directory Services summary window:



- 3 Click the **Summary** tab to see basic information about the directory service. You cannot modify these properties.

- 4 Click the **Properties** tab to see the **General Settings** and **Connection Settings**. You can modify any of these settings. All parameters marked with an asterisk (*) are required. Click **Save** after making modifications.
- 5 Click **Close** to acknowledge the dialog.

Modify Directory Service Property Settings

You can modify the property settings for any Directory Services objects that have been defined.

To modify Directory Service options:

- 1 From the Configuration tab, click **Directory Services** in the left pane.
- 2 Click the name of the directory service that you want to change.
- 3 Click the **Properties** tab to display the directory service options.
- 4 Click **General Settings** or **Connection Settings** to display the settings that you want to change. All parameters marked with an asterisk (*) are required.
- 5 Make changes to the settings. To see a list of these settings, see the following topics:
 - [Configure a Connection to the Configuration Server Directory Service](#) on page 272
 - [Configure Connections to External Directory Services](#) on page 273
- 6 Click **Save**.
- 7 Click **Close** to acknowledge the Execution Status dialog. Click the **X** in the upper right corner to close the Property Settings window.

The options for the directory service have changed. Depending on which settings you modify, you may be required to log out of the HPCA Console and log back in.

Configure a Connection to the Configuration Server Directory Service


Before you configure a connection to your external directory services, you must first create a connection to the internal Configuration Server Directory Service. This is called the HPCA-CS connection.



The HPCA-CS connection cannot be used for policy resolution.

The Configuration Server Directory Service connection (HPCA-CS) is a prerequisite for using the HPCA Console to administer policy. Be sure to configure this connection first before configuring an LDAP or LDAPS (Secure) connection.

To configure the Configuration Server directory service:

- 1 From the Configuration tab, click **Directory Services** in the left pane.
- 2 From the Directory Services detail section, click the  (Create New Directory Service) button. The Directory Service Connection Wizard starts.
- 3 Specify a Display Name and Description. From the **Type** list, select **HPCA-CS**. Only one HPCA-CS directory service can be created.
- 4 Click **Next**.
- 5 Under Connection Settings, you have the following options. All parameters marked with an asterisk (*) are required.
 - For **Startup**, select **Automatic** to automatically start this directory service when the Portal starts.
 - For **Host**, enter the host name or IP address of the Configuration Server.
 - For **Port**, enter the port number for the Configuration Server. The default is 3464.
 - Use **Service Account ID** to set which account you will use to sign in to the Configuration Server. The Service Account is used for both read and write operations. It should have full read and write access to this directory source.
 - Use **Password** to specify the password for the Service Account ID. Retype the password in the **Confirm Password** text box.

- Use **Timeout** to specify in seconds the timeout for your connection to your Configuration Server. Keep the default of 120 unless directed to by HP Support.
- Use **Connection Attempts** to specify how many times the HPCA Console should attempt to connect to your Configuration Server before failing.
- Use **Connection Delay** to specify the amount of time in seconds to delay between connection attempts.

6 Click **Next**.

7 Review the Summary screen. If all properties are correct, click **Commit**.

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

The directory source is added to the Directory Services list.

Configure Connections to External Directory Services



Before you configure a connection to your external directory services, follow the instructions to [Configure a Connection to the Configuration Server Directory Service](#) on page 272.

You can administer LDAP policies through the HPCA Console by assigning Services to Directory Service objects.

Before you can do this, however, you must configure connections to your external directory services. The following types of external directory services are supported:

- Lightweight Directory Authentication Protocol (LDAP)
- LDAP with Secure Sockets Layer (SSL) support (LDAPS (Secure))

If you are using SSL on your LDAP server, then you should use the LDAPS (Secure) type of connection.

Each external LDAP directory service may be used for any combination of:

- Authentication
- Reporting
- Policy Entitlement

For example, suppose that you have two directories. One contains all user accounts, and the other is specifically for policy. You want to authenticate against the user account directory. In this case, you should create two directory services with their connections defined differently:

- Create one directory service for authentication with a connections where:
 - **Used for Authentication** is selected
 - **Used for Policy** is not selected
 - **Use Service Account** is not selected

Selecting **Used for Authentication** enables users to log in to the HPCA Console using their external LDAP directory account for this directory service.


- Create another for policy where:
 - **Used for Authentication** is not selected
 - **Used for Policy** is selected
 - **Use Service Account** is selected

This configuration will enable you to sign in using the first directory service, and configure policy using the second directory service.



Note that if a directory source is configured with **Used for Authentication**, but **Use Service Account** is not selected, users must sign in using their external LDAP directory credentials. If **Use Service Account** is selected, users can sign in using their local HPCA Console user name and password.

To configure LDAP or LDAPS (Secure) Directory Services:

- 1 From the Configuration tab, click **Directory Services**.
- 2 From the Directory Services detail section, click the  (New Directory Service) button. The Directory Service Creation Wizard starts.
- 3 Specify a **Display Name** and **Description**.
- 4 From the **Type** list, select one of the following options:
 - Select **LDAP** if your LDAP server does not use SSL.
 - Select **LDAP (Secure)** if your LDAP server uses SSL.
- 5 Click **Next**.

- 6 Enter the required connection parameters. You have the following options. All parameters marked with an asterisk (*) are required.
 - For **Startup**, select **Automatic** to automatically start this directory service, when the Portal starts.
 - **Host** is the fully qualified host name or IP address of the LDAP Server.
 - **Port** is the LDAP Port. For LDAP without SSL, the default value is 389. For LDAP(Secure), the default value is 636.
 - Use **Service Account ID**, to set which account that the HPCA Console will use to sign in to the directory services server. The Service Account is used for both read and write operations. It must have full read and write access to this directory source.
 - Use **Password** to specify the password for the Service Account ID. Retype the password in Confirm Password.
 - **Base DN** is used as the root distinguished name (DN) when browsing the directory through the HPCA Console.
 - For LDAP(Secure), also specify the following information:
 - Use **CA Certificate Directory** to specify the directory of the SSL certificate. The path is relative to the server where the Portal is located. For example:


```
<InstallDir>\HPCA\ManagementPortal\etc\CACertificates
```
 - Use **CA Certificate File** to specify the location of the SSL certificate. The path is also relative to the server where the Portal is located. For example:


```
<InstallDir>\HPCA\ManagementPortal\etc\CACertificates\  
<LDAP Certificate File Name>
```
- 7 Click **Next**.
- 8 Enter the required user interface parameters. You have the following options.
 - **Used for Reporting:** When enabled, this directory service becomes enabled in the Reporting tab of the HPCA Console as a filter source. The Reporting Server must be configured to use the Portal as its directory source for this feature to work.
 - **Used for Policy:** When enabled, this directory service can be used in the HPCA Console for policy management.

- **Used for Authentication:** When enabled, this directory service becomes enabled as a sign-in option on the HPCA Console login screen to allow user authentication based on your existing directory users. The following two parameters will become available.
 - **Authentication Group DN:** This is used as the source for authorized users into the HPCA Console. Any user that is a member of this group will be enabled to sign in to the HPCA Console.
 - **Use Service Account:** When enabled, all read and write requests for this directory service will use the **Service Account ID** specified in the **Connection Settings**. When disabled, all read and write requests for this directory service will use the signed-on user's credentials.
- **Leaf Node Filter:** Enter an LDAP-style filter value to filter out nodes with large numbers of data types so that they will not be displayed in the tree navigation view. Objects such as computers and users should be filtered for better usability. Refer to your directory-specific schema to determine the best way to filter each node. The following example filters out computers and users:

```
(!(|(objectclass=user)(objectclass=computer)))
```

- 9 Click **Next**.
- 10 Review the Summary information. If all properties are correct, click **Commit**.
- 11 Click **Close** to acknowledge the dialog.

Job Action Templates

Job Action Templates enable you to pre-define parameters used when creating new jobs.

Job Action Templates are managed in the Infrastructure Management area on the Configuration tab. To view the list of available Job Action Templates, click the **Job Action Templates** link in the left navigation menu.

In the Job Action Templates window, the Enabled column indicates whether or not the template is available when you create a new job using the HPCA Job Creation Wizard. Click any template name to edit its parameters, or click the **New Job Action Template** button to create a new template. See [Create a New Template](#) on page 277 for detailed instructions.

The following Job Action Templates are provided when you install the HPCA Core:

- Patch Connect
- Refresh DTM Schedules
- Security Connect
- Software Connect
- Satellite Synchronization (All)
- Satellite Synchronization (Configuration)
- Satellite Synchronization (Data)

Each of these templates instructs the agent on a target device to connect to the pertinent domain in the CSDB. For example, the Security Connect template causes the agent to connect to the SECURITY domain. This, in turn, forces all services in the SECURITY domain to which the device is entitled to be executed.




Before you can successfully run a Satellite Synchronization or Refresh DTM Schedules job on a client device, the HPCA agent on that client must have performed a prior connect operation to the HPCA Core.

Create a New Template

Use the following procedure to create a new Job Action Template. To modify an existing template, simply click its name in the Job Action Templates list.

To create a new Job Action Template

- 1 From the **Configuration** tab, click and expand **InfrastructureManagement**.
- 2 Click **Job Action Templates**.
- 3 Click the **New Job Action Template** button . The Job Action Template Creation Wizard opens.

- 4 Select a starting point for your new template. You can select from:
 - Blank Template – enables you to define all of the parameters available.
 - Sample Templates – contain pre-defined parameters depending on the connect type or options selected when the template was created. See [Sample Templates](#) on page 280.
 - User-Defined Template – contains the settings specified in another template.
- 5 Click **Next**.
- 6 Define the parameters for the template. All parameters marked with an asterisk (*) are required.

The **UI Setting** drop-down box associated with some parameters determines whether the parameter is displayed when you create a job with the HPCA Job Creation Wizard.

- **Hidden** will not display the parameter.
- **View Only** will show the parameter in the wizard.
- **View & Edit** will show the job and allow you to modify the parameter.

Display Name: Type a name for the template. This name is displayed on the Job Action Templates page.

Description: Type a detailed description for the template. The description is also displayed on the Job Action Templates page.

Enable Template: Select to enable the template. Enabled templates are available for use when you create a job.

Connection Parameters

These items pertain to the managed client system:

Notify Port: Type the Notify port. The default port is 3465.

Job User ID: Type the Job User ID. This is required if job security is enabled on the client device.

Password: Type the password. This is also required if job security is enabled on the client device. Only asterisks will appear when you type the password.

Action Parameters

These items pertain to both Notify and DTM jobs:

Service Selection: Select to display a service selection list in the HPCA Job Creation. Only entitled services are included in the list.

Command: Type the command to run on the remote system when the job is executed. This executable is limited to those available in the HPCA Agent root folder.

Parameters: Type the parameters for the command.

Additional Parameters: Include any additional parameters for the command. Note that any **Additional Parameters** are combined with the **Parameters** specified.

Job Parameters

Concurrent Process Limit: Enter the maximum number of processes allowed for the job. This is the number of “threads” used to process a job—in other words, how many notifies that you want to perform at the same time. The default is 25.

- Use a smaller number for a small network or a risky job
- Use a larger number for a large network

New Process Delay: Enter the time (in seconds) to wait between activating new processes for this job. The default value is based on the connect type. Change this value based on the estimated time it will take for the job to complete on a single target system. The valid range is 60-65,535.

You can use this parameter to manage network traffic and avoid over-running (flooding) the network. Allow at least 20 minutes for OS connects and 5 minutes for Software connects.

7 Click **Submit**.

The new template is displayed in the Job Action Templates window. If **Enable Template** was selected, the template will be available when creating a new jobs with the HPCA Job Creation Wizard. See [Managing Jobs](#) on page 158 for details on using the wizard to create a Notify job.

Sample Templates

Sample templates enable you to create a Job Action Template based on pre-defined parameters normally used for particular connect types. The Sample Templates are defined below.

Patch Connect

Patch Connects are used to update the patches entitled to devices.

Refresh DTM Schedules

DTM job schedules can be refreshed by creating a Notify or DTM job and using the Refresh DTM Schedules job action template. See [Refresh DTM Schedules on Targets](#) on page 167.

Satellite Synchronization (All, Configuration, and Data)

The Satellite Synchronization templates are used to synchronize Satellite servers with the Core server in order to make the latest data available to the Satellites. See [Creating Satellite Synchronization Jobs](#) on page 171.

Security Connect

A Security Connect will resolve any security entitlements from the SECURITY Domain.

Software Connect

A Software Connect is used to update the list of software entitled to the group or device.

Multicast

Multicast is the delivery of information to a group of destinations simultaneously using the most efficient strategy, it is used for Operating System image and application delivery.

- To enable Multicast, click the checkbox and then click **Save**.

Live Network

Live Network settings required to communicate with the HP Live Network content server are configured in the Infrastructure Management area on the Configuration tab. See [Configure the Connection to the HP Live Network Server](#) on page 281.

Live Network updates are configured in the Infrastructure Management area on the Operations tab. See [Live Network](#) on page 232.

Configure the Connection to the HP Live Network Server

Use the LiveNetwork settings to configure the connection used to automatically download the latest security and compliance content from HP Live Network and to establish the RSS feed for the [HP Live Network Announcements](#) dashboard pane. This includes the following items:

- URL for the HP Live Network content server used to download the most recent scanners and data.
- Login credentials for the HP Live Network content server

Passwords entered on this page are encrypted.

You can test your configuration information before you save it. When you request a test, the HPCA Console attempts to connect to the HP Live Network content server. If the connection succeeds, you know that your configuration information is valid. See [Test Your Live Network Settings](#) on page 282 for details.

To specify the HP Live Network connection settings:

- 1 On the Configuration tab, expand the Infrastructure Management area, and click **Live Network**.
- 2 Specify the following information. All parameters marked with an asterisk (*) are required.
 - **HP Live Network User ID**—the user ID for your HP Live Network subscription account.
 - **HP Live Network Password**—the password for your HP Live Network subscription account.

- **HP Live Network Content URL**—the location of the HP Live Network content server for vulnerability definitions and scanners (URL filled in by default).
- **HP Live Network Connector**—the path to the Live Network Connector executable on the system hosting the HPCA Core (path filled in by default).

For more information, see [Run the HP Live Network Connector Manually](#) on page 76 and [Download the HP Live Network Connector](#) on page 236.

- 3 To test the settings that you have specified, click **Test**. See [Test Your Live Network Settings](#) on page 282 for more information.
- 4 Click **Save** to implement your changes.

▶ The HPCA Console does not automatically save your configuration settings after a successful test. You must click the **Save** button if you want to save your settings.

▶ If you leave this page, any information that you entered in the text boxes prior to clicking **Save** will be lost. Be sure to click **Save** if you want to keep this information.

▶ You can use the **Reset** button to restore the most recently saved settings.

Test Your Live Network Settings

When you are configuring your Live Network settings, you can test your settings to make sure that they work before you save them.




To run a test, click the **Test** button in the lower right corner of the page. The HPCA Console first confirms that all required settings are specified and that all settings have the proper format. It then takes the following action:

The HPCA Console attempts to connect to the HP Live Network content server and log in using the user name and password specified. Any proxy information that appears on the Proxy Settings page in the Infrastructure Management configuration area is used.

Depending on network traffic and other parameters, this test can take up to three minutes. A dialog box asks you whether you want to continue with the test. If you want to continue, click **Yes**.

After the test is completed, the Test Results dialog box shows you the outcome of the test. The following table summarizes the possible outcomes and implications of each.

Table 41 Live Network Settings Test Results

Icon	Outcome	Explanation and Suggested Action
	Test was successful.	All settings are valid. Save your configuration.
	Test failed.	<p>Here are some of the more common reasons that a test can fail:</p> <ul style="list-style-type: none"> • A required setting is missing. • A setting is specified using an invalid format (for example, an invalid URL or path name). • A setting is spelled incorrectly. • The login credentials for the HP Live Network content server are not valid (for example, if your subscription has expired).
	Unknown	<p>This outcome does not necessarily mean that your configuration information is invalid. It simply means that the test could not be completed.</p> <p>For example, if the HPCA Console is unable to connect to the HP Live Network content server within three minutes, the test times out. This can occur for the following reasons:</p> <ul style="list-style-type: none"> • The server is unavailable. • Network traffic impedes the connection. • A firewall blocks the connection. <p>This outcome can also occur if the connection goes through a proxy server, and either the proxy information specified is not correct or the proxy server blocks the connection.</p>

To troubleshoot a failed or inconclusive test result, check the spelling and format of all the settings on the tab. Also check the `vms-server.log` file for errors .



You must click the **Save** button to save your settings—even if the test is successful. The HPCA Console does not automatically save your settings.

Device Management

Use the Device Management section to configure alert options, Thin Client, and Remote Control settings.

The following sections describe the available device management options:

- [Alerting](#) on page 284
- [Thin Clients](#) on page 285
- [Configure Remote Control](#) on page 286

Alerting

Use the Alerting section to configure CMI alerts and reporting options.

- [CMI](#) on page 284

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 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**.
- 3 Select the minimum alert severity to report.
- 4 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**.
- 5 Select the minimum alert severity to display on the client device.
- 6 Type the number of seconds an alert should appear on the client device. By default, an alert is displayed for five seconds.
- 7 Click **Save**.

Thin Clients

Thin Client Management service provides Windows CE devices with configuration data. When this service is disabled on a Core, this information will not be available for Satellites or Agents requesting this information.

- To enable Thin Client Management, select the check box and then click **Save**.

Configure Remote Control

The HPCA Console provides the capability to remotely access devices in either the internal or external repository using Windows Remote Desktop Connection, Virtual Network Computing (VNC), or Windows Remote Assistance.

As the HPCA administrator, you can configure the HPCA Console to enable any or all of these connection types. You can also disable remote control altogether.

For each type of connection, you must specify the port on which the remote target devices will be listening for the remote connection. See [Requirements for Remote Connections](#) on page 181 for additional requirements associated with each connection type.

To configure remote control:

- 1 On the Configuration tab, click **Remote Control** in the left navigation tree.
- 2 Select the type of connection (or connections) that you want to enable:
 - **Enable VNC (Virtual Network Computing)**
 - **Enable Windows Remote Desktop**
 - **Enable Windows Remote Assistance**
- 3 For VNC and Windows Remote Desktop, specify the **Port** on which the remote devices will be listening for the remote connection.

It is not necessary to specify a port for Windows Remote Assistance, because Windows Remote Assistance always uses a Distributed Component Object Model (DCOM) interface on port 135.
- 4 Click **Save**.
- 5 Click **Close** to close the Execution Status dialog box.

For information about using the remote control function, see [Controlling Devices Remotely](#) on page 180.

Patch Management

Use the Patch Management section to enable patch management and define ODBC parameters for your patch database. Patch Management options are explained in the following:

- [Database Settings](#) on page 287
- [Preferences](#) on page 295
- [Agent Options](#) on page 291
- [Agent Updates](#) on page 294
- [Vendor Settings](#) on page 297
- [Patch Distribution Settings](#) on page 288
- [Acquisition Jobs](#) on page 311

Patch Distribution Settings allow you to choose a new, lightweight model for applying Microsoft patches. For details, see the chapter:

- [Patch Management Using Metadata](#) on page 325.

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 Patch database with the Core authoritative CSDB 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.

Patch Distribution Settings

Use the Patch Distribution Settings area to enable and configure the:

- Patch Metadata Download option

When this option is enabled, the page also displays the related options for:

- Patch Gateway Operations settings

These options allow you to patch Microsoft devices using Microsoft Update Catalog with the lightweight acquisition and distribution model.



The use of Patch Management using Metadata also *requires* you to **Enable the Download Manager**. To do this, go to the **Configuration > Patch Management > Agent Options** page.

HP recommends using the Patch Metadata download and gateway operations for patching Microsoft devices whenever possible. It offers several advantages as discussed in the chapter [Patch Management Using Metadata](#) on page 325.

- **Enable Download of Patch Metadata only** Check this box to manage Microsoft patches using the lightweight, Metadata mechanism. It requires the use of a Microsoft Update Catalog data feed.

With this option, only metadata is downloaded and published to the Configuration Server Database, and the patch binary files are downloaded and cached to the Patch Manager Gateway when an Agent requests them or when the Gateway is preloaded.

Patch Metadata Download

Enabling this option results in the patch metadata and NOT the binaries being acquired and populated to the Configuration Server. Once the agent determines the exact binary it requires, the same can be fetched from the Patch gateway. (This option is available with Microsoft Update Catalog option only).

Enable Download of Patch Metadata only



If you Enable Patch Metadata downloads, you must also enable and configure the following before running an acquisition:

- **Patch Gateway Operations (Required)**
- **Agent Options: Enable the Download Manager (Required)**



When Enable Patch Metadata downloads is checked, the Vendor value to acquire patches switches from MICROSOFT to MSFT.



For additional details on configuring your environment and acquiring patches using Metadata download and gateway operations, see [Patch Management Using Metadata](#) on page 325. Make sure to configure Offline Scanning and set the Download Manager Preload option.

Patch Gateway Operations

The Patch Gateway Operations settings are available if the Patch Metadata Download option is enabled from the Patch Distribution page.

Use these settings to enable the gateway.

Once enabled, additional entries allow you to configure it for caching and managing the patch binaries.

The Patch Gateway is required in order to use the Patch Metadata Download option for the lightweight patching of Microsoft Agents with one of the Microsoft Update Catalog data feeds.

The role of the Patch Gateway is to download, cache and deliver the actual patch binary data to the Agents when Enable Patch Metadata downloads, only, is turned on. There is an optional Gateway preload option that allows patch binaries to be cached into the gateway upon acquisition, as opposed to when they are requested from the agents.

- **Enable Gateway** Check this box to make the Gateway available for on-demand downloading and caching of Microsoft patch binary data. This is required to use the lightweight Patch Metadata Download option with one of the **Microsoft Update Catalog** data feeds.

When Enable Gateway is checked, the following fields are available:

- **Maximum Cache Size** Specifies the maximum size of the Gateway cache in megabytes. Blank or zero means “do not limit the cache”.

Default: 1000 MB

- **Time for which the Binary is valid** Specifies the maximum time, in hours:minutes:seconds format, that the gateway will keep a cached binary file without re-validating it from the upstream server. A value of -1 or blank means the binary will not be refreshed. A value of 10:00:00 means the binary will be downloaded again after 10 hours of being in the cache.

Default: Blank (no refresh)

- **Preload Gateway Cache** Optionally, specify **Yes** to have the patch binaries cached on the Gateway when you run an acquisition. HP cautions you before setting the preload option. The advantage of preloading is that the first agent that requests the patch binary can obtain it without having to first wait for the gateway to download it. However, the disadvantage of preloading is that it results in downloads of all the patch binaries for an acquisition—regardless of whether the agents will need them or not.

Specify **No** (the default) if you want the gateway to download and cache the patch binary data only when it receives Agent requests for the patches.

Patch Gateway Operations

The Patch Gateway is a server where the binaries can be downloaded, cached and provided to the Agent machines.

Enable Gateway

Maximum Cache Size MB

Time for which the Binary is valid HH:MM:SS

Preload Gateway Cache

[Return to Top](#)

Agent Options

These Agent Options apply to patching Microsoft devices, only.

Use the Agent Options available from the Configuration tab > Patch Management area to enable and configure these Patch Manager Agent options for patching Microsoft Devices.

The next time the Patch Agents connect to the HPCA servers they will receive any configuration changes that you set on these panels.

- [Download Manager Option](#) on page 291
- [Agent Options for Patch Agents](#) on page 293

Download Manager Option

- **Enable Download Manager:** Check this box to have Download Manager control the download of the required patch files onto the Agent machines using a background, asynchronous process. The Download Manager operates outside of the normal HPCA Agent Connect process.




Download Manager must be enabled to use Patch Distribution using Metadata.


When checked, several Download Manager options are displayed.


Download Manager Options


Enable Download Manager to transfer the files required to apply patches onto the managed devices in the background, outside of the usual HPCA Agent connect process. This option allows for bandwidth throttling and an automatic stop and start of the download until it completes.

Enable Download Manager

 **Network Utilization** %

 **Network Utilization in Screensaver Mode** %

 **Delay initialization** Minutes

 **Apply patches after download completion**

Complete the Download Manager Options using the following information.

Set specific options for network utilization, network utilization in Screen Saver Mode, delay after initialization, and whether or not to apply the patches after download completion.

Table 42 Download Manager Options for Patch Agents

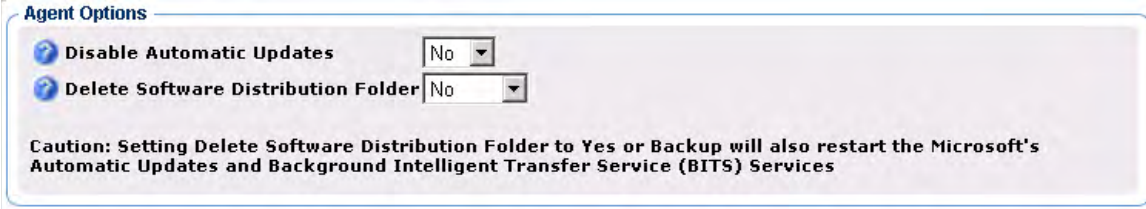
Option and Valid Values	Description
<p>Network Utilization Values = 0 to 100 % 0 is default</p>	<p>Specifies the maximum percent of available network bandwidth to use to download the patch files when the device is active.</p> <p>A value of 0 means the download will use the available network bandwidth.</p> <p>Example: 25 specifies no more than 25% of the available bandwidth should be used for the patch download process.</p>
<p>Network Utilization in Screensaver Mode Values = 0 to 100 % 0 is default</p>	<p>Screen Saver network utilization option. Specifies the maximum percent of available network bandwidth to use to download the patch files when Screen Saver is on. This is typically a larger percent than when Screen Saver is off.</p> <p>A value of 0 means the download will use the available network bandwidth when Screen Saver is on.</p> <p>Example: 80 increases the bandwidth used to download the patch files 80% when screen saver is on.</p>
<p>Delay initialization Values = 0 to 999 minutes 0 is default</p>	<p>Upon initialization, specifies the number of minutes to delay before starting or resuming the download of patches. This allows other processes to startup first, and then resume the patch download.</p> <p>Example: Set to 15 to delay initialization 15 minutes.</p> <p>A value of 0 means there is no delay.</p>
<p>Apply patches after download completion Values = Yes or No (default)</p>	<p>After download completion, set to Yes to trigger a Patch Agent Connect to apply the patches. HP recommends setting the value to Yes.</p> <p>Leave the default of No to have the patches applied whenever the next Patch Agent Connect takes place.</p>

Click Save to set these configuration options. The Patch Agents will receive the new configuration the next time they connect to the HPCA servers.

Agent Options for Patch Agents

The following Agent Options are available for patching Microsoft devices.

- **Disable Microsoft Automatic Updates:** Select Yes or No from the drop-down box. Use this option to address issues whereby the Patch Agent scan or deployment is getting interrupted because Automatic Updates is set to ON.
 - **Yes:** The Patch Agent will disable Microsoft Automatic Updates before each scan or deployment. Once Patch scan/deployment is done, it reverts the Automatic Updates to its original state.
 - **No:** (The default) The Patch Agent will not disable Automatic Updates before each scan or deployment..




Agent Options

Disable Automatic Updates

Delete Software Distribution Folder

Caution: Setting Delete Software Distribution Folder to Yes or Backup will also restart the Microsoft's Automatic Updates and Background Intelligent Transfer Service (BITS) Services

- **Delete Software Distribution Folder:** Select Yes, Backup, or No from the drop-down box. This option is available to address the following issues:
 - Drastic growth in the size of the SoftwareDistribution folder
 - SoftwareDistribution folder corruption
 - Increased load on the Configuration Server during Patch connects
-  Setting Delete Software Distribution folder to Yes or Backup automatically restarts the services for Microsoft Automatic Updates and BITS. HP warns against setting this option if the service restarts will cause issues in your environment, especially for those customers who are using both HPCA Patch Management and Automatic Updates as co-located patch solutions.

Set this option to Yes or Backup to improve Patch Manager performance due to folder size, corruption, or infrastructure load issues.

- **Yes:** The Patch Agent deletes the contents of the SoftwareDistribution folder before every patch scan. Read the Caution (above) on service restarts.
- **Backup:** The Patch Agent first backs up and then deletes the contents of the SoftwareDistribution folder before every patch scan. Read the Caution (above) on service restarts.
- **No: (Default)** The Patch Agent will not do anything to the SoftwareDistribution folder.

Click Save to set the configuration option. The Patch Agents will receive the new configuration the next time they connect to the HPCA servers.

Agent Updates

Use Agent Updates to configure agent updates for Patch Management.

HP Patch Agent Updates Settings

These settings are used to acquire and apply maintenance for HP Client Automation (HPCA) Patch Manager agent files. For more information on this, see [View Agent Updates](#) on page 244. The following settings are configured in the HP Patch Agent Updates section.

- **Updates:** If you select Publish, the updates will be published to the PATCHMGR Domain, but will not be connected for distribution (deployment) to Patch Manager target devices. You will need to create these connections. If you select Publish and Distribute, the updates will be published to the PATCHMGR Domain and connected to the DISCOVER_PATCH instance. This option will distribute the updates to your Patch Manager target devices.
- **OS:** Specify the vendor operating system types for which you wish to acquire and manage Patch Manager agent updates.
- **Version:** Select the Patch Manager Version for which you would like to acquire agent updates. You can only publish one version to one Configuration Server. The default is the latest available Version.



If you are installing Patch Manager for the first time, do not modify the Version parameter from the installation default.

HP Client Automation Patch Agent Updates

Updates None Publish Publish and Distribute

OS Windows Linux

Version Version 3 Version 5 Version 7

[Return to Top](#)

Preferences

Under Preferences, configure vendors and acquisition settings. These settings will be reflected in the Vendor Settings and Acquisition Jobs.

- **Enable Patch Management For:** Specify the OS vendors you will be acquiring patches for. These vendors will be represented in Vendor Settings and Acquisition Settings. If you decide at a later date to acquire patches for additional vendors, they must be enabled here, first.
- **Save Acquisition Summary:** Specify how long in days to keep the Patch Auth Store (PASTORE) instances. This class contains one instance for each patch acquisition session. If this value is smaller than the Save History Detail value, then Save History Detail will be set to the value for Save Acquisition Summary. The value 0 means never delete any history of Patch Acquisition.
- **Save History Detail:** Specify how long in days to keep the Publisher Error (PUBERROR) instances. This class contains one instance for each patch acquisition error.
- **Patch Data Repository Path:** The directory where patches are downloaded to before they are published to the Configuration Server. If you choose to perform an acquisition using a directory that is pre-populated with data from a previous acquisition, specify the pre-populated directory path in this parameter.
- **Retired Bulletins:** Shows the bulletins to retire separated by commas. This parameter works on the bulletin level, not at the product or release level.

The retire function performs these functions.

- Deletes specified bulletins if they exist in the Configuration Server DB during the current publishing session.
- Does not publish the bulletins specified in the retire parameter to the Configuration Server DB during the current publishing session. The use of the Retire option supersedes the Bulletins option.
- **Excluded Products:** Precede any products you want excluded with an exclamation point (!) in the format of *vendor::product* in a comma separated list. If an include filter is not set, all products are assumed. If you provide any included filters, then the excluded filters will be a subset of the included products. Be sure to conform to the vendor's naming standards. For example, Microsoft refers to Internet Explorer using its full name, rather than a common abbreviation such as IE. For example, to include all Windows products except Windows 95, type
`{Microsoft::Windows*,Microsoft::!Windows 95}`.

For new Patch Manager installations, the acquisition and management of Security patches for the following products are *excluded, by default*: Microsoft Office, Windows 95, Windows 98, Window Me, and Microsoft Office products and SuSE specific products *-yast2, *-yast2-*, and *-liby2. The automated management of SuSE OS yast specific products are not supported by Patch Manager.

- ▶ If you are migrating from a previous version of Patch Manager and did not remove your `patch.cfg` before migration, if you wish to exclude all Microsoft Office products or their standalone versions from Patch Manager acquisition and management, append the following text to your product exclusion list:

```
" ,!Access* ,!Excel* ,!FrontPage 200 [023] ,!FrontPage 9 [78] ,!InfoPath* ,!Office* ,!OneNote* ,!Outlook* ,!PowerPoint* ,!Project 200 [023] ,!Project 98 ,!Publisher* ,!Visio* ,!Word* ,!Works* "
```

Note the text shown above is all one line and the quotes displayed above are *not* to be included in the user interface Excluded Product text box.

Preferences

Enable Patch Management For:

Microsoft Red Hat

SUSE HP SoftPaq

Save Acquisition Summary

Save History Detail

Patch Data Repository Path*

Retired Bulletins

Excluded Products

- **Default Patch Acquisition Download Language:** Specify the languages for which you want to acquire and manage security patches. The default is en (English).

Vendor Settings

Vendor Settings displays vendor-specific URLs and other options required for patch acquisition and management activities on the agents in your enterprise.

Before entering Vendor Settings, first use the Preferences page to enable the appropriate vendor(s) and OS selections.



If you change vendor settings from one acquisition session to the next so that you exclude one or more products or operating systems that were previously selected, all patches specific to the excluded products or operating systems will be removed from the Configuration Server Database. This also means the excluded products or operating systems are no longer eligible for vulnerability assessment and management. This applies to all vendors.

Vendor Settings:

- [Microsoft Data Feed Prioritization](#) on page 298
- [Red Hat Feed Settings](#) on page 301
- [SuSE Feed Settings](#) on page 303

- [HP SoftPaq Feed Settings](#) on page 307

Microsoft Data Feed Prioritization

The following Microsoft Data Feed Prioritization settings are configured in the Vendor Settings section to support and prioritize the available Microsoft update repositories and methods for acquisition and download.

When the Patch Distribution Settings have the option to **Enable Download of Patch Metadata only** turned on, you have the option to choose one of the Microsoft Update Catalog data feeds.

Microsoft Data Feed Prioritization

Microsoft Update Catalog Only - All devices and products managed by Patch Manager must meet minimum service pack levels.

Microsoft Update Catalog, Legacy Catalog

[Return to Top](#)

When the Patch Distribution Settings have the option to **Enable Download of Patch Metadata only** turned off, the Microsoft Data Feed Prioritization panel includes three choices:

Microsoft Data Feed Prioritization

Do not change data feed prioritizations until you have read and understood Microsoft's operating system and service pack requirements for Microsoft Update Catalog.

Data Feed Prioritization:

MSSecure, Microsoft Update Catalog, Client Automation

Microsoft Update Catalog Only - All devices and products managed by Patch Manager must meet minimum service pack levels.

Microsoft Update Catalog, Legacy Catalog

[Return to Top](#)



For more information on Microsoft patch management activities, see the Patch Acquisition chapter in the HPCA Patch Manager Installation and Configuration Guide.

- **MSSecure, Microsoft Update Catalog, Client Automation:** This option is displayed when the Patch Metadata Download option is turned off. Patches are acquired from both MSSecure and Microsoft Update Catalog. If a patch exists in both the MSSecure and Microsoft Update Catalog, then the technologies supporting MSSecure are used.

▶ Due to MSSecure technologies, this option cannot patch devices running Windows Vista (32-bit or 64-bit) or Windows on 64-bit architectures. To patch these devices, choose a Data Feed Prioritization that includes Microsoft Update Catalog.

⚠ At the time of this writing, Microsoft's web site states that MSSecure.xml will no longer be updated after October 9, 2007, although they have continued to update their legacy catalog into 2008.

- **Microsoft Update Catalog Only:** (Default option) All patches are acquired from the Microsoft Update Catalog. To use this option, all devices in the enterprise must meet minimum operating system and product levels as set by Microsoft. Devices not meeting these minimum requirements will not be patched.

If you change to this option, the following warning message will open, which you must accept to continue.

Microsoft Data Feed Prioritization

Do not change data feed prioritizations until you have read and understood Microsoft's operating system and service pack requirements for Microsoft Update Catalog.

Data Feed Prioritization:

MSSecure, Microsoft Update Catalog, Client Automation

Microsoft Update Catalog Only - All devices and products managed by Patch Manager must meet minimum service pack levels.

Microsoft Update Catalog, Legacy Catalog

The Microsoft Update Catalog Only feed was selected. Only select this option if ALL managed devices in your enterprise meet minimum operating system and service pack levels supported by Microsoft Update Catalog.

By selecting the option Microsoft Update Catalog Only, security bulletin acquisition and management is limited to the operating systems and products supported by Microsoft Update Catalog and Patch Manager. Patch acquisition and management capabilities are NOT provided for Microsoft legacy operating system platforms.

Confirm selection? [More Information](#)

[Return to Top](#)

When you click **Yes**, you will again be prompted to make sure that this is the option you want. Click **Save** to confirm.

- **Microsoft Update Catalog, Legacy Catalog:** Patches are acquired from the Microsoft Update Catalog and an HP repository containing current MSSECURE and HP-corrected metadata, referred to as the Legacy Catalog. If a patch exists in both the Microsoft Update Catalog and the Legacy repository, then:
 - If the target device meets the minimum OS requirements supported by Microsoft Update Catalog, the device will be patched by leveraging Microsoft Update Catalog and Windows Update Agent technologies.
 - If the target device does not meet the minimum OS requirements supported by Microsoft Update Catalog, the device will be patched using MSSECURE technologies, using meta data hosted in the Legacy Catalog.
- ▶ The HP Legacy Catalog will continue to be updated by HP as new patches are added to MSSECURE. Patches hosted in the HP Legacy Catalog may require HP metadata correction. If you choose to enable the **Microsoft Update Catalog, Legacy Catalog** option Microsoft security bulletins deemed applicable to legacy Microsoft Operating systems (including Service Pack variants) and Microsoft products will have a “_L” appended to the Microsoft bulletin name for identification purposes within the Configuration Server PATCHMGR Domain as well as Patch Manager reports as viewed through the Reporting Server.
- ⚠ Office patches that are acquired and managed using Microsoft Update Catalog technologies will not detect if Office Applications are managed by HP Client Automation Application Self-service Manager or an Administrative Control Point. In either case, if a bulletin affecting an Office application is entitled to a device, Patch Manager will manage the Office patch and install it locally on the devices that are vulnerable.

Microsoft Feed Settings

The following settings are configured in the Vendor Feeds section:

Advanced-only Fields

- **MSSecure*:** Specifies the URL for Microsoft’s MSSecure cabinet file which contains the Microsoft supplied MSSECURE.XML file.

Default: **http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB**

▶ At the time of this writing, Microsoft Knowledge articles suggest Microsoft plans to discontinue support and updates for `MSSecure.xml` after October 9, 2007 even though they have continued to update this catalog into 2008.

- **SUS***: Specifies the URL for the Microsoft cabinet file that contains the Microsoft SUS data feed.

Default: **<http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab>**

Basic and Advanced Fields

- **Architecture**: Select the architectures for the acquisition of Microsoft patches. The supported architectures include:
 - **x86** for 32-bit Intel architectures
 - **x64** for AMD64 or Intel EM64T. If this target architecture is selected, your Microsoft Data Feed Prioritization must be set to either **Microsoft Update Catalog Only** or **Microsoft Update Catalog, Legacy Catalog**.

Microsoft Feed

MSSecure*

SUS*

Architecture x86 x64 (AMD64/Intel EM64T)

[Return to Top](#)

Red Hat Feed Settings

The following settings are configured in the Red Hat Feed section:

Advanced-only Fields

- **Red Hat**: Specifies the URL for the Red Hat Network data feed. The default is **<http://xmlrpc.rhn.redhat.com/XMLRPC>**.

Basic and Advanced Fields

- **Publish Package Dependencies**: Specify **yes** if you want to publish additional Red Hat packages that downloaded security advisories may depend on. The default is No.

Prerequisite, or dependent, Red Hat packages required to install Red Hat Security Advisories can be acquired from two places. They can either be downloaded from the Red Hat Network during acquisition or they can be found locally if previously copied from the Red Hat Linux installation media. During an acquisition, Patch Manager will first look for the .rpm packages in the appropriate directory. For example:

- For Red Hat Enterprise Linux 4ES on x86, place the baseline operating system rpm files supplied on Red Hat installation media in `Data\PatchManager\Patch\redhat\4es`.
- For Red Hat Enterprise Linux 4ES on x86-64, place the baseline operating system rpm files supplied on Red Hat installation media in `Data\PatchManager\Patch\redhat\4es-x86_64`.
- When naming the `Data\PatchManager\Patch\redhat\packages` subdirectories, refer to the list of **OS Filter Architecture** values below. Use the applicable folder name based on the value following `REDHAT::` as the subdirectory name.

If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, HP recommends copying the dependency packages to the appropriate packages directory from your Linux installation media. The Red Hat RPM packages can be found on the Linux installation media under the `RedHat/`RPMS directory.

- **OS Filter:** Support is provided for x86 (32-bit Intel) and x86-64 (Opteron/EMT64) architectures for: all combinations of Red Hat Version 4 and Releases AS, ES and WS, and all combinations of Red Hat Version 5 Releases for Servers and Desktop clients. For a given architecture, select the operating system and release combination for the acquisition of Red Hat patches.

- **x86** Architectures: Possible values for Red Hat x86 architectures in the `patch.cfg` file are:

```
REDHAT::4as,          REDHAT::4es,          REDHAT::4ws,
REDHAT::5server,     REDHAT::5client
```

- **x86-64** Architectures: Possible values for Red Hat x86-64 architectures in the `patch.cfg` file are:

```
REDHAT::4as-x86_64,   REDHAT::5server-x86_64,
REDHAT::4es-x86_64,   REDHAT::5client-x86_64,
REDHAT::4ws-x86_64
```

Red Hat Feed

Red Hat

Publish Package

Dependencies?

OS Filter

x86 4AS 4ES 4WS 5 Server 5 Client

x86-64 4AS 4ES 4WS 5 Server 5 Client

[Return to Top](#)

SuSE Feed Settings

To configure settings for patching SuSE Linux, choose one or both SuSE Linux Product Types, and then choose the SuSE Feed Setting for the Version Levels and OS platforms that are in your environment. SuSE 9 feed settings are grouped separately from those for SUSE 10.

Related Topics:

- [SuSE Requirements for Patch Management](#) on page 309

Switch from the Basic to Advanced settings if you also need to set or fix the URLs for the SuSE meta data feeds.

Product Type

Select the SuSE Linux product types installed on the devices in your environment.

- **Enterprise Server:** Specifies the SuSE Linux Enterprise Server (SLES) product type, available with SuSE Versions 9, and 10.
- **Enterprise Desktop:** Specifies the SuSE Linux Enterprise Desktop (SLED) product type, available with SuSE Version 10.

SUSE Feed

Product Type Enterprise Server Enterprise Desktop

SuSE 9 Feed Settings

Click **Advanced** to view or modify the default URLs for SuSE 9 feed settings that are listed below.

Advanced-only Fields

- **SuSE 9:** Specifies the secure URL to acquire security advisory meta data for SuSE 9. The defaults are:

`https://you.novell.com/update/i386/update/SUSE-CORE/9/`
`https://you.novell.com/update/i386/update/SUSE-SLES/9/`

- **SuSE 9-x86_64:** Specifies the secure URL for acquiring updates for SuSE 9 on AMD64 or Intel EM64T architectures. The defaults are:

`https://you.novell.com/update/x86_64/update/SUSE-CORE/9/`
`https://you.novell.com/update/x86_64/update/SUSE-SLES/9/`

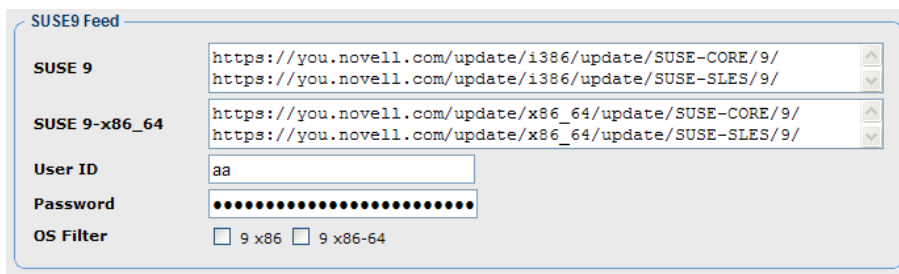
Basic and Advanced Fields

Use the Basic or Advanced page to enter the required settings for obtaining SuSE 9 Data Feeds.

- **UserID:** Specifies your SuSE user ID. Obtain a user id from the vendor.
- **Password:** Specify the password for the SuSE UserID.
- **OS Filter:** Select the operating system version and architecture combinations for the acquisition of SuSE Linux Enterprise Server patches. Support is provided for SuSE Versions 9 on x86 (32-bit) architecture as well as x86-64 (AMD64 and Intel EM64T) architectures.

The valid OS Filter value for x86 architectures in patch.cfg is `suse::9`.

The valid OS Filter values for x86-64 architectures in patch.cfg is `suse::9-x86_64`.



The screenshot shows a web form titled "SUSE9 Feed" with the following fields:

- SUSE 9:** A text area containing two lines of default URLs: `https://you.novell.com/update/i386/update/SUSE-CORE/9/` and `https://you.novell.com/update/i386/update/SUSE-SLES/9/`. It has up and down arrow icons on the right.
- SUSE 9-x86_64:** A text area containing two lines of default URLs: `https://you.novell.com/update/x86_64/update/SUSE-CORE/9/` and `https://you.novell.com/update/x86_64/update/SUSE-SLES/9/`. It has up and down arrow icons on the right.
- User ID:** A text input field containing the value "aa".
- Password:** A password input field with 12 dots representing the masked characters.
- OS Filter:** Two radio button options: 9 x86 and 9 x86-64.

SuSE 10 Feed Settings

SuSE Version 10 support includes SuSE Linux Enterprise Server 10 (SLES10) and SuSE Linux Enterprise Desktop 10 (SLED10).

- To obtain SLES 10 security advisories, check the Product Type of Enterprise Server.
- To obtain SLED 10 security advisories, check the Product Type of Enterprise Desktop.

Click **Advanced** to view or modify the default URLs for SuSE 10 feed settings that are listed below.

Advanced-only Fields

- **SUSE 10:** Specifies the secure URL to acquire security advisory meta data for SUSE 10 (SLES10 and SLED10) on x86 architectures.

Defaults:

[https://nu.novell.com/repo/\\\$RCE/SLES10-Updates/sles-10-i586/](https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-i586/)
[https://nu.novell.com/repo/\\\$RCE/SLED10-Updates/sled-10-i586/](https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-i586/)

- **SUSE 10SP1:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 1 on x86 architectures.

Defaults:

[https://nu.novell.com/repo/\\\$RCE/SLES10-SP1-Updates/sles-10-i586/](https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-i586/)
[https://nu.novell.com/repo/\\\$RCE/SLED10-SP1-Updates/sled-10-i586/](https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-i586/)

- **SUSE 10SP2:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 2 on x86 architectures.

Defaults:

[https://nu.novell.com/repo/\\\$RCE/SLES10-SP2-Updates/sles-10-i586/](https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-i586/)
[https://nu.novell.com/repo/\\\$RCE/SLED10-SP2-Updates/sled-10-i586/](https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-i586/)

- **SUSE 10-x86_64:** Specifies the secure URL to acquire security advisory meta data for SUSE 10 (SLES10 and SLED10) on x86-64 architectures.

Defaults:

[https://nu.novell.com/repo/\\\$RCE/SLES10-Updates/sles-10-x86_64/](https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-x86_64/)
[https://nu.novell.com/repo/\\\$RCE/SLED10-Updates/sled-10-x86_64/](https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-x86_64/)

- **SUSE 10SP1-x86_64:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 1 on x86-64 architectures.

Defaults:

**https://nu.novell.com/repo/\\$RCE/SLES10-SP1-Updates/
sles-10-x86_64**

**https://nu.novell.com/repo/\\$RCE/SLED10-SP1-Updates/
sled-10-x86_64/**

- **SUSE 10SP2-x86_64:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 2 on x86-64 architectures.

Defaults:

**https://nu.novell.com/repo/\\$RCE/SLES10-SP2-Updates/
sles-10-x86_64/**

**https://nu.novell.com/repo/\\$RCE/SLED10-SP2-Updates/
sled-10-x86_64/**

Basic and Advanced Fields

Use the Basic or Advanced page to enter these required settings for obtaining SuSE 10 Data Feeds.

- **UserID:** Specifies your SUSE 10 user ID. Obtain a user id from the vendor. For details, see [SuSE Requirements for Patch Management](#) on page 309.
- **Password:** Specify the password for the SUSE UserID.
- **OS Filter:** Select the operating system *version*, *service pack* and *architecture* combinations for the acquisition of SUSE Version 10 patches. Support is provided for SUSE Version 10 base and Service Packs 1 and 2 on x86 (32-bit) architectures, as well as SUSE Version 10 base and Service Packs 1 and 2 on x86-64 (AMD64 and Intel EM64T) architectures.

Valid OS Filter values for x86 architectures in patch.cfg are `suse::10`, `suse::10SP1`, and `suse::10SP2`.

Valid OS Filter values for x86-64 architectures in patch.cfg are `suse::10-x86_64`, `suse::10SP1-x86_64` and `suse::10SP2-x86_64`.

SUSE10 Feed	
SUSE 10	https://nu.novell.com/repo/SRCE/SLES10-Updates/sles-10-1586 https://nu.novell.com/repo/SRCE/SLED10-Updates/sled-10-1586
SUSE 10SP1	https://nu.novell.com/repo/SRCE/SLES10-SP1-Updates/sles-10-1586 https://nu.novell.com/repo/SRCE/SLED10-SP1-Updates/sled-10-1586
SUSE 10SP2	https://nu.novell.com/repo/SRCE/SLES10-SP2-Updates/sles-10-1586 https://nu.novell.com/repo/SRCE/SLED10-SP2-Updates/sled-10-1586
SUSE 10-x86_64	https://nu.novell.com/repo/SRCE/SLES10-Updates/sles-10-x86_64 https://nu.novell.com/repo/SRCE/SLED10-Updates/sled-10-x86_64
SUSE 10SP1-x86_64	https://nu.novell.com/repo/SRCE/SLES10-SP1-Updates/sles-10-x86_64 https://nu.novell.com/repo/SRCE/SLED10-SP1-Updates/sled-10-x86_64
SUSE 10SP2-x86_64	https://nu.novell.com/repo/SRCE/SLES10-SP2-Updates/sles-10-x86_64 https://nu.novell.com/repo/SRCE/SLED10-SP2-Updates/sled-10-x86_64
User ID	<input type="text"/>
Password	●●●●●●●●●●●●●●●●●●●●
OS Filter	<input checked="" type="checkbox"/> 10 x86 <input checked="" type="checkbox"/> 10SP1 x86 <input type="checkbox"/> 10SP2 x86 <input type="checkbox"/> 10 x86-64 <input type="checkbox"/> 10SP1 x86-64 <input type="checkbox"/> 10SP2 x86-64

HP SoftPaq Feed Settings

The following settings are configured in the HP SoftPaq Feed section. Click **Advanced** to see all fields, including the HP SoftPaq URL field, click **Basic** to return to the Basic page.

Use the predefined job named `hpsoftpaq` to acquire the HP Softpaqs for the SysIDs and Bulletins specified here. The `hpsoftpaq` job is listed with the available jobs on the **Start Acquisition** operation.

Advanced field

- **HP SoftPaq URL:** Specifies the URL for the HP SoftPaq data feed. The default is <http://h20278.www2.hp.com/hpapps/onlineDiag/ActiveCheck>.

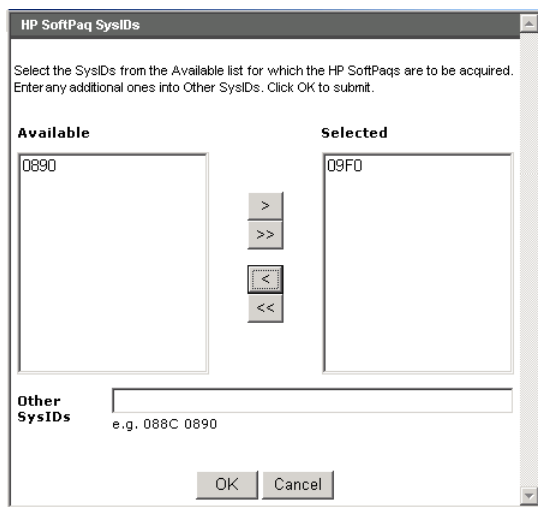
Basic and Advanced fields

- **HP SoftPaq Types:** Check the types of HP SoftPaqs to acquire and manage.
 - Application
 - Bios
 - Driver
 - Firmware

- **SysIDs:** Specifies the SysIDs that will be acquired for HP SoftPaqs.

If your HP devices have reported inventory information to the HPCA database, SysIDs can be selected from a list using the Get SysIDs button:

- Click **Get SysIDs** button. This opens the HP SoftPaq SysIDs dialog box. The Available column lists any HP SoftPaq SysIDs reported from your HPCA-inventoried HP devices.
- Use the arrow buttons to move individual SysIDs from the **Available** column to the **Selected** column. SysIDs in the Selected column will be acquired.
- Optionally, use the **Other SysIDs** text area to enter space-separated SysIDs not already listed in the Selected column. For example, enter:
0890 8844 30A4 300F
- Click **OK** to return to the Vendor page for HP SoftPaq.



The **SysIDs** list will show the ‘Selected’ plus ‘Other SysIDs’ entries from the HP SoftPaq SysIDs dialog box.

- **Bulletins:** HP SoftPaqs are acquired using the pre-defined acquisition job, named hpsftpaq. Use the Bulletins area to enter the bulletins to be acquired when the hpsftpaq job is run. To acquire all bulletins for the

SysIDs, enter:

SP*:

HP SoftPaq Feed

HP SoftPaq URL

HP SoftPaq Types Application Bios
 Driver Firmware

SysIDs

Bulletins

[Return to Top](#)

Click **Save** to save your Vendor settings. Click **Apply Configuration Changes Now** before exiting the Configuration tab area to have them applied to the system.

A job to acquire HP Softpaqs is predefined. To run it, select `hpsoftpaq` from those listed within the **Start Acquisition** operation.

SuSE Requirements for Patch Management

SuSE feed settings require a secure (SSL) connection and a Vendor-supplied User ID and password, as discussed in this topics.



SuSE 10 devices have additional requirements; see [SuSE 10 Registration Requirements](#) on page 310.

SSL: The Novell website requires a secure (SSL) connection for patch acquisition. The need for a secure connection within Patch Manager is only required on the server that is used to perform secure patch downloads from the Novell website. At the time of this writing, the Novell website does not require or perform certificate validation.

SuSE Linux Vendor User ID and password: The requirements for obtaining a Vendor User ID and password vary by SuSE Version number.

- **SuSE 9:** For SuSE 9 security patch acquisition, you must establish a User ID and password through your SuSE Linux vendor to access SuSE Internet resources. Specify these credentials when you configure SuSE devices for Patch Management using the Console's **Configuration tab > Patch Management > Vendor Settings** page.

- **SuSE 10:** For SuSE 10 security patch acquisition of SLES10 or SLED10, you must establish mirror credentials through your SuSE 10 Linux vendor to access SuSE 10 Channels. Specify these credentials when you configure SuSE for Patch Management using the Console's **Configuration tab > Patch Management > Vendor Settings** page.

To obtain SuSE 10 mirror credentials:

- 1 Establish the username and password for login to the Novell Customer Center (NCC) through your SuSE Linux vendor when the SuSE 10 product is bought.
- 2 Login to the NCC using using the login account information given by the vendor when the SuSE10 product was bought.
- 3 Click on **Mirror Credentials** under the **Myproduct** link in the left panel.
In the Credentials area of the Mirrors Credentials page, you will see the Username and Password. In the Channels area, you will see the SuSE 10 Channel details.
- 4 Use the Username and Password obtained from the above steps when completing the SuSE 10 User ID and password credentials for SuSE 10 Patch Acquisition. See the Vendor Settings topic for configuring [SuSE 10 Feed Settings](#) on page 305.

SuSE 10 Registration Requirements

Starting with SuSE 10 and onwards, Novell's explicit policy states that in order to receive security patches and updates each SuSE 10 agent Operating System must be registered with Novell and have their licenses managed and validated either directly through the Novell Customer Center (NCC) or Subscription Management Tool.



HPCA Patch Management does not validate that Novell's SuSE10 license or registration policy is met. It is the customer's responsibility to adhere to Novell's policy and have their SuSE10 machines registered with validated licenses.

To register your SuSE 10 systems with the Novell Customer Center

Refer to the Novell website for details on registering your SuSE 10 systems with the Novell Customer Center.

As of this writing, the topic *Registering and Updating SUSE Linux Enterprise 10* is available at:

<http://www.novell.com/support/dynamicckc.do?cmd=show&forward=nonthreadedKC&docType=kc&externalId=3410833&sliceId=1>

Acquisition Jobs

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

To create and run Patch Management acquisition jobs, use these areas of the Console:

- Use the Configuration tab, Infrastructure Management area to enter any necessary HTTP and FTP Proxy settings.
- Use the Configuration tab, Patch Management area, Acquisition Jobs task to defined the Acquisition Jobs.
- Use the Operations tab, Patch Management area, Start Acquisiton task to run the jobs.



HP recommends acquiring from only one vendor at a time. In addition, some SuSE Security Advisories and Microsoft Office Security Bulletins may take an extended period of time to download.

The acquisition job settings that are required depend on your environment.

To create or edit an acquisition profile using the Console

- 1 From Configuration, click **Patch Management**, then **Acquisition Jobs**.
- 2 Either select an existing file to edit, or click **New** to create a new file. Click the trashcan icon to delete an acquisition file. In this example, we click **New**.

New Acquisition File

Filename	Description
November.acq	November 2004

- 3 If you are creating a new file, type a Filename and Description, then click **Next**.
- 4 You will be taken to Step 2, where you can complete Acquisition Settings for the new job.

- **Acquisition File Description:** Create a description for the acquisition file.
- **Bulletins:** Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. For Red Hat Security advisories, use a hyphen (-) in place of the colon (:) that appears in the Red Hat Security advisory number as issued by Red Hat.
 - Microsoft Security bulletins use the naming convention `MSYY-###`, where `YY` is the last two digits of the year that the bulletin was issued and `###` is a sequential number of the bulletin number being released for this the year specified. Microsoft service pack patch descriptor files supplied by HP are supplied with the following naming convention: `MSSP_operatingsystem_spnumber`. To acquire *sample* Microsoft Operating System service packs, specify `MSSP*`. This will download sample service packs acquired from the `novadigm` or `custom` folders. To acquire Microsoft Advisories, specify the KB articles using the naming convention `MS-KB*`, where `*` represents the number assigned to the Knowledge Base Article.
 - Red Hat Security advisories are issued using the naming convention `RHSA-CCYY:###`, where `CC` indicates the century and `YY` the last two digits of the year when the advisory was issued, and `###` the Red Hat patch number. However, because the colon is a reserved character in products, you must use a hyphen (-) in place of the colon (:) that appears in the Red Hat-issued Security advisory number. Specify individual Red Hat Security advisories to Patch Manager using the modified naming convention of `RHSA-CCYY-###`.

- SuSE Security patches use the naming convention `SUSE-PATCH-####`, where `###` represents a numbering scheme provided by SuSE.

▶ If you do not want to download any bulletins, type **NONE** in the Bulletins field.

- **Mode:** Specify **BOTH** to download the patches and the information about the patches. Specify **MODEL** to acquire only the metadata for patches. Only the Bulletins and Numbers for the patches are downloaded, but not the actual patch files. Use this mode so that you can use the reports to expose vulnerabilities on managed devices.
- **Force:** Use force in the following situations.
 - You previously ran an acquisition using the mode **MODEL**, and now you want to use **BOTH**.
 - You previously ran an acquisition filtering for one language (`lang`), and now, you need to acquire bulletins for another.
 - You previously ran an acquisition specifying one product, and, now, you need to acquire for another.

For example, suppose that originally you had only Windows 2000 computers in your enterprise, so you used `-product {Windows 2000*}`. A month later, you roll out Windows XP. If you want to acquire the same bulletins, you will need to run the acquisition with `-product {Windows XP*,Windows 2000*}` and `-force y`.

▶ If `replace` is set to **Y**, the bulletins will be removed and reacquired, regardless of the value of `force`.

- **Replace:** Set `replace` to **Y** to delete old bulletins, specified in the `bulletins` parameter, and then re-acquire them. This will supersede the value for `force`. In other words, if you set `replace` to **Y**, then any bulletin specified for that acquisition will be deleted and reacquired, whether `force` is set to **N** or **Y**.
- **Command Line Overrides:** Use this parameter only when it is necessary to override your regular acquisition parameters. If used incorrectly, the acquisition will fail. Use the format of `-parameter value`.

Microsoft Settings

- **Acquire Microsoft Patches?:** Select **Yes** if you want to acquire Microsoft Patches. For additional settings, go to the Vendor Settings 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 314
- [Device Type Selection](#) on page 314
- [vPro System Defense Settings](#) on page 316

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.

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 315

- [vPro Devices](#) on page 315
- [Both](#) on page 315

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 316.

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 43 Configuration and Operations options

	DASH	vPro
Configuration	No additional options	vPro System Defense Settings
Operations	Device Management	Provisioning vPro Devices Group Management Alert Notification

- ▶ You must log out and log in again to the HPCA Console when you make or change your device type selection in order to see the device-type related options in the navigation panel on the Configuration and Operations tab.

vPro System Defense Settings

Before managing System Defense features on vPro devices and device groups you must define vPro System Defense Settings.

- ▶ This configuration option appears only if you have selected the vPro device type. System Defense settings do not apply to DASH devices.

- **Managing System Defense Filters**

For vPro devices, you can create, modify, and delete System Defense filters. System Defense filters monitor the packet flow on the network and can drop or limit the rate of the packets depending if the filter condition is matched. Filters are assigned to System Defense Policies that can be enabled to protect the network.

- **Managing System Defense Policies**
For vPro devices, you can create, modify, and delete System Defense policies and then deploy them to multiple vPro devices on the network. System Defense policies can selectively isolate the network to protect vPro devices from 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. For additional information on OS Management, refer to the *OS Manager Guide*.

- [Settings](#) on page 318

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. For additional information on OS Management, refer to the *OS Manager Guide*.

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

During OS deployment, if you are planning to boot devices across the network, you must first enable the Boot Server (PXE/TFTP) installed with the Core. This will start two Windows services on the Core server, Boot Server (PXE) and Boot Server (TFTP).

- To enable the Boot Server (PXE/TFTP) select the check box and click **Save**.

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 [Vulnerability Management](#) dashboard provides data pertaining to security vulnerabilities on the client devices in your enterprise.

The [Compliance Management](#) dashboard provides information about how well the managed client devices in your enterprise comply with regulatory standards, such as FDCC.

The [Security Tools Management](#) dashboard shows you information about the anti-spyware, anti-virus, and software firewall products installed on the managed client devices in your enterprise.

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 90


[Service Events](#) on page 92

The Executive View also includes the following pane:

[12 Month Service Events by Domain](#) on page 94

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 89.

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.

Vulnerability Management

The Vulnerability Management dashboard provides information about any publicly known security vulnerabilities that are detected on the managed client devices in your network.

The Vulnerability Management dashboard Executive View includes the following four information panes:

- [Vulnerability Impact by Severity \(pie chart\)](#) on page 97

- [Historical Vulnerability Assessment](#) on page 99
- [Vulnerability Impact by Severity \(bar chart\)](#) on page 107
- [Vulnerability Impact](#) on page 101

The Operational View includes the following four information panes:


- [HP Live Network Announcements](#) on page 106
- [Most Vulnerable Devices](#) on page 109
- [Most Vulnerable Subnets](#) on page 110
- [Top Vulnerabilities](#) on page 112

You can use the configuration settings to specify which panes appear in the dashboard. For detailed information about these panes, see [Vulnerability Management Dashboard](#) on page 96.



HP Live Network provides a vulnerability scanner and updated vulnerability content to HPCA. You must configure the Live Network settings before you can use the HPCA vulnerability management features.

To configure the [Vulnerability Management dashboard](#):

- 1 From the Configuration tab, click **Dashboards**.
- 2 Under Dashboards, click **Vulnerability Management**.
By default, this dashboard is enabled. To disable it, clear the **Enable Vulnerability Management Dashboard** box, and click **Save**.
- 3 Under Vulnerability Management, click either **Executive View** or **Operational View**.
- 4 Select the box for each pane that you want to show in the dashboard. Use the  icon to display information about any related HPCA configuration that is required for each pane.

The following panes require additional information:

- **Vulnerability Impact (Executive View)**
Specify the default age of vulnerabilities to display in the chart. For example, if you enter 90 days, only those vulnerabilities published during the last 90 days will be displayed in the chart. The default value is 45 days.

- **HP Live Network Announcements (Operational View)**
Enter the following information pertaining to your HP Live Network subscription:
 - a URL for the HP Live Network RSS notification feed
 - b Fully qualified host name for the HP Live Network authentication serverCurrently valid defaults are provided. You may also need to enable a proxy server using the **Console Settings** page.
- 5 Click **Save** to implement your changes.

Compliance Management

The Compliance Management dashboard provides information about how well the managed client devices in your network comply with various regulatory standards, such as the Federal Desktop Core Configuration (FDCC) standard.

The Compliance Management dashboard includes two views: the Executive View and the Operational View.

The Executive View includes the following information panes:

- [Compliance Summary by SCAP Benchmark](#) on page 118
- [Compliance Status](#) on page 116
- [Historical Compliance Assessment](#) on page 119

The Operational View includes the following information panes:

- [Top Failed SCAP Rules](#) on page 121
- [Top Devices by Failed SCAP Rules](#) on page 123


You can configure the dashboard to show or hide any of these panes. For detailed information about the panes, see the [Compliance Management Dashboard](#) on page 115.

You can also enable or disable the entire dashboard. If you disable the dashboard, the Compliance Management link will not appear in the left navigation menu on the Home tab.



HP Live Network provides a compliance scanner and updated compliance content to HPCA. You must configure the Live Network settings before you can use the HPCA compliance management features.

To configure the Compliance Management dashboard:

- 1 From the Configuration tab, click **Dashboards**.
- 2 Under Dashboards, click **Compliance Management**.
By default, this dashboard is enabled. To disable it, clear the **Enable Compliance Management** box, and click **Save**.
- 3 Under Compliance 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.
- 5 Click **Save** to implement your changes.

Security Tools Management

The [Security Tools Management Dashboard](#) shows you information about the anti-spyware, anti-virus, and software firewall products installed on the managed client devices in your enterprise.

The Security Tools Management dashboard has two views: the Executive View and the Operational View.

The Executive View includes the following information panes:

- [Security Product Status](#) on page 126
- [Security Product Summary](#) on page 128

The Operational View includes the following information panes:

- [Most Recent Definition Updates](#) on page 130
- [Most Recent Security Product Scans](#) on page 131


You can configure the dashboard to show or hide any of these panes. For detailed information about the panes, see the [Security Tools Management Dashboard](#) on page 125.

You can also enable or disable the entire dashboard. If you disable the dashboard, the Security Tools Management link will not appear in the left navigation menu on the Home tab.



HP Live Network provides a security tools scanner and related content to HPCA. You must configure the Live Network settings before you can use the HPCA security management features.

To configure the Security Tools Management dashboard:

- 1 From the Configuration tab, click **Dashboards**.
- 2 Under Dashboards, click **Security Tools Management**.
By default, this dashboard is enabled. To disable it, clear the **Enable Security Tools Management Dashboard** box, and click **Save**.
- 3 Under Security Tools Management, click **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 134
- [Device Compliance by Bulletin](#) on page 136

The Operational View includes three information panes:

- [Device Compliance by Status \(Operational View\)](#) on page 138
- [Microsoft Security Bulletins](#) on page 139
- [Most Vulnerable Products](#) on page 140

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 134.


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.

9 Patch Management Using Metadata

This release introduces a lightweight model for acquiring and delivering patch updates to your Agent devices. Because the model only uses Metadata to perform the patch scans on your agents, it is called Patch Management using Metadata.

The chapter discusses the concepts, configuration and implementation details needed to take advantage of Patch Management using Metadata.

Patch Management using Metadata is only available for:

- Microsoft operating systems using a Microsoft Update Catalog data feed
- HPCA Core and Satellite Enterprise-level environments

Topics include:

- [Overview](#) on page 325
- [Configuring Patch Management for Metadata Distribution \(Microsoft only\)](#) on page 329
- [Configuring the Patch Agents](#) on page 331
Note: Download Manager must be enabled for Metadata Distribution.
- [Entitling Agents to Patches](#) on page 335
- [Patch Acquisition and Gateway Operations](#) on page 336

Overview

The lightweight Patch Management using Metadata model is currently available for patching Microsoft devices and requires the use of a Microsoft Update Catalog feed.

It offers several advantages that are described below and illustrated in [Figure 46](#) on page 327.

The Metadata Patch Management model differs from the traditional HPCA patching model in that:

- 1 Only the bulletin Metadata information is stored in the Core server Configuration Server Database (CSDB), and not the actual patch binaries.

This model makes patch acquisition run faster and also eases the load on the infrastructure traffic when running the Patch Discovery on an Agent and when synchronizing the HPCA servers.

- 2 The actual patch binaries are downloaded and cached on the Patch Gateway, a component of the Core server. The Gateway downloads the patch binaries upon the first request from an agent machine and caches them for other agent machines to use. Optionally, the Patch Gateway can have patch binaries preloaded onto it when you run an acquisition.

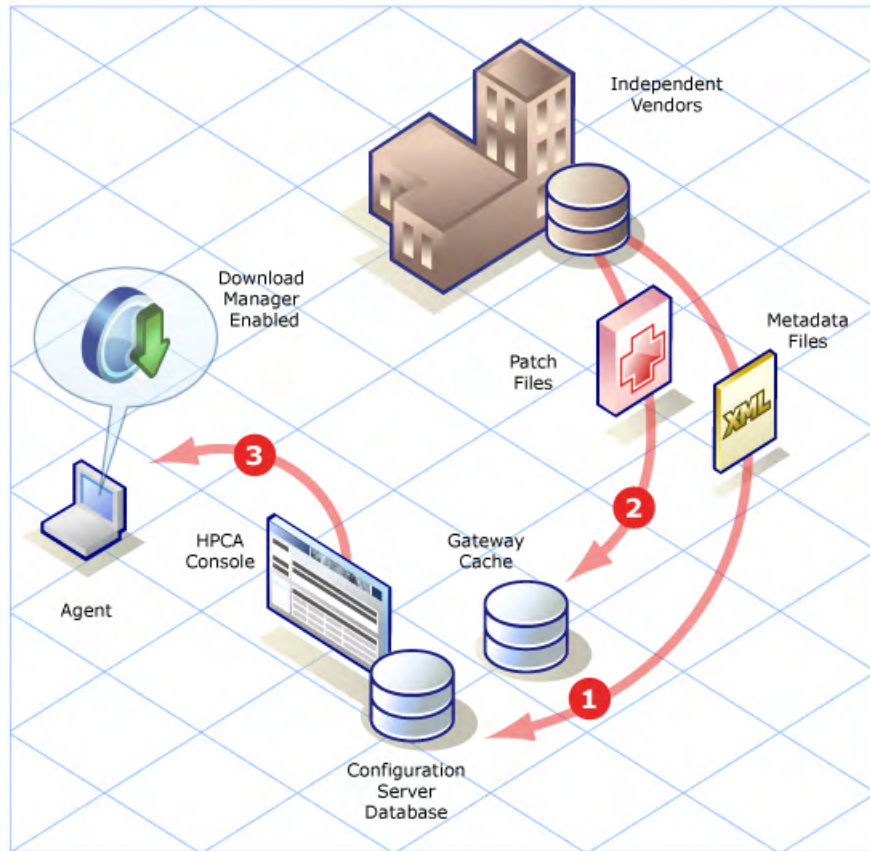
- 3 When using the Metadata model, the Agents must have the Download Manager enabled which allows them to contact the Patch Gateway at the end of the scanning phase with requests for applicable patch binaries.

The Download Manager handles the passive transfer of the patch files to the Agents. Once the file transfer is complete, an Agent connection is triggered to have the patches installed.

[Figure 46](#) on page 327 illustrates the Patch Management using Metadata model.

For comparison, [Figure 47](#) on page 328 illustrates the traditional Patch Management model.

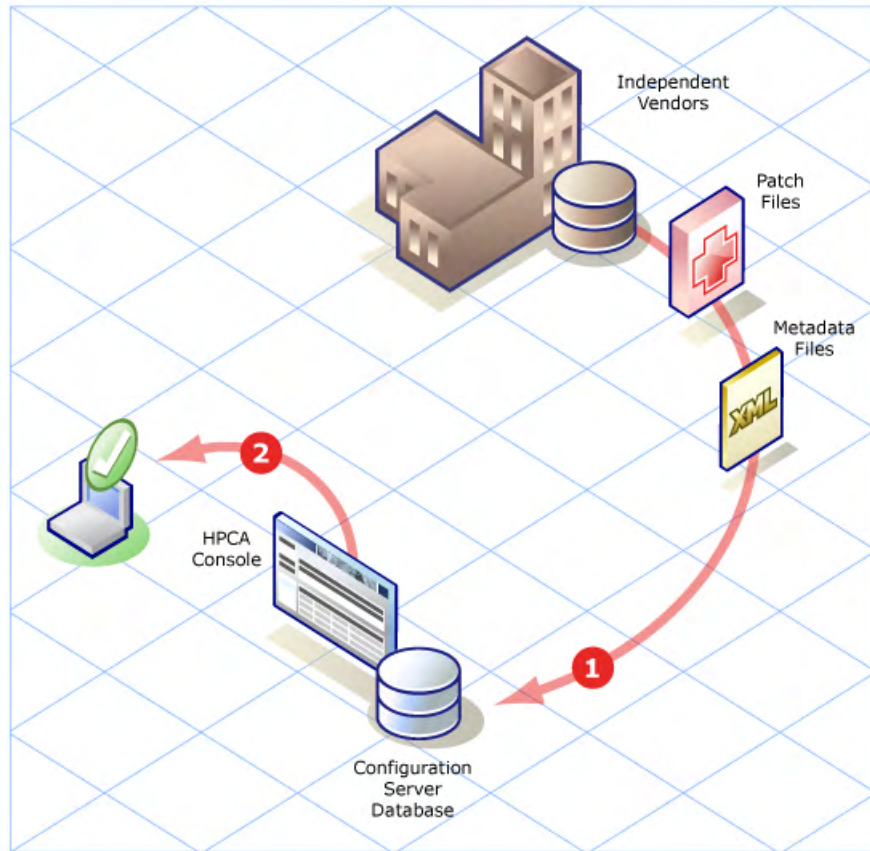
Figure 46 Patch Management using Metadata Model



Legend:

- 1 A Patch Acquisition downloads only patch metadata files from the Vendor. The patch metadata is published to the Core CSDB and used to discover the exact list of patch files required by the Agents being managed.
- 2 Upon request by an Agent (or optional preload), the Patch Gateway downloads the patch files from the Vendor and caches them for additional Agents to use. The patch files never need to be published to the CSDB.
- 3 Patch Agents require the Download Manager to be enabled. The Download Manager uses a background process to handle the passive download of the required patch files onto the Agent.

Figure 47 Patch Management Model - traditional



Legend:

- 1 A traditional Patch Acquisition downloads both metadata and all related patch files for bulletins from the Vendor. All of these files are published to the Core CSDB, regardless of whether Agents in the enterprise require them or not.
- 2 Patch Agents can be patched with or without the use of the Download Manager option. Without it, the Agent connect handles the download of the required patch files in a foreground process. In contrast, the Download Manager uses a background process to handle the passive download of the required patch files onto the Agent.

Related Topics:

The following topics discuss how to take advantage of using Metadata distribution and the Patch Gateway for Patch Management in your enterprise:

- [Configuring Patch Management for Metadata Distribution \(Microsoft only\)](#) on page 329
- [Agent Configuration for Gateway Access](#) on page 331
- [Agent Configuration for Offline Scanning](#) on page 332
- [Agent Configuration for Download Manager](#) on page 333
- [Patch Acquisition and Gateway Operations](#) on page 336

Configuring Patch Management for Metadata Distribution (Microsoft only)

- 1 Metadata distribution is not enabled by default. It is enabled from the Core console Configuration tab > Patch Management > Distribution Settings page. For this release, Metadata distribution is only available for Microsoft devices and requires a Microsoft Update Catalog (MUC) feed.
 - a From the Core Console, click the **Configuration** tab, open the **Patch Management** group and click **Distribution Settings**.

The Patch Distribution Settings page opens, with areas for Patch Metadata Download and Patch Gateway Operations.
 - b Use the **Patch Metadata Download** area to check the option:
Enable Download of Patch Metadata only.

Note: When you enable Metadata distribution Microsoft, Patch Manager switches to using the Vendor feed named **MSFT**, instead of **MICROSOFT**.
 - c Use the **Patch Gateway Operations** area to enable and configure the Patch Manager Gateway. The Gateway is a component of the Patch Manager Server that downloads and caches the patch binary data that are requested by the Agents.
 - d Specify the following:

Check **Enable Gateway**. This must be turned on for Metadata Distribution.

Enabling the Gateway displays additional fields to configure it.

Specify a **Maximum Cache Size** in megabytes. Leave this blank if the cache size is to be unlimited.

Specify the maximum **Time for which the Binary is valid** in hours:minutes;seconds (HH:MM:SS). If a requested binary is older than this when an Agent requests it, the Gateway will check to see if there's a later version before providing it.

Patch Gateway Operations

The Patch Gateway is a server where the binaries can be downloaded, cached and provided to the Agent machines.

Enable Gateway

Maximum Cache Size MB

Time for which the Binary is valid HH:MM:SS

Preload Gateway Cache

[Return to Top](#)

Optionally, set the **Gateway Preload** option to **Yes** to cache the patch binaries on the gateway when you run the acquisition; however, HP recommends using the preload gateway option with caution.

The advantage of preloading is that the first agent to request a specific patch binary does not have to wait for the Gateway to download it.

The disadvantage of preloading is that the Gateway downloads all the patch binaries related to an acquisition—*regardless of whether the agents need require them or not*. Leave the Preload Gateway option set to **No** to have the Gateway download and cache the patch binaries upon the first agent request (on-demand download).

- e Click **Save** to save your settings.
- 2 Use the Configuration tab, Patch Management area's **Acquisition Jobs** panels to define a job to acquire bulletins. This task is no different whether you are using Metadata Distribution or not.
- 3 The next task is to ensure your Core and Satellite servers are defined with Service Access Profiles, as discussed in [Configure Client Operations Profiles](#) on page 30.

For Patch Management using Metadata and the Gateway, use the HPCA Administrator CSDB Editor to verify the SAP entries normally created with a Type of DATA for the Core and Satellite servers all include the Role of P.

The P role passes Agent requests for patch binaries to the Patch Manager Gateway.

- ▶ If the SAP instances with TYPE of DATA do not include the role of P, make the change using the topic [Modify Service Access Profiles for Patch Distribution using the Gateway](#) on page 33.

This completes the Patch Configuration for Metadata Distribution on the server side.

Configuring the Patch Agents

The next step is to configure the Patch Agents to access the Patch Manager Gateway using Client Operation Profiles (COP) and enable the silent preload of patch binaries. These are discussed below.

Agent Configuration for Gateway Access

To access the Patch Manager Gateway servers, setup your Patch Manager Agents to use Client Operations Profiles (COP) and the appropriate Patch Manager Gateway enabled server.

- 1 First configure your Agents to use COP. COP can be configured in many ways, for example, per computer or per subnet. For more information on how to use COP, refer to the *HPCA Application Manager and Self-Service Manager User Guide* or the Client Domain chapter in the *HPCA Configuration Server Database Reference Guide*.
- 2 After configuring COP for the Agent machines, ensure that the SAP entries for data delivery (TYPE of DATA) include the Role of P and are associated with the appropriate PRIMARY.CLIENT.LOCATION instance.

In the sample configuration below, the SAP instance for delivering data is named PRIMARY.CLIENT.SAP.MAHWAH_PMG1 and is associated with a PRIMARY.CLIENT.LOCATION for a network subnet. Your configuration will likely differ.

ALWAYS_	Core Settings Class Connect...	SETTINGS.DEFAULT_SETTIN...
ALWAYS_	Diagnostics Class Connection	DIAGS.DEFAULT_DIAGS
ALWAYS_	UI Class Connection	
ALWAYS_	Hardware Class Connection	
ALWAYS_	Connect To Class	
ALWAYS_	Connect To Class	
SAPPRI	SAP Priority	10
ALWAYS_	Connect To	CLIENT.SAP.MAHWAH_PMG1
SAPPRI	SAP Priority	20
ALWAYS_	Connect To	
SAPPRI	SAP Priority	30

- 3 Modify the Agent connect parameters to include COP=Y. For details, see the *HPCA Application Manager and Application Self-Service Manager User Guide*.

This completes the setup for Metadata Distribution using MSFT feed and Patch Manager Gateway using COP.

Agent Configuration for Offline Scanning

When managing patches through the Metadata acquisition model, once the acquisition file for the MSFT Vendor is downloaded to the Agents, the scanning phase takes place without relying on any connection to the network or the HPCA Core or Satellite servers.

At the end of the scanning phase, the list of patch binaries required for each Agent to be in compliance is available.

The Agent starts the Download Manager, which will begin the preload of the binary files once a network connection is available.

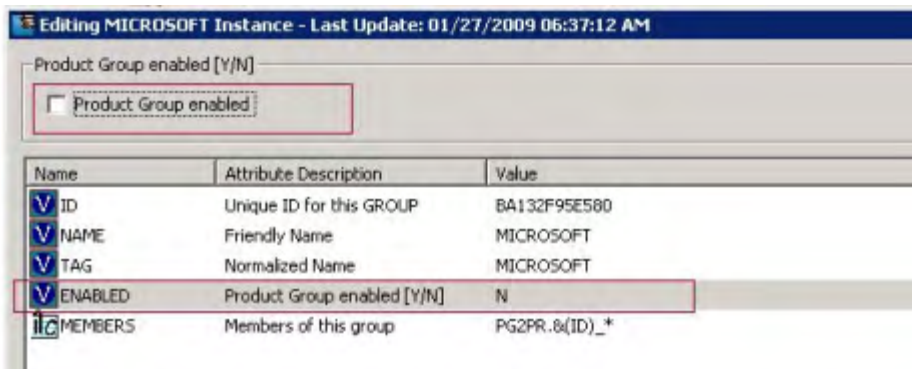
Offline Scanning Requirements

The patch offline scanning ability is built into the Agents as of Version 7.50 and is automatically enabled under the following conditions. Be sure to meet these conditions for offline scanning if you are using Patch Management using Metadata.

- Configure the Patch Management > Distribution Settings to have **Patch Metadata Download** enabled.
- Configure the Patch Management > Agent Options to have the **Download Manager** enabled. For details, see [Agent Configuration for Download Manager](#) on page 333.
- The Core's Configuration Server Database must have the following entry disabled:
 - The MICROSOFT instance in the PRIMARY.PATCHMGR.PROGROUP class must be disabled. This configuration is discussed below.

To disable the MICROSOFT instance in the PATCHMGR.PROGROUP Class

- 1 On the Core server, login to the HPCA Administrator CSDB Editor.
- 2 Navigate to the MICROSOFT instance of the PRIMARY.PATCHMGR.PROGROUP class.
- 3 Edit and remove the check mark to set the Product Group Enabled attribute to N, as shown in the following figure:



Make sure this Enabled attribute is set to N in order to allow Offline Scanning to take place on the Agents.

Agent Configuration for Download Manager

With Metadata distribution, the Agents request a set of binary files to be downloaded from the Patch Gateway at the end of the scanning phase.

The Patch Agents must be configured to use the Download Manager. This works silently in the background to bring down the patch files to the Agents as an asynchronous process. The Download Manager allows this passive file transfer to stop and start, as needed, but continues the download from where it left off.

When enabled, the Download Manager for Patch Agents allows you to set several options to control how the binaries are downloaded to the Agents. The Download Manager options include network utilization in normal mode and in screen saver mode, delay after initialization, and apply patch updates after download completion.

The Download Manager option is not enabled by default. To enable it, use the Console **Configuration** tab > **Patch Management** Area > **Agent Options** page. Details are given below.

When you enable the Download Manager and save the options on the Console, the Patch Manager DISCOVER instances in the CSDB Database are modified to reflect your selections.

To enable the Patch Agents to use the Download Manager

Use the Console Configuration tab > Patch Management area > Agent Options page to enable the Download Manager and set related options.



The Download Manager must be enabled in order to patch Microsoft devices when using Patch Metadata Distribution.

- 1 From the Console **Configuration** tab, click **Patch Management** and **Agent Options**.
- 2 On the Agent Options page, go to the Download Manager Options area.
- 3 Check the box for **Enable Download Manager**.

When checked, the Download Manager options are displayed.

- 4 Set the Download Manager options. Set specific options for network utilization, network utilization in Screen Saver Mode, delay after initialization, and whether or not to apply the patches after download completion.

For details on setting these options, see [Agent Options](#) on page 291.

Example: The following entries enable the Download Manager for Patch Agents with up to 34% Network Utilization during device activity, up to a 45% Network Utilization in Screen Saver Mode, and a 45-minute delay after initialization. After the patch files are downloaded, they will be available to be applied during the next Patch Agent connect

Download Manager Options

Enable Download Manager to transfer the files required to apply patches onto the managed devices in the background, outside of the usual HPCA Agent connect process. This option allows for bandwidth throttling and an automatic stop and start of the download until it completes.

<input checked="" type="checkbox"/> Enable Download Manager	
<input type="text" value="34"/> Network Utilization	%
<input type="text" value="45"/> Network Utilization in Screensaver Mode	%
<input type="text" value="45"/> Delay initialization	Minutes
<input type="text" value="No"/> Apply patches after download completion	

- optionally, use the Agent Options area to set additional Agent Options:
 - Disable Automatic Updates
 - Delete Software Distribution Folder

For details on setting these options, see [Agent Options](#) on page 291.

Note: Saving the Patch Agent options modifies the Patch Manager DISCOVER instance for all methods in the Configuration Server Database (Create, Delete, Verify, Update and Repair).

- Click **Save** to save your changes.

Entitling Agents to Patches

Entitle the Agents to the appropriate patches using the standard patch deployment procedures. For more information, refer to the Management chapter topics.

The Patch Agent downloads the applicable binaries through the patch Gateway, utilizing the Download Manager's background process for asynchronous transfer of the applicable patch files.



The Patch Agents will not receive patch binaries unless the Agents have been entitling to those services.

As the Gateway obtains requested patch files, it caches them for other Agents to use.

Patch Acquisition and Gateway Operations

Patch Acquisition using Metadata takes minutes as opposed to hours, on average, because it is lightweight—meaning only the patch information is downloaded and published to the CSDB.

- 1 Use the Operations tab, Patch Management area to run an Acquisition.

From the Console, click the Operations tab and go the Patch Management group. Select **Start Acquisition**.

After acquisition, the CSDB only contains the patch metadata information and not the actual patch binary data.

- 2 Optionally, you can view the status of an acquisition.

From the Console, click the Operations tab. Expand the Patch Management group and click **Report Acquisition Status**.

- 3 Entitle the Agents to the appropriate patches using the standard patch deployment procedures.

The Patch Agent downloads the applicable binaries through the patch Gateway. The Gateway then caches the binary for other clients to use.

- 4 Once the files are downloaded and cached on the Gateway, the available patch URLs are listed on the Cache File Statistics page

To access this page from the Console, click Operations and select Patch Manager, Gateway Operations, and **Cache File Statistics**.

10 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.

For Windows operating system images, see the following sections:

- [Preparing and Capturing Images](#) on page 338
- [Using Microsoft Sysprep](#) on page 355
- [About the Image Preparation Wizard](#) on page 358

For Thin Client operating systems, see:

- [Preparing and Capturing Thin Client Images](#) on page 367

Preparing and Capturing Images

The OS image preparation and capture steps will vary based on the operating system and deployment method.

For instructions on preparing and capturing thin client images, see [Preparing and Capturing Thin Client Images](#) on page 367.



If you are planning to use supported Disk Encryption products the image must be captured from an unencrypted partition.

- [Capturing pre-Windows Vista for Legacy Deployment](#) on page 338
- [Capturing pre-Windows Vista for ImageX Deployment](#) on page 340
- [Capturing Windows Vista for ImageX Deployment](#) on page 342
- [Capturing Windows Server 2008 for ImageX Deployment](#) on page 344
- [Capturing pre-Windows Vista for Windows Setup Deployment](#) on page 345
- [Capturing Windows Vista for Windows Setup Deployment](#) on page 352
- [Capturing Windows Server 2008 for Windows Setup Deployment](#) on page 353

Capturing pre-Windows Vista for Legacy Deployment

The following steps describe how to prepare and capture a pre-Windows Vista operating system image for Legacy Deployment.

- [Task 1: Prepare the Reference Machine](#) on page 339
- [Task 2: Prerequisites](#) on page 340
- [Task 3: Run The Image Preparation Wizard](#) on page 340

Task 1: Prepare the Reference Machine

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



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

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

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

- 3 Install the HPCA agent from the HPCA media. The Agent is required so that when the OS image is deployed, the device can connect to the HPCA Server.
- 4 Configure the BIOS power management so that the device does not power down after a few minutes of keyboard or mouse inactivity before the upload process to the HPCA Server is finished.
- 5 Keep the image file size as small as possible. The ideal configuration is a partition just large enough to fit the operating system, plus additional space for the HPCA agent.



HP supports deploying the image to the primary boot partition of the primary boot drive.

The following steps help to minimize the size of the image file:

- a Create free space.

HP recommends that after you have created the smallest partition with the least amount of free disk space as possible, set the `ExtendOemPartition = 1` in the [Unattended] section of `Sysprep.inf`, to allow for the small image to be installed on a target device with a much larger drive. When the `ExtendOemPartition` is set to true, the Microsoft Mini-Setup Wizard will extend the OS installation partition into any available non-partitioned space that physically follows on the disk. The HPCA agent can then use the free space on the volume for application installations.

- b Disable hibernation if you are using a laptop.

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

Task 2: Prerequisites

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



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

- 2 Set up Microsoft Sysprep.
- 3 Create a Sysprep.inf.

See [Using Microsoft Sysprep](#) on page 355 for details.

Task 3: Run The Image Preparation Wizard

See [About the Image Preparation Wizard](#) on page 358.

Capturing pre-Windows Vista for ImageX Deployment

The following steps describe the process for preparing and capturing pre-Windows Vista operating systems for ImageX deployment.

- [Task 1: Copy utilities to the HPCA Server](#) on page 341
- [Task 2: Prepare the Reference Machine](#) on page 341
- [Task 3: Prerequisites](#) on page 342
- [Task 4: Run The Image Preparation Wizard](#) on page 342

Task 1: Copy utilities to the HPCA Server

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

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

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

Task 2: Prepare the Reference Machine

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



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

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

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



HP supports deploying the image to the primary boot partition of the primary boot drive.

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

Task 3: Prerequisites

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



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

- 2 Set up Microsoft Sysprep.
- 3 Create a Sysprep.inf.

See [Using Microsoft Sysprep](#) on page 355 for details.

Task 4: Run The Image Preparation Wizard

See [About the Image Preparation Wizard](#) on page 358.

Capturing Windows Vista for ImageX Deployment

The following steps describe the process for preparing and capturing Windows Vista operating systems for ImageX deployment.

- [Task 1: Copy utilities to the HPCA Server](#) on page 342
- [Task 2: Prepare the Reference Machine](#) on page 343
- [Task 3: Prepare unattend.xml](#) on page 343
- [Task 4: Run The Image Preparation Wizard](#) on page 344

Task 1: Copy utilities to the HPCA Server

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

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

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

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

Task 2: Prepare the Reference Machine

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



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

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

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



HP supports deploying the image to the primary boot partition of the primary boot drive.

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

Task 3: Prepare unattend.xml

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

Task 4: Run The Image Preparation Wizard

See [About the Image Preparation Wizard](#) on page 358.

Capturing Windows Server 2008 for ImageX Deployment

The following steps describe the process for preparing and capturing Windows Server 2008 operating systems for ImageX deployment.

- [Task 1: Copy utilities to the HPCA Server](#) on page 344
- [Task 2: Prepare the Reference Machine](#) on page 344
- [Task 3: Prepare unattend.xml](#) on page 345
- [Task 4: Run The Image Preparation Wizard](#) on page 345

Task 1: Copy utilities to the HPCA Server

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

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

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

Task 2: Prepare the Reference Machine

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



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

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

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

▶ HP supports deploying the image to the primary boot partition of the primary boot drive.

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

Task 3: Prepare unattend.xml

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

Task 4: Run The Image Preparation Wizard

See [About the Image Preparation Wizard](#) on page 358.

Capturing pre-Windows Vista for Windows Setup Deployment

▶ Capture and Deploy of pre-Windows Vista images for Windows Setup Deployment is not supported for HPCA Starter and Standard.

This is the only case in which you will use the HPCA Windows Native Install Packager to prepare an image. The image is of the installation media for a pre-Windows Vista operating system on a hard drive on the reference machine. The resulting image has completed the file copy phase of a Windows installation and contains the HPCA agent. The image is sent to the HPCA servers's \upload directory and then you will use the Admin Publisher to publish the image to the Configuration Server DB.


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

- [Task 1: Prepare the Reference Machine](#) on page 346
- [Task 2: Create Unattend.txt](#) on page 347
- [Task 3: Install the HPCA Windows Native Install Package](#) on page 348
- [Task 4: Run the HPCA Windows Native Install Package](#) on page 349


Task 1: Prepare the Reference Machine

The image of the original installation media created on the reference machine is deployed to target devices. Before using the HPCA Windows Native Install Packager to create the image, ensure that you have the HPCA media and that the reference machine meets the following requirements:

- 1 Connectivity to an HPCA Server.
- 2 A target drive, recommended being on an extended partition, that:
 - Will be used as if the target drive is currently formatted and empty (has no data). If the target drive is not formatted or it is formatted and contains data, the user will be prompted to format the drive.
 - A user can pre-format the drive with FAT32 if they format the drive and ensure that there is no data on the drive.

 Note that FAT32 cannot be expanded after deployed. NTFS can be expanded and is the default.


 - Is at least 1.5 GB. If the target drive is larger, it will take more processing time when the drive is imaged or the image may be larger than necessary depending on how the "Optimize Compression of Unused Disk Space" check box is set in the Image Preparation Wizard.

 All data on the target drive will be lost.
- 3 A separate drive (to increase speed), such as the C: drive, with the HPCA Windows Native Install Packager software already installed. See [Task 3: Install the HPCA Windows Native Install Package](#) on page 348.

- 4 You must also have access to the following items; specify their location when using the HPCA Windows Native Install Packager:

- The setup files for the HPCA agent.
- The i386 directory from your operating system media.

You can slipstream any necessary service packs into this directory. See the readme.txt file associated with each service pack for more information about how to do this.

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


- If your device is running Windows XP, you cannot use the i386 directory for Windows 2000.
- If your device is running Windows 2003, you cannot use the i386 directory for Windows 2000 or Windows XP.

- unattend.txt

You can create the file manually or use Windows Setup Manager on your Windows media. Sample files are available on the Image Capture media in the samples directory.

Task 2: Create Unattend.txt

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

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

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

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

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

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

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

- You can also create separate `unattend.txt` files for any necessary customizations. You can use the Publisher to publish these files to the SYSPREP class in the HPCA DB and then you can connect them to the appropriate OS image. When the image is deployed, the customized `unattend.txt` will be merged with the original file.

▶ See the Publishing chapter for details about publishing files. When publishing `unattend.txt`, follow the instructions as if you were publishing a `Sysprep.inf` file.

Task 3: Install the HPCA Windows Native Install Package

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

Task 4: Run the HPCA Windows Native Install Package

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

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

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



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

- 2 In the Client Automation Client Source Directory field, enter the path for the HPCA agent.
- 3 Select the check boxes for the Client Automation products that you want installed.
- 4 Select the Run first connect after install check box to perform an HPCA OS connect after the OS is installed. If this is not selected, the HPCA OS connect will not occur automatically after the OS is installed.
- 5 In the Optional Packager Command Line Arguments box, type parameters used by the WNI application. The options can be placed all on one line or on several lines. Specify the options in the keyword-value format, such as
`-trace_level 9`

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

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

There are many parameters that can be used to create logs. The following example describes how to create a file called C:\temp\nvdwni.log.

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

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

- "-trace_file filename.log

6 Click **Next**.

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

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

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

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

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

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




All existing data found on this drive will be lost.

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



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

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

- 19 When the HPCA Windows Native Install Packager is done, a message prompts you to reboot using the Linux CD-ROM. This refers to the Image Capture media.
 -  Remember the boot order must be set to boot from the CD-ROM first.
- 20 Insert the Image Capture media, and then click **OK**.
- 21 Click **Finish**.
- 22 Reboot the device and the image is uploaded the \upload directory.
- 23 When a message appears that the OS Image has been successfully sent to the HPCA Server, you can remove the media from the drive and reboot your device.

Capturing Windows Vista for Windows Setup Deployment

The following steps describe the process for preparing and capturing Windows Vista operating systems for Windows Setup deployment.

- [Task 1: Copy utilities to the HPCA Server](#) on page 352
- [Task 2: Prepare the Reference Machine](#) on page 353
- [Task 3: Run The Image Preparation Wizard](#) on page 353

Task 1: Copy utilities to the HPCA Server

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

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

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

Task 2: Prepare the Reference Machine

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



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

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

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



HP supports deploying the image to the primary boot partition of the primary boot drive.

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

Task 3: Run The Image Preparation Wizard

See [About the Image Preparation Wizard](#) on page 358.

Capturing Windows Server 2008 for Windows Setup Deployment

The following steps describe the process for preparing and capturing Windows Server 2008 operating systems for Windows Setup deployment.

- [Task 1: Copy utilities to the HPCA Server](#) on page 354
- [Task 2: Prepare the Reference Machine](#) on page 354
- [Task 3: Run The Image Preparation Wizard](#) on page 355

Task 1: Copy utilities to the HPCA Server

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

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

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

Task 2: Prepare the Reference Machine

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



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

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

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



HP supports deploying the image to the primary boot partition of the primary boot drive.

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

- 4 If you are going to run the Image Preparation Wizard from the Image Capture media, set the boot order to CD-ROM first. If you are going to run the Image Preparation Wizard from another location, set the boot order to network first.

Task 3: Run The Image Preparation Wizard

See [About the Image Preparation Wizard](#) on page 358.

Using Microsoft Sysprep

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

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

To set up Sysprep

- 1 Go to DEPLOY.CAB in the SUPPORT\TOOLS folder of the Microsoft operating system installation media. See Microsoft's documentation for details.

- 2 Extract the Microsoft Sysprep files from the Deploy.cab file using the appropriate operating system media. Copy these files to C:\SysPrep on the reference machine and make sure the directory and files are not set to read-only.



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

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

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

You must be an administrator to run this application.

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

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

To create Sysprep.inf

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



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

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



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

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

- Adjust the TimeZone value for your enterprise.

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

How Sysprep.inf files are prioritized

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

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

- 1 Sysprep embedded in the image (lowest priority). If there is no separately published Sysprep.inf (override Sysprep), just the Sysprep.inf in the image will be used.
- 2 Override Sysprep (a Sysprep file that is separate from the gold image).
 - ▶ Only one override Sysprep.inf will be resolved.
- 3 Sysprep attached to policy criteria (highest priority).

About the Image Preparation Wizard

The Image Preparation Wizard performs the following tasks:

- 1 Creates an object that contains information (including hardware and OS information capabilities) about the reference machine.
- 2 (Optional Exit Points, not available for Legacy images) Executes the exit points that are available for your use as needed. PRE.CMD is executed before the Image Preparation Wizard starts SysPrep to seal the image. POST.CMD is executed after Sysprep has sealed the image. See [Using the Image Preparation Wizard Exit Points](#) on page 359 for details.
- 3 Runs Microsoft Sysprep on supported operating systems.
- 4 Restarts the reference machine into the Service OS (booted from the appropriate media). The Service OS runs to collect the image and its associated files.
- 5 Creates and copies files to SystemDrive:\Program Files\
SystemDrive:\Program
Files\Hewlett-Packard\HPCA\OSManagerServer\upload on the HPCA
Server.

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

— ImageName.IMG

This file contains the gold image. This is a compressed, sector-by-sector copy of the boot partition from the hard drive system that may be very large. The file contains an embedded file system that will be accessible when the image is installed.

— ImageName.MBR

This file contains the master boot record file from the reference machine.

— ImageName.PAR

The file contains the partition table file from the reference machine.

— ImageName.EDM

This file contains the object containing inventory information.

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

- ImageName.WIM

This file contains a set of files and file system information from the reference machine.

- ImageName.EDM

This file contains the object containing inventory information.

Using the Image Preparation Wizard Exit Points

You can use exit points for the Image Preparation Wizard as needed. For example, you may use them to clean up a device before performing a capture.

▶ This is not supported for Legacy images.

To use the exit points:

- 1 Create the files PRE.CMD and POST.CMD.
- 2 Save these files and any supporting files in OSM\PREPWIZ\payload\default\pre and OSM\PREPWIZ\payload\default\post respectively.

The Image Preparation Wizard copies these files to %temp%\prep wiz\pre and %temp%\prep wiz\post on the reference device and removes them before the capture begins. PRE.CMD is executed before the Image Preparation Wizard starts SysPrep to seal the image. POST.CMD is executed after Sysprep has sealed the image.

Preparing To Capture Remote Images

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

▶ Currently supported for Microsoft ImageX only.

To capture remote images

- 1 Connect to the remote machine to be captured.
- 2 Copy \image_preparation_wizard from the ImageCapture media to a network share.

- 3 Map a drive from the remote machine to be imaged to the network share that has `\image_preparation_wizard`.
- 4 Prepare the remote machine as necessary. See the following for information on how to prepare the machine.
 - [Capturing pre-Windows Vista for ImageX Deployment](#) on page 340
 - [Capturing Windows Vista for ImageX Deployment](#) on page 342
 - [Capturing Windows Server 2008 for ImageX Deployment](#) on page 344

Using the Image Preparation Wizard

- ▶ If you are capturing an image locally, before continuing, set the reference machine to boot from the CD-ROM drive. You must do this because the ImageCapture media is bootable. When you run the ImageCapture media, it reboots the device in order to upload the image.

When capturing a remote image, the CD-ROM is not required. See [Preparing To Capture Remote Images](#) on page 359.

To use the Image Preparation Wizard

- 1 Insert the Image Capture media into the reference machine.
- 2 Go to the `image_preparation_wizard` directory and double-click `prep wiz.exe`.
 - ▶ If you are using a legacy operating system and the agent is not installed, you will see the following message.

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

If you want the device to be managed, you must install the agent before running the Image Preparation Wizard.
 - If you are capturing an image to be deployed using the Legacy method, the Image Preparation Wizard verifies that the `C:\Sysprep` folder exists and that HPCA agent is installed before continuing.

- If you are capturing an image to be deployed using ImageX or Windows Setup, the Image Preparation Wizard will locate Sysprep in C:\Windows\system32\sysprep for Windows Vista or C:\sysprep for pre-Windows Vista operating systems.



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

3 Click **Next**.

The End User License Agreement window opens.

4 Click **Accept**.

The deployment methods that may appear are:

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

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

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.

6 Click **Next**.

7 Type a name for the image file. This is the image name that will be stored in the /upload directory.

8 Click **Next**.

The Span Disk Image window opens.

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

Use spanned images to break the image file into smaller segments. Each segment of a spanned image is restricted to 4 GB. This is helpful so that you can comply with the restriction of whole images needing to be less

than 4 GB so that they can be stored in the Configuration Server. If you choose not to use the spanned image option (by typing 0) your images must be less than 4 GB.

10 Click **Next**.

If appropriate, the Additional Sysprep Options window opens.

The text box is pre-filled with a command that clears all the SIDs to prepare the machine for capture.

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

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

12 Review Microsoft's documentation for information about additional Sysprep options.

13 Click **Next**.

If you chose ImageX for the deployment method, the Select Image Preparation Wizard payload window opens with the default option selected.

▶ The payload contains Local Service Boot (LSB) data to be delivered to target devices.

14 Type a description for the image file and click **Next**.

The Select the Windows Edition window may open.

15 Select the Windows edition that you are capturing and click **Next**.

The Options window may open.


▶ If you do not have the HPCA agent installed, you will not see the Perform client connect after OS install check box. However, please remember that it is important to have this agent installed if you are using the Legacy method to capture an image.

16 Select the appropriate options.

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

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

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

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

— **Optimize compression of unused disk space**

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

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

— **Resize partition before OS upload**

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

— **Perform client connect after OS install**

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

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

17 Click **Next**.

The Summary window opens.

18 Click **Start**.

19 Click **Finish**.

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

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



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

- 21 Click **Next**.

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

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

- 23 Click **Finish** to run Sysprep.

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



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

```
sysprep.exe -reseal -reboot
```

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

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



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

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

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

The Image Preparation Wizard connects to the network and stores the image on the HPCA Server in the upload directory.

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

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

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

Next, you will want to publish your image to the HPCA database. Refer to the Publishing information in the HPCA Documentation.

Using the Image Preparation Wizard in Unattended Mode

You may use a configuration file to run the Image Preparation Wizard in unattended mode.

To use the Image Preparation Wizard in Unattended Mode

- 1 Insert the ImageCapture media into the reference machine.
- 2 Go to \samples\prep wiz_unattend and copy setup.cfg to your local machine or a network location.
- 3 Make the necessary modifications. Below are the values that you may need to change.

Table 44 Variables in setup.cfg

Name	Description	Sample Value
RISHOSTPORT	The HPCA Server's IP address	<i>xxx.xxx.x.x:port</i>
IMAGENAME	Prefix used to create the uploaded files. This is appended to .WIM to create the name of the uploaded image.	Vista
IMAGEDESC	Description of the image that is published to the database.	"Windows Vista Unattended Test Image"
PREPWIZPAYLOAD	Payload the administrator wants to use. Contains the LSB data to be delivered to target devices.	Use the default value: "/OSM/PREPWIZ/payload/default"
OSEDITION	Specifies the edition of Vista used.	"Enterprise"
set ::setup(DEPLOYOS,SELECTED)	Set to 1 or 0 to indicate whether or not you want to redeploy the OS after the image capture.	"0"
se ::setup(ClientConnect,SELECTED)	Set to 1 or 0 to indicate whether or not to target the device to perform an OS connect after the image is deployed.	"1"

- 4 On the reference machine, open a command window and change to the CD/DVD directory. Go to Image_Preparation_Wizard\win32. Then, run the following command:

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

The Image Preparation Wizard starts Sysprep; this can take 15-20 minutes to complete. Sysprep reboots the device when complete, connects to the network and stores the image in the upload directory on the HPCA Server.

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 367
- [Windows CE OS Images](#) on page 371
- [Embedded Linux OS Images](#) on page 373

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 367
- [Task 2 – Run the Image Preparation Wizard](#) on page 368



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\fa`
- 4 Install the HPCA agent. Enterprise license users should refer to the *HPCA Application and Application Self-service Manager Guide* for thin client Agent installation 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 **prep wiz.exe**. The Image Preparation Wizard verifies that etprep.exe and fbreseal.exe are available before continuing. The Welcome window opens.
- 5 Click **Next**. The End User Licensing Agreement window opens.
- 6 Click **Accept**.
- 7 Type the IP address or host name and port for the 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 367.



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 371
- [Task 2 - Run the Image Preparation Wizard](#) on page 371

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. Enterprise license users should refer to the *HPCA Application and Application Self-service Manager Guide* for thin client Agent installation 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 **prep wiz.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 371.

 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 374
- [Task 2 - Run the Image Preparation Wizard](#) on page 374

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. Enterprise license users should refer to the *HPCA Application and Application Self-service Manager Guide* for thin client Agent installation 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 374.



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.

11 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 45](#) on page 380 shows which publishing options are available for each of the three license levels.

Table 45 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. If you select a thin client publishing option, follow the instructions in the appropriate section below.

- [Publishing Software](#) on page 381
- [Publishing Operating System Images](#) on page 385
- [Publishing OS Add-ons/extra POS Drivers](#) on page 390
- [Publishing BIOS Settings](#) on page 392

Publishing Software

Depending on the type of software you intend to publish, you will use one of two publishing options. At the login screen, you are given the choice of Windows Installer to publish Windows Installer files (.msi) or Component Select to use when publishing non-Windows Installer files. The following sections explain the steps for publishing each file type.

- [Publishing Windows Installer Files](#) on page 381
- [Publishing Using Component Select](#) on page 383

Publishing Windows Installer Files

Windows Installer uses MSI files to distribute software services to your operating system. The Publisher uses the files to create a service that is then published to HPCA. When the software service is contained in HPCA, it is ready for distribution to managed devices in your environment.

To publish Windows Installer files

- 1 Start the Publisher (see, [To start the Publisher](#) on page 379).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.
 - ▶ Log in to the Publisher using the HPCA user name and password. By default, the user name is **admin** and the password is **secret**.
- 3 In the Publishing Options area, select **Windows Installer** and click **OK**.
- 4 Navigate to the Windows Installer file in the left pane. The right pane displays any information that is available for the MSI file you select.
- 5 Click **Next**.
- 6 Review the available Publishing Options.
 - **Management Options**
To create an administrative installation point (AIP) select **Use setup** or **Use msiexec..**
 - ▶ The AIP path is a temporary location and will be removed after the publishing session completes.

- **Transforms**
Select and reorder the application of any transform files associated with the Windows Installer file.
- **Additional Files**
Include additional files as part of the AIP.
 - Click **Select all** to select all available files listed.
 - Click **Select none** to deselect all files.
- **Properties**
View and modify the msi file properties. Some Windows Installer files may require additional command line parameters to deploy correctly. For example, an application may require a custom property to pass a serial number during installation. Use the Properties dialog to include any additional parameters.
 - Click **Add** to add a new property.
 - Click **Remove** to delete an existing property.
 - To modify a property **Name** or **Value**, click the item you want to change and enter the new value.

When you are finished editing your publishing options, click **Next**.

- 7 Use the **Application Information** section to enter the software service information.
 - 8 Use the **Limit package to systems with** section to limit the service to any specific operating system or hardware. Click any link to display the configurable options.
 - 9 Click **Next**.
 - 10 Review the **Summary** section to verify the service information you provided during the previous steps. When you are satisfied, click **Publish**.
 - 11 Click **Finish** when the publishing process is finished to close the Publisher.
- The Windows Installer service is now ready for distribution to your enterprise.

To apply additional parameters using a transform file

- 1 Create the transform using Orca or another MSI editor. Be sure to save the transform in the same directory as the Window Installer file are publishing.

- 2 Start a Windows Installer publishing session. Follow the instructions above for details.
- 3 At the Edit step, click **Transforms**.
- 4 Select the available transform file and continue with the publishing session.

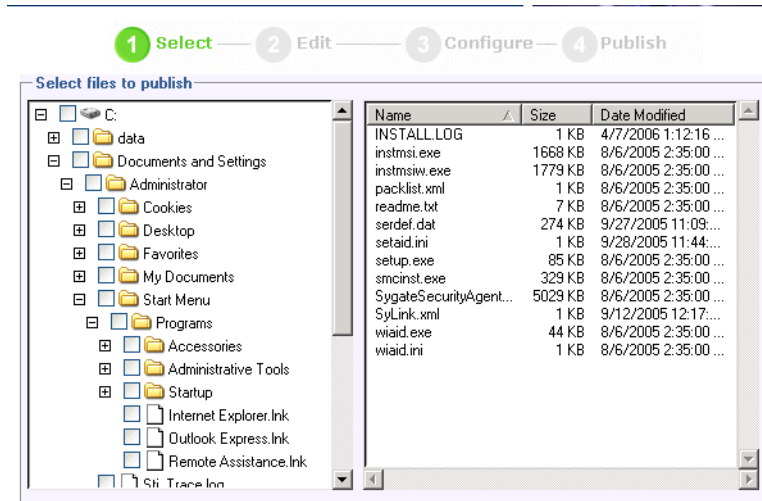
When the software service is deployed, the transform file will be applied, supplying the additional command line parameters.

Publishing Using Component Select

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

To publish using Component Select

- 1 Start the Publisher (see [To start the Publisher](#) on page 379).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.
 - ▶ Log in to the Publisher using the HPCA user name and password. By default, the user name is **admin** and the password is **secret**.
- 3 In the Publishing Options area:
 - If you are publishing for thin clients, select **Thin Client Publishing**.
 - From the drop-down list, select **Component Select**.
- 4 Click **OK**. The Select files to publish window opens.

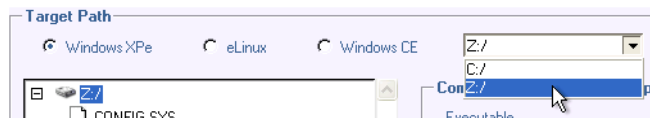


5 Select the files to publish and click **Next**.

- ▶ The directory path where the software is located (and published from) will be the directory path to where the software is deployed on target devices.
- ▶ Although network shares are displayed, they should not be used to publish software (since they may not be available during deployment).


The Target Path window opens.

6 If you are publishing for thin clients, select the install point, as shown in the following figure.



7 Enter the commands to run on application install and uninstall. For example, a command to run on install might be: `C:\temp\installs\install.exe /quietmode /automatic c:\mydestination`

A command to run on uninstall could be: `C:\temp\installs
\uninstall.exe /quietmode /automatic`

 You can right-click any file to set it as the install or uninstall command.

- 8 Click **Next**. The Application Information window opens.
- 9 Use the Application Information section to enter the software service information.
- 10 Use the **Limit package to systems with** section to limit the service to any specific operating system or hardware. Click any link to display the configurable options.
- 11 Click **Next**.
- 12 Review the Summary section to verify the service information you provided during the previous steps. When you are finished, click **Publish**.
- 13 Click **Finish** when the publishing process is finished to exit the Publisher.

The software service is now ready for distribution to your enterprise.

Publishing Operating System Images

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

- If you will be publishing `.WIM` images, see [Prerequisites for publishing .WIM images of a Vista OS](#) on page 385.
- See [Publishing OS Images](#) on page 388 for a description of the steps required to use the Publisher to publish OS images.

Prerequisites for publishing `.WIM` images of a Vista OS

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

- Have access to the `Media\client\default` folder on the HPCA media. This folder is only required the first time you publish a `.WIM` file or if you want to publish an updated agent package. The HPCA Agent will be published as a separate package, which ensures that all future deployments of your `.WIM` files will automatically receive the latest agent available.
- Have WAIK installed (WAIK is available from the Microsoft web site. It is not included as part of a normal Vista installation).
- Copy `filename.wim` and `filename.edm` from the HPCA Server's `\upload` directory (`C:\Program Files\Hewlett-Packard\HPCA\OSManagerServer\upload`, by default) to the device where you are publishing the image.
- Copy `substitutes` and `unattend.xml` to the same directory as `filename.wim`. Samples of these files are available on the Image Capture media in `\samples`. If you choose to use the samples, modify information as needed such as the setting the time zone and entering the product key. See the instructions below for more information. Note that all of these files must have the same prefix. For example, `install.wim`, `install.subs`, and `install.xml`.



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

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

`Filename.subs` and `filename.xml` are used to customize information. During deployment of the operating system, `filename.subs` and `filename.xml` will be combined to create an `unattend.xml` file that is used to provide information during all phases of the Windows setup on the target device.

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



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

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

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

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



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

Example of Substitution

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



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

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

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="specialize">
```

```

<component name="Microsoft-Windows-UnattendedJoin"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
/www.w3.org/2001/XMLSchema-instance">
    <Identification>
        <JoinDomain>anything</JoinDomain>
    </Identification>
</component>
</settings>

<cpu:offlineImage cpu:source="wim://hpfcovcm/c$/vista_inst/
vista.wim#Windows Vista ULTIMATE"
xmlns:cpu="urn:schemas-microsoft-com:cpu" />
</unattend>

```

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

```

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

```

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


Preparing filename.xml

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

Publishing OS Images

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

To publish operating system images

- 1 Start the Publisher (see [To start the Publisher](#) on page 379).
- 2 At the Logon window, type your administrator User ID and password and click **OK**.
 -  Log in to the Publisher using the HPCA user name and password. By default, the user name is **admin** and the password is **secret**.
- 3 In the Publishing Options area:
 - If you are publishing for thin clients, select **Thin Client Publishing**.
 - From the drop-down list, select **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.

Publishing OS Add-ons/extra POS Drivers

You can add drivers to previously prepared images by creating delta packages that are deployed after the image is laid down on a new local partition. This is limited to the Microsoft Windows Setup deployment method based on Microsoft's documentation. Additional options may exist but would require further scripting.

Prerequisites

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

To publish delta packages

- 1 Go to **Start>All Programs>HP Client Automation Administrator Publisher>Client Automation Admin Publisher**. The Logon screen opens.
- 2 In the User ID text box, type your HPCA Administrator user ID and password (**admin** and **secret**).
- 3 In the Publishing Options windows select OS Add-ons/extra POS drivers from the drop-down list.
- 4 Click **OK**.
- 5 Use the Select Drivers window to select the file you want to publish from the appropriate directory.
- 6 From the Add-on Type drop down list, select OS Driver file or Service OS Driver.
- 7 From the Select Target Service drop down list, select the OS service to which you want to add these drivers.
- 8 In the optional Suffix text box, you can type a number that can be used to track packages. For example, if the the instance is called VISTA_PDD and you type 0 in this text box, then the new ADDON instance name will be VISTA_PDD_0.
- 9 In the ADDON Instance Name text box, the instance name will be prepopulated based on the OS service name you selected. It is recommended that you leave this as is. If you modify this name, there will be no connection between the OS service and the ADDON instance unless you create the connection yourself.
- 10 Click **Next**.
- 11 Review the summary screen and click **Publish**.

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

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 393.

To publish BIOS settings

- 1 Start the Publisher (see [To start the Publisher](#) on page 379).
- 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 392.

Publish Hardware Configuration Elements

In this section, you will use the Publisher to publish Hardware Configuration Elements to the HP Client Automation Configuration Server Database.

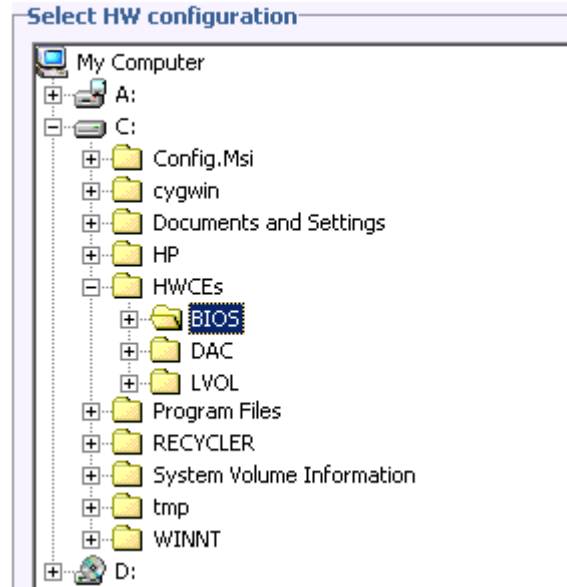
Before you publish your HWCEs, gather your resource files into a single folder. See the *HP Client Automation OS Manager Hardware Configuration Management Guide* for more information.

To publish a Hardware Configuration Element

- 1 Go to **Start>All Programs>HP Client Automation Administrator>HP Client Automation Administrator Publisher**. Refer to the *HP Client Automation Administrator User Guide* for details on how to use the Publisher.
- 2 Type your User ID and Password.
- 3 From the Publishing Options drop-down list, select HW Configuration.
- 4 Click **OK**.
- 5 Select the folder that contains the resources needed to create your HWCE. In our example, we selected `C:\HWCEs\BIOS`.



Make sure that you gathered the correct files that match the system to which you intend to deploy this. If you choose the wrong files you may leave your system in a damaged state.



- 6 In the Description field, type a description of the elements that you are publishing. For this example, type **Pro32 WS Bios Rev 1.00 Resources**.
- 7 In the Package Instance Name field, type the instance name for the package. For this example, type **P32_BIOS_100**.
- 8 Click **Next**.
- 9 Review the information and then click **Publish**. The package resources will be published in a non-compressed format.
- 10 When the Publisher is done, click **Finish**.
- 11 Click **Yes** to confirm that you want to close the Publisher.

Use the CSDB Editor to view the package that has been created in PRIMARY.OS.PACKAGE.

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.

12 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 398
- [Application Self-service Manager Overview](#) on page 398
- [Using the Application Self-service Manager User Interface](#) on page 402
- [Customizing the User Interface](#) on page 409
- [HPCA System Tray Icon](#) on page 415

Accessing the Application Self-service Manager

The Self-service Manager user interface can be accessed through either of the following methods.

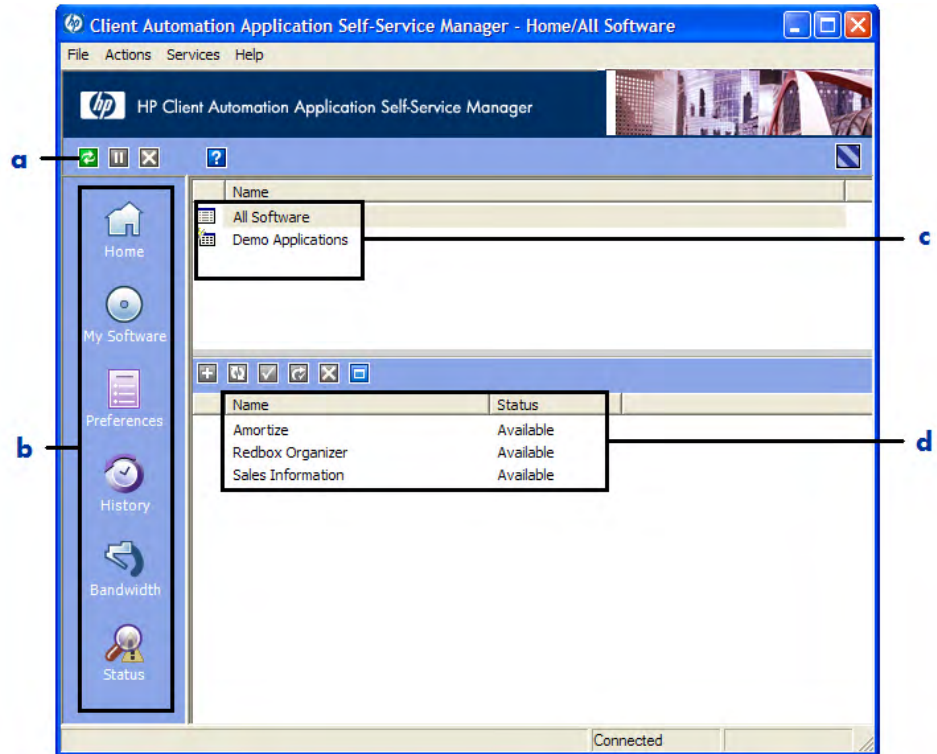
To access the user interface

- 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 48](#) on page 399) 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 48 Application Self-service Manager user interface



Legend

- a **Global Toolbar** – Allows you to refresh the catalog, and pause or cancel the current action
- b **Menu Bar** – Displays various menu choices available while using the Application Self-service Manager
- c **Catalog List** – Lists the different software catalogs available
- d **Service List** – Lists the applications to which the user are entitled

The following sections describe the user interface sections in more detail.


- [Global Toolbar](#) below
- [The Menu Bar](#) on page 400
- [Catalog List](#) on page 401
- [Service List](#) on page 401

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

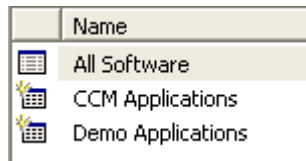
The Catalog List section lists the available software catalogs and any virtual catalogs.




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 400 for more information.

Table 46 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 403
- [Refreshing the Catalog](#) on page 404
- [Viewing Information](#) on page 404
- [Removing Software](#) on page 405

- [Verifying Software](#) on page 406
- [Repairing Software](#) on page 406
- [Viewing History](#) on page 406
- [Adjusting Bandwidth](#) on page 407
- [Viewing Status](#) on page 407

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.

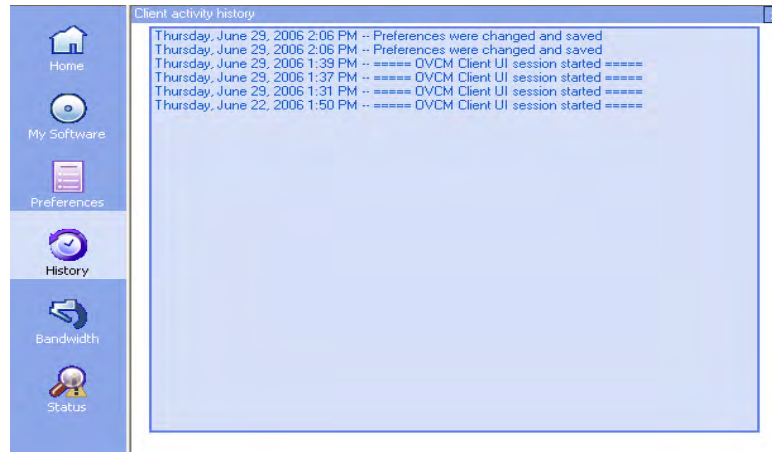
To repair software

- 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 49 History window



- 2 Close the history window to return to the service list.

Adjusting Bandwidth

In the Menu Bar, click **Bandwidth** to display the bandwidth slider. Changing this value dynamically changes the throttling value.

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.

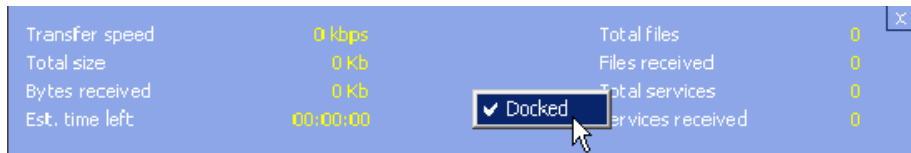
Figure 50 Status display for selected application



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

To un-dock the Status window

- 1 Click **Status** in the Menu Bar.
- 2 Right-click in the Status window that opens.
- 3 Select **Docked** from the shortcut menu. When the Status window is docked, a check mark will appear next to the word **Docked** in the shortcut menu.



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

To dock the Status window

- 1 Click **Status** in the Menu Bar.
- 2 Right-click in the Status window that opens.

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



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

Customizing the User Interface

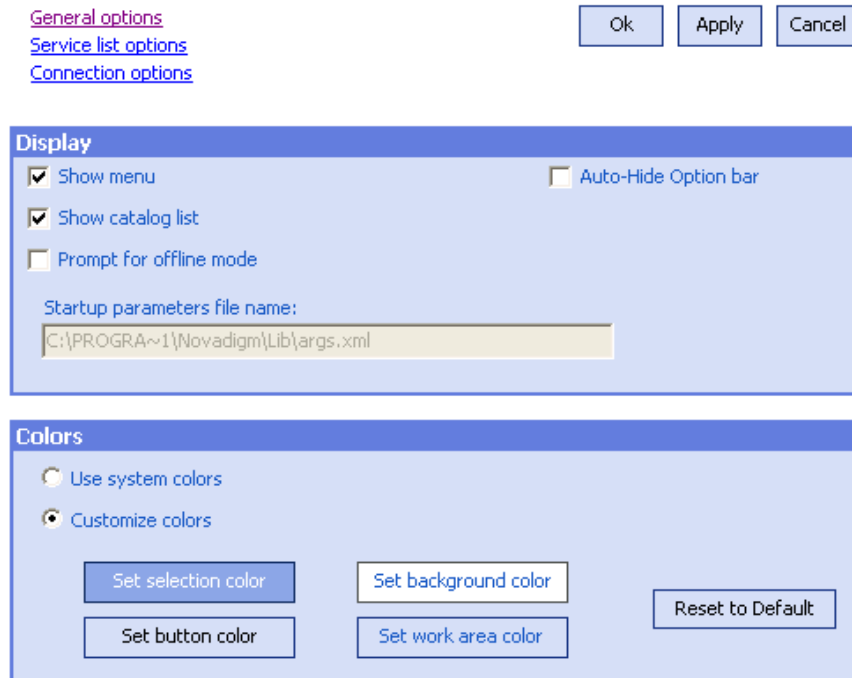
Click the **Preferences** button in the Menu Bar to view the available customization options. The following sections describe each customization area.

- [General Options](#) on page 409
- [Service List Options](#) on page 411
- [Connection Options](#) on page 414

General Options

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

Figure 51 General options window



To modify the display

- If you want to display the menu, select **Show menu**.
- If you want to display the catalog list, select **Show catalog list**.
- If you want to be prompted to use the Application Self-service Manager in offline mode at the beginning of each session, select **Prompt for offline mode**.
- If you want to have the Option bar automatically hidden, select **Auto-Hide Option bar**.

To modify the colors

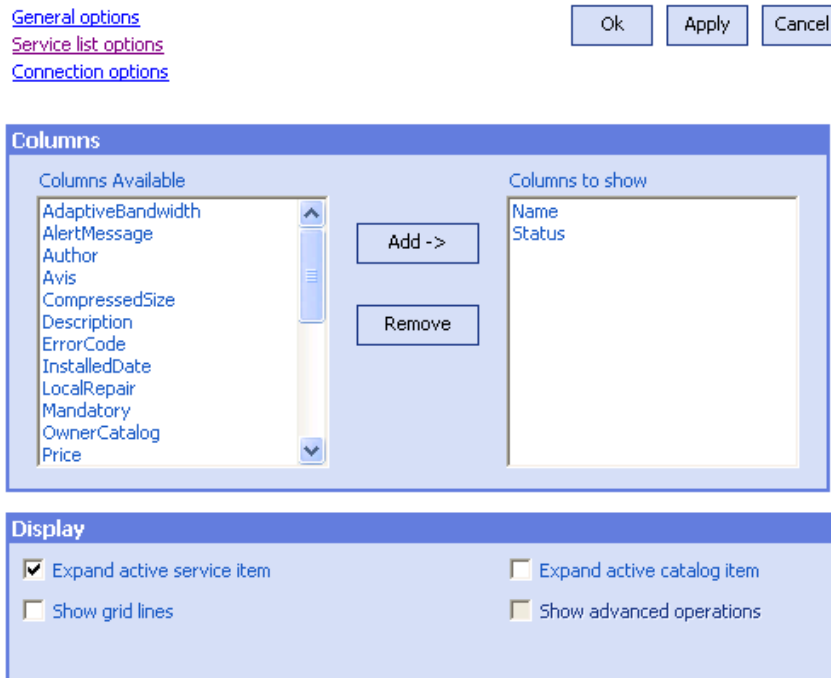
- If you want to use the system colors, select **Use system colors**.
- If you want to customize the color scheme, select **Customize colors**.
 - After selecting Customize colors, click the box labeled:

- **Set selection color** to modify the color of selections.
- **Set button color** to modify the button colors.
- **Set background color** to modify the background color.
- **Set work area color** to modify the background color.

Service List Options

Use the **Service list options** to modify the appearance of the Service List.

Figure 52 Service List options



To customize the column names in the Service List

Use the Columns area to customize the columns that appear in your Service List. The right column lists the names of the column that are currently displayed in your Service List. For a description of each available column heading, see [Customizing the Display](#) on page 412.

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 47 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 47 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 <ul style="list-style-type: none"> • 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 47 Column headings available for the Service List

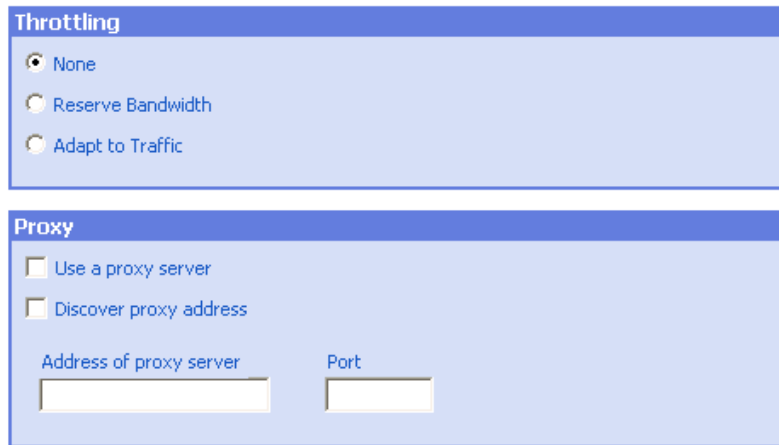
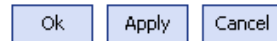
Column Heading	Description
Url	The software vendor's web address.
Vendor	The software vendor who supplied the application.
VerifiedDate	The date on which the application was last verified.
Version	The version of the application.

Connection Options

Use **Connection options**, see [Figure 53](#) on page 414, to select the type of bandwidth throttling to use and to specify proxy server settings.

Figure 53 Connection Options

[General options](#)
[Service list options](#)
[Connection options](#)



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

- Select **Reserve Bandwidth** to slide along the scale to indicate the maximum percentage of the network bandwidth to use. The reserve bandwidth can be changed in the interface by the user as the download is happening.
- Select **Adapt to traffic** to slide along the scale to indicate the minimum percentage of the network bandwidth to use. The adaptive bandwidth cannot be changed during a data download process. It can be set only before a job is dispatched.
- **Proxy**
 - The Application Self-service Manager can detect an internet proxy when one is used. The internet proxy's address is then stored in PROXYINF.EDM located in the client computer's IDMLIB directory. The default location of IDMLIB is *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 54 HPCA System Tray Icon



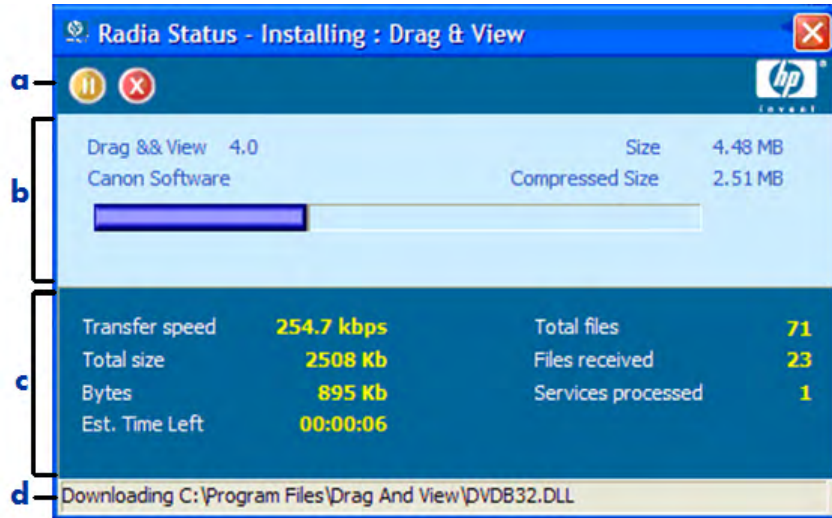
Move your cursor over the icon to see HPCA states:

- **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 55 HPCA Status




Legend

- a Button bar
- b Information panel
- c Status area
- d Status message

The Status window contains the following areas:

- **Button Bar:** Contains buttons for Pause and Cancel, and a logo that becomes animated when the HPCA agent is actively working.
- **Information Panel:** This area contains information about the active application, and a progress bar that shows the percentage of the task finished.
- **Status Area:** Contains statistics about the active processes, including transfer speed, total size of transmission, bytes received, estimated time left of transmission, total files to be transmitted, number of files received, and number of services processed.

- **Status Message Area:** This area shows a message about the current process.
 - **Bandwidth Control:** If you set bandwidth throttling for the application on the HPCA server, and you click the bandwidth toggle button  in the System Tray Console, a slider for bandwidth control appears. Adjust the slider to change the bandwidth throttle value.

13 Troubleshooting

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

- [Log Files](#) on page 419
- [OS Deployment Issues](#) on page 420
- [Application Self-service Manager Issues](#) on page 421
- [Power Management Issues](#) on page 421
- [Patch Management Issues](#) on page 422
- [Troubleshooting the HPCA Server](#) on page 422
- [Browser Issues](#) on page 427
- [Dashboard Issues](#) on page 430
- [Security and Compliance Issues](#) on page 431
- [Other Issues](#) on page 433

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.

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.

Troubleshooting the HPCA Server

The following sections describe how to troubleshoot issues related to your HPCA server.

- [Troubleshooting HPCA Core Components](#) on page 422
- [Troubleshooting HPCA Satellite Components](#) on page 426

Troubleshooting HPCA Core Components

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

- [HPCA Core Configuration Files](#) on page 423

- [HPCA Core Log Files](#) on page 425

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 48 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

Table 48 HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (C:\Program Files\Hewlett-Packard\HPCA\...)
		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
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

Table 48 HPCA Core Configuration Files

HPCA Product	Configuration File Type	Location and File Name (C:\Program Files\Hewlett-Packard\HPCA\...)
		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
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**.

Troubleshooting HPCA Satellite Components

The following section describes how to troubleshoot Satellite Components.

- [HPCA Satellite Log Files](#) on page 426

HPCA Satellite Log Files

If you are having issues with the Satellite server and need to access its log files for troubleshooting, the Satellite Console provides immediate access to the entire set of log files.

To access Satellite server log files

- 1 On the Satellite 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 logs, 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 427
- [Cannot Enable HTTP 1.1 with Internet Explorer 6 and SSL](#) on page 427

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).

Job Issues

The following troubleshooting tip pertains to job management issues.

DTM Jobs Not Working Correctly / RMP Jobs Missing

In a classic CAE installation, a manual post-installation step is required to ensure that the Enterprise Manager properly resolves all target devices when running a DTM job where the target is a group.

This step is also necessary to ensure that all RMP Agent Deployment and OS Deployment jobs are included in the lists of **Current Jobs** and **Past Jobs**.

For more information about these types of jobs, see [Managing Jobs](#) on page 158.

Solution:

- 1 On the system where the Enterprise Manager is installed, open the following file:

```
<InstallDir>\CM-EM\tomcat\webapps\ope\config\dtm.properties
```

2 Configure the following parameters:

```
rmpServer=<rmpServerHostName or IPAddress>  
rmpPort=3471  
rmpUser=admin  
rmpPassword={AES256}3gM1spmbrGbqVXNPDx8tWg==  
rmpProtocol=http\:// or https\://
```

In this case, *<rmpServerHostName or IPAddress>* is the name or address of the system where the HPCA Management Portal is installed.



If you have changed the password for the admin account after installing the Enterprise Manager, be sure to change the `rmpPassword` parameter to reflect the new password.

Dashboard Issues

The following troubleshooting tips pertain to issues that may arise with the HPCA dashboards:

- [Delete Dashboard Layout Settings](#) on page 430
- [Most Vulnerable Products Dashboard Pane Loads Slowly](#) on page 430
- [Dashboard Panes in Perpetual Loading State](#) on page 430

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

Most Vulnerable Products Dashboard Pane Loads Slowly

This pane relies on a database query that can take a very long time if there are a large number of managed devices in the enterprise. In some cases, the query can time out and prevent the pane from loading at all. This pane is disabled by default.

Solution:

Disable the Most Vulnerable Products dashboard pane. See [Dashboards](#) on page 318.

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.

Security and Compliance Issues

The following troubleshooting tips pertain to Security and Compliance configuration, scanning, and reporting:

- [HP Live Network Connector Unable to Connect](#) on page 432
- [Managed and Scanned Device Counts are Zero](#) on page 432
- [Report Presentation is Slow](#) on page 432

HP Live Network Connector Unable to Connect

The most likely cause of this issue is an incorrect proxy server setting. If the system where the HPCA Console is installed requires a proxy to access the Internet, you must specify a proxy server on the HTTP Proxy tab on the Proxy Settings configuration page.

The HPCA Console does not perform any type of validation of the **Proxy Server** field on the HTTP Proxy tab. It does not validate the format or make any attempt to determine whether the proxy server that you have specified is a valid proxy host. Be sure to double-check this setting before you save your changes.

Managed and Scanned Device Counts are Zero

If the Compliance Management, Vulnerability Management, or Security Tools Management dashboard home page indicates that the number of managed devices and scanned devices is zero, this may indicate that there is a problem in the reporting subsystem.

For more information, contact your HPCA administrator.

Report Presentation is Slow

If your vulnerability, compliance, or security tools management reports display slowly in the HPCA Console, you should enable report caching.

Solution:

- 1 Open a web browser and type:

```
http://InstallHost:3466/reportingserver/setup.tcl
```

where *InstallHost* is the host name or IP address of the system where HPCA is installed.

The configuration file page opens.

- 2 In the left navigation menu, click **Vulnerability Management Configuration**.
- 3 Set the following two options:

- a For the **Enable VM Report Caching** option, choose “1” from the drop-down list.
 - b Specify the **VM Cache Lifetime** in seconds. For example, 1200 seconds is 20 minutes.
- 4 Click **Apply**.
- 5 In the left navigation menu, click **Compliance Management Configuration**.
- 6 Set the following two options:
 - a For the **Enable Compliance Management Report Caching** option, choose “1” from the drop-down list.
 - b Specify the **Cache Lifetime** in seconds.
- 7 Click **Apply**.
- 8 In the left navigation menu, click **Security Tools Management Configuration**.
- 9 Set the following two options:
 - a For the **Enable Security Tools Management Report Caching** option, choose “1” from the drop-down list.
 - b Specify the **Cache Lifetime** in seconds.
- 10 Click **Apply**.


Other Issues

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

- [Cannot Open a Report](#) on page 434
- [Additional Parameters Disregarded by the HPCA Job Wizard](#) on page 435
- [Virtual Machines Will Not Start](#) on page 435
- [Query Limit Reached](#) on page 436

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.

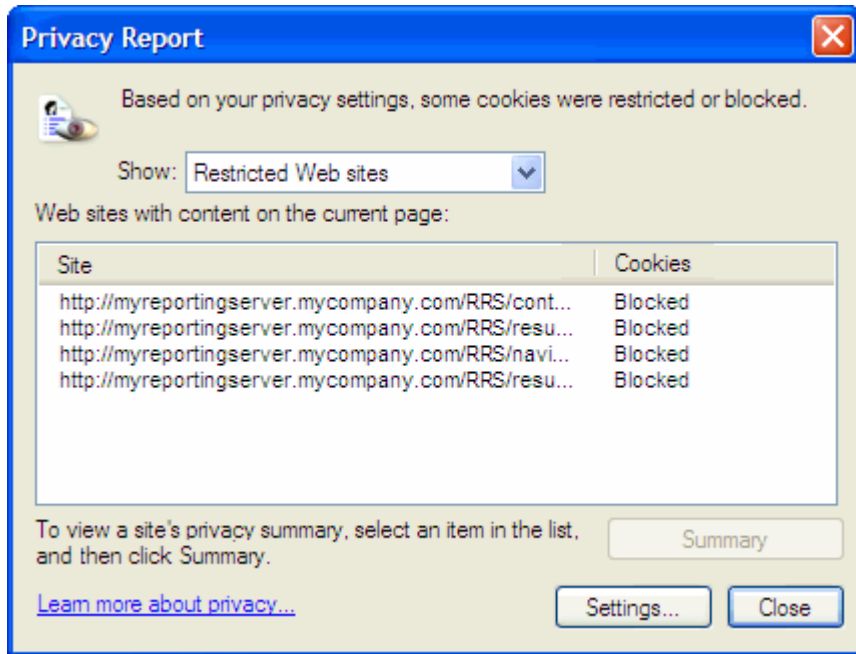
This behavior is most prevalent with Internet Explorer 6 and 7 on the Windows 2003 Server platform. It can, however, happen on any supported platform.

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:



- 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 Tomcat service.



Modifying the `directory_object_query_limit` property may negatively impact performance of the HPCA Console.

A SSL Settings on the HPCA Core and Satellite Servers

In order to fully understand how to use the SSL settings that are available on the HPCA Console, it is important to understand the various “parts” of SSL and their functions. This appendix offers a brief overview of SSL, including how it relates to an HPCA environment. See the following sections:

- [SSL Parts](#) on page 439
- [SSL in an HPCA Environment](#) on page 440
- [The SSL Certificate Fields on the Consoles](#) on page 441

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 be shared.

The SSL Certificate Fields on the Consoles

The Infrastructure Management area of the Configuration tab of the HPCA Console contains two SSL Certificate areas: [SSL Server](#) and [SSL Client](#). The differences between these areas and the necessity of each are explained in this section. To complete the SSL set up for the HPCA, review the information in this appendix, then see [Infrastructure Management](#) on page 263.



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 443
- [Changing the Locale](#) on page 444

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

Supported Languages

[Table 49](#) on page 443 presents the list of supported languages and their valid language codes.

Table 49 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 49](#) on page 443).

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 49](#) on page 443 for a list of supported languages and their valid codes.
- The file `romsinfo.ini` is part of the Service CD iso.

Double-byte Support for Sysprep Files

If using double-byte character support in Sysprep, the file must be encoded in UTF-8 coding.

C IPv6 Networking Support

Client Automation Core and Satellite servers now include features to support customers who are using Internet Protocol version 6 (IPv6) in their networks in a dual stack (IPv4 and IPv6) environment.

Topics in this appendix include:

- [IP Networking Terms and Basics](#) on page 445
- [Overview of IPv6 Support in HPCA](#) on page 448
- [Configuring HPCA Windows Servers for IPv6 Support](#) on page 451
- [Using IPv6 Literal Addresses with Core and Satellite Consoles](#) on page 455.
- [IPv6 How To's and Troubleshooting](#) on page 456

IP Networking Terms and Basics

This topic defines some terms and basic information related to IP version 4 and IP version 6.

An IP address was intended to be a unique number identifying a unique device or port of a device. The 32-bit address space of IPv4 addresses puts severe limits on the number of unique addresses available, and the supply is running out. The IPv6 128-bit address space was created to address this problem.

Terms

- **IPv4 Address:** An IPv4 address contains four sections separated by periods (or “dots”). Each section, called an octet, contains 8 bits expressed in decimal (0-255). When entering an IPv4 address, you can omit leading zeroes.
- **IPv6 Address:** An IPv6 address contains eight sections separated by colons. Each section contains 16 bits expressed in case-insensitive hexadecimal (0000-FFFF).

Example: **2001:0db8:0000:0001:f8f3:a7bb:2cb:6037**

To make it easier to remember and type an IPv6 address, you can use one instance of a double colon (::) to indicate multiple contiguous sections of zeros. You can also omit leading zeroes. For example, you can simplify the address:

2001:0db8:0000:0001:f8f3:a7bb:2cb:6037

to **2001:db8:0:1:f8f3:a7bb:2cb:6037** or

2001:db8::1:f8f3:a7bb:2cb:6037.

- **IPv6 address types:**
 - **Global unicast address:** This is the IPv6 address that can be used for *external communication*. A sample global unicast address is:
2001:db8:0:1:f8f3:a7bb:2cb:6037.
 - **Link-local address:** This address can be used for *communication with neighbors on the same subnet (link), only*. Link-local addresses are not forwarded by routers. Their syntax includes “%n” at the end, for example: **fe80::20c:29ff:fed4:5ab%4**.
 - **IPv4-mapped address:** This address can be used for tunneling an IPv4 address through an IPv6 network. For example:
fe80::5efe:192.168.6.154 tunnels the IPv4 address **192.168.6.154**.

IP Address Shortcuts: IPv4 versus IPv6

The Table below summarizes IP address shortcut conventions for IPv4 and IPv6.

Table 50 IPv4 and IPv6 Reserved IP Address Values

Reserved Meaning	IPv4 Value	IPv6 Value
localhost	127.0.0.1	::1
Any address Any interface	0.0.0.0	::
Tunneling IPv4/IPv6	Not Applicable	fe80::5efe:<IPv4addr> where <IPv4addr> is the IPv4 address, as in: fe80::5efe:192.168.1.2

Bracketing IPv6 Addresses

You must enclose a literal IPv6 address in brackets “[” and “]” in URLs, URIs, or other syntax that allows the IP address to be followed by “:port”. Examples include schemes for HTTP, HTTPS, LDAP and LDAPS entries. The brackets around the IPv6 address are required in order to distinguish the beginning and end of the IPv6 address (which includes colons) from the colon used to identify the port.

Example:

http://[literal_IPv6_address]:port

Omit the brackets when entering an IPv6 address through the Core or Satellite Console pages or a configuration file where the field does not allow for a port entry.

Examples:

- User Interface: **Upstream host: literal_IPv6_address**
- Conf file: **HOST=literal_IPv6_address**
-host literal_IPv6_address

Overview of IPv6 Support in HPCA

Client Automation adds supports for IPv6 on its Windows infrastructure Core and Satellite servers. Specifically:

- The Core and Satellite servers have been enabled to perform HPCA *server-to-server* communications using either IPv4 or IPv6.
- The Core and Satellite servers, as well as the HPCA Configuration Server service, are automatically configured to listen on the available IPv4 and IPv6 stacks that are detected during installation. If only IPv4 is detected, they are configured for IPv4. If IPv6 is also detected, they are configured to listen on both stacks.

IPv6 Support Limitations

The following Client Automation components support IPv4 only and are not IPv6-capable:

- Client Automation agents
- Client Automation Administrative tools
- Traditional, component-based Client Automation infrastructure servers that were installed separately from Core or Satellite servers.
- Out of Bound Management (OOBM) surfaces: IPv6 is intentionally excluded in this release across all OOBM surfaces, including:
 - Core engines to OOBM Web Services
 - OOBM to SCS (SCS is the Intel AMT Setup and Configuration Service)
 - OOBM to Agent

Support for IPv6 in a Core-Satellite Environment

In the current release, Client Automation support for IPv6 focuses on enabling the IPv6 routing of traffic among its in Windows-based Core and Satellite infrastructure servers.

The IP networking features in this release allow the Client Automation servers to use IPv6 or IPv4, as appropriate, to route the following traffic:

- Core and Satellite traffic to sync the Configuration Server metadata
- Core and Satellite traffic to sync the Cache data
- Core or Satellite Authentication and Policy traffic (HTTP and LDAP)
- Inter-Satellite and Core Messaging traffic
- Inter-Satellite and Core HTTP traffic

IP Communications Support Table

The following table identifies the HPCA communication pathways among the Core, Satellites, Agents and external directories. It identifies the communication pathways that support IPv4 only, and those that support IPv4 or IPv6 (IPv4/IPv6). The IPv4/IPv6 support is shown with yellow highlights.

Table 51 IP Communications Support Table

			Target (Server)		
		Agent	Satellite	Core	AD / LDAP
Source:	Agent	N/A	IPv4	IPv4	N/A
(Client):	Satellite	IPv4	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6
	Core	IPv4	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6

The Core and Satellite servers listen on two points (an HTTP listening point and a Configuration Server listening point). Either of these communication points can be IPv4 or mixed, as needed.

The HPCA Agents communicate with Core and Satellite Servers using IPv4, only.

How to Enable IPv6 Server Communications

This release of the Core and Satellite servers still require IPv4 for Agent communications. Thus, to take advantage of IPv6 for server-to-server communications, you need to install the Core and Satellite servers in a dual-stack (IPv4 / IPv6) environment.

If the Core and Satellite Setup programs detect an IPv6 stack on the host server, the Core and Satellite servers are automatically configured to listen on both IPv4 and IPv6 protocols.

Before you run the Core or Server installation, review the prerequisites on [page 450](#).

Prerequisites for IPv6 Support

- The HPCA Core and Satellite Servers must be installed on Windows XP, Windows 2003 Server or Windows 2008 Server Operating Systems that are IPv6-enabled and are running in IPv6-enabled networks. Refer to the Hardware Support Table in the accompanying *HPCA 7.50 Release Notes* document for additional details on these supported platforms.
- Because this release does not provide IPv6 support for the HPCA agents, HPCA servers should be run in a dual stack IPv4\IPv6 environment.
- Your DNS and DHCP must be configured for IPv6 support.
- In order to support IPv6 communications between an HPCA server and a customer-provided external **Active Directory Service (ADS)** being used for Policy and Authentication communications:
 - the ADS must be installed on Windows Server 2008
 - the ADS must be configured for IPv6
- When using Internet Explorer as your web browser, Version 7 or above is required to support IPv6.

Configuring HPCA Windows Servers for IPv6 Support

This section identifies the IPv6-related configuration changes that are automatically made to the HPCA Core and Satellite Windows Server components when they are installed on IPv6-enabled servers.

The configuration topics are discussed in this section:

- [Component: HPCA Apache-based Core and Satellite Servers](#) on page 451
- [Component: HPCA Configuration Server](#) on page 451

For each component, the following details are mentioned:

- How IPv6 is enabled for the component
- How to use the logs to identify if IPv6 is in use
- Limitations and dependencies, if any

Component: HPCA Apache-based Core and Satellite Servers

The HPCA Core and Satellite servers run under an Apache service which is IPv6-enabled by default. The Apache service does not require any configuration changes for IPv6. However, make sure your environment meets the previously stated prerequisites.

To verify that Apache is listening for IPv6 addresses

- 1 Open a command prompt
- 2 Type `netstat -an`
- 3 On the resulting display, check that an entry for `:::3466` exists. If present, this verifies that Apache is listening for v6 addresses.

Component: HPCA Configuration Server

The Configuration Server must listen on IPv4 for Agent communications. If the Core installation program detects an available IPv6 stack, it will automatically enable the Configuration Server to listen on both IPv4 and IPv6 stacks.

How IPv6 is Enabled for the Configuration Server Component

If the Core or Satellite is enabled for IPv6 when the Core and Satellite servers are installed, the Configuration Server is enabled automatically to listen on IPv4 and IPv6 stacks. This includes:

- Enabled session connectivity to accept connections on IPv6 as well as IPv4.
- Enabled session connectivity with the **Secure Sockets Layer (SSL)** for IPv4 as well as IPv6.

To verify the Configuration Server is listening for IPv6 addresses in non-SSL mode

These modifications are made by the Core or Satellite setup program when IPv6 is enabled on the server. You can view and verify the Configuration Server configuration changes used to enable IPv6 using the steps below:

- 1 Use Microsoft Notepad to open `edmprof`, located in the `\bin` directory of where the HPCA server was installed. Notepad supports UTF-8, which is the required encoding for the `edmprof` file.
- 2 Go to the `MGR_ATTACH_LIST` section and locate the `ATTACH_LIST_SLOTS` attribute. When IPv6 is detected, the Core Setup program explicitly adds the following `CMD_LINE` entry for IPv6 enablement. (The `edmprof` default for `ztcpmgr` to listen on IPv4 is also in effect.)

```
CMD_LINE=(ztcpmgr, NAME=tcpmgr6,ADDR=::) RESTART=YES
```

➤ This command line reflects an HPCA Configuration Server using the default port of 3464. If a non-default port is being used, a `PORT` will also be specified after the `ADDR` attribute using the same syntax as shown in [To verify the Configuration Server is listening for IPv6 addresses in SSL mode](#) on page 453.

- 3 The Core setup program also increases the `ATTACH_LIST_SLOTS` value by 1 to accommodate the new `CMD_LINE` entry.

➤ If the `edmprof` file has been changed manually, ensure it is save with UTF-8 encoding, and restart the service for the HPCA Configuration Server (`ZTopTask.exe`).

- 4 To confirm these configuration changes are reflected in the HPCA Configuration Server service (`ZTopTask.exe`), check the Configuration Server log files. You will see two TCP managers waiting to accept incoming requests. For examples, see [Log Messages](#) on page 453.

To verify the Configuration Server is listening for IPv6 addresses in SSL mode

These changes are done automatically by the Core and Satellite setup programs when IPv6 is enabled on the server.

- 1 Use Microsoft Notepad to view `edmprof`, located in the `\bin` folder of where the HPCA Server was installed. Notepad supports UTF-8, which is the required encoding for the `edmprof` file.
- 2 The Core configuration program adds the following lines under the `MGR_ATTACH_LIST` section for SSL Manager IPv4 and IPv6 enablement:

```
[MGR_ATTACH_LIST]
```

```
CMD_LINE=(zsslmgr, NAME=sslmgr4,PORT=443) RESTART=YES
```

```
CMD_LINE=(zsslmgr, NAME=sslmgr6,ADDR=::,PORT=443) RESTART=YES
```

- 3 The Core configuration program also increase the `ATTACH_LIST_SLOTS` value by 2 to accommodate the new `CMD_LINE` entries.

▶ If the `edmprof` file has been changed manually, ensure it is saved with UTF-8 encoding, and restart the service for the HPCA Configuration Server (`ZTopTask.exe`).

- 4 To verify the SSL configuration changes are reflected in the HPCA Configuration Server service (`ZTopTask.exe`), check the log files; you will find two SSL managers waiting to accept incoming requests. See the examples shown in [Log Messages](#) on page 453.

Log Messages

Session Log Messages with SSL Disabled

```
02I 22:22:04 <ztcpmgr /1DC> System Task --- TCP
Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager /1DC> System Task ---
TCP/IP Manager accepting requests at address <RPS> on port <3464>

NVD0402I 22:22:04 <ztcpmgr /954> System Task ---
TCP Manager task has started

NVD0404I 22:22:04 <TCP/IP Manager /954> System Task ---
TCP/IP Manager accepting requests at address <::> on port <3464>
```

Session Log Messages with SSL Enabled

```
NVD0414I 15:04:36 <zsslmgr          /7E8>  System Task    ---  
SSL Manager Task has started  
  
NVD0472I 15:04:36 <SSL Manager      /7E8>  System Task    ---  
SSL Manager accepting requests at address <RPS> on port <0443>  
  
NVD0414I 15:04:36 <zsslmgr          /188>  System Task    ---  
SSL Manager Task has started  
  
NVD0472I 15:04:36 <SSL Manager      /188>  System Task    ---  
SSL Manager accepting requests at address <::> on port <0443>
```

Using IPv6 Literal Addresses with Core and Satellite Consoles

In an IPv6-enabled environment, the following Core and Satellite-related fields can be used with IPv6 addresses or IPv4 addresses. That is, you can use these fields to specify:

- a hostname that resolves to an IPv6 address or an IPv4 address
- a literal IPv6 address or IPv4 address:

Sample IPv6 address: 2001:db8:0:1:f8f3:a7bb:2bcb:6037

Sample IPv4 address: 192.168.0.4

If you are entering a literal IPv6 address in a URL, URI or other field that supports a port designation following the server, always enclose the IPv6 address in brackets. For an example, see the Browser Support entry, below.

Core and Satellite Support of IPv6 Addresses

Browser Support

- URL Access to a Core or Satellite Console installed on an IPv6 server:
Example: **http://[literal_IP_address]:3466**

Satellite Server Installation

- **First Time Wizard, Step 3: Upstream Server**

Satellite Console - Configuration tab

- **Upstream Server page > Upstream Host**
- **Infrastructure Management > Policy > Directory Host**

Core Console - Configuration tab

- **Infrastructure Management > Directory Services > Creation Wizard**
- **Infrastructure Management > Policy > Directory Host**
- **Patch Management > Vendor Settings**

- **Operations > Patch Management > Perform Sync**

IPv6 How To's and Troubleshooting

Use the following sections to get answers to common questions about IPv6 and be able to troubleshoot common problems you may encounter while using HPCA with IPv6.

- [Frequently Asked “How To” Questions](#) on page 456
- [Troubleshooting an IPv6 Environment](#) on page 458

Frequently Asked “How To” Questions

Q1. How do I enable IPv6 for the HPCA Servers?

A. Please see the earlier topics in this Appendix. For details, see [Configuring HPCA Windows Servers for IPv6 Support](#) on page 451 and [How to Enable IPv6 Server Communications](#) on page 449.

Q2. I have enabled IPv6, but when I use my web browser to access the Core I get an error about a bad request or connection refused? How do I resolve this?

A. You could try to isolate the problem using the following options:

- Ping the box (v4) and ping the box (v6).
- Check if you can connect using telnet to the address and port 3466 or 3464. If you can, then the problem must be either a local issue (IE7 is required for IPv6 literal support) or some kind of server-side problem. Check the logs to verify the servers are running and listening.

CA log files are located in the following directories under C:\Program Files\Hewlett-Packard\HPCA on the server:

- \ApacheServer\logs
- \ConfigurationServer\log

Q3. When I connect using my web browser it is **extremely** slow. There are multi-second delays for no apparent reason. Yet the person next door (using v4) has no such problems. Is there a solution?

A. Slow browser connections may be due to a DNS issue where the server hangs for a while trying to figure out the hostname of the caller.

Q4. I have v6 enabled and have v6-aware DNS. If I connect to the console using the hostname as in: `http://myCore:3466`, how can I tell if this connection is using IPv4 or IPv6?

A. You could check the logs for Apache and the Configuration Server. Sample log entries are in the IPv6 Network Support Appendix topics.

Q5. I have v6 enabled and v6-aware DNS. When I perform a Satellite sync, how can I tell if it's using IPv4 or IPv6?

A. You could check the logs for Apache and the DCS.

Q6. When I connect over HTTPS to my Core/Satellite using a literal IPv6 address I get a certificate warning from IE. What's up?

A. If your host can't do a reverse-lookup in DNS for the address, then it can't validate the man-in-the-middle defense. This is because certificates are keyed on FQDN, not on IP addresses. The same holds true for any IP address, not just IPv6 ones.

Q7. I get an error when I specify a link-local address for the upstream host. How do I resolve this?

A. The HPCA Core Server runs under Apache; it does not support a link-local address entry. A global unicast IPv6 address must be specified for the upstream host. For more information, see this Troubleshooting entry: [Is there a problem with the IP addresses I am using? How can I double check them?](#) on page 460.

Troubleshooting an IPv6 Environment

The following diagnostic or verification tips can help troubleshoot simple IPv6 environment problems. Most of these are not specific to working with HPCA's implementation of IPv6, but apply to IPv6 in general.

The topics below help you answer these diagnostic questions:

- [From a remote browser I can access the Core or Satellite, but my login fails with Unknown login failure, or no response. Is there a solution?](#) on page 458
- [Is it a local tool problem, such as a problem with the Web Browser?](#) on page 459
- [Is it a local OS problem? Does the OS have IPv6 support?](#) on page 459
- [Is it a problem with the local OS? How do I test for DNS name resolution of the hostname?](#) on page 459
- [Is there a problem with the IP addresses I am using? How can I double check them?](#) on page 460
- [Is it a problem with the network between my client and the server? Again, how can I validate that?](#) on page 461

[From a remote browser I can access the Core or Satellite, but my login fails with Unknown login failure, or no response. Is there a solution?](#)

Problem: Your login to the Core or Satellite is unsuccessful from a remote browser. You are either getting the message: "Unknown login failure" or no response.

Solution: Unsuccessful remote logins are generally due to one of the following reasons:

- Due to the browser security. **Solution:** Add `http://[<IPv6 address>]:3466/` to your trusted site list.
- Due to IE7 browser Cookies that are not being honored/refreshed. **Solution:** Delete the cookies from your IE7 browser, refresh the page and try logging in again. The navigation path to the Delete Cookies function on an IE7 Browser is given below:

Tools > Internet Options > General Tab > Browsing History > Delete >

Delete Cookies

After deleting the cookies, refresh the page and login again.

Is it a local tool problem, such as a problem with the Web Browser?

If your browser responds with: "**Internet Explorer cannot display the page**" when you try to access the Core or Satellite Console, check the IE browser version you are using.

You must use IE7 or later to open up pages with IPv6 addresses.

Is it a local OS problem? Does the OS have IPv6 support?

To check if your local OS is enabled for IPv6 support, here are some basics:

- On Windows 2000, IPv6 is not supported. Windows 2003 or higher is required.
- On Windows 2003, IPv6 is supported but the IPv6 stack is not loaded by default. If you want your Windows 2003 to have an IPv6 stack (along with the existing IPv4 stack) , execute the following in a command line window of the box: **netsh interface ipv6 install**. This command installs the IPv6 stack.
- On Windows 2008/ Vista, IPv6 is supported by default.

Is it a problem with the local OS? How do I test for DNS name resolution of the hostname?

Especially in the IPv6 world with stunningly long IPv6 addresses, a best practice is to use a hostname that resolves to an IPv6 address. How can you check that the hostname is resolving properly?

You could check this by using either the **Ping** tool or **Nslookup**. Note that you could use Nslookup to resolve the correct hostname and IP address in both v4 and v6 scenarios.

Using the Ping tool: To test DNS name resolution, use the Ping tool and ping a destination by its hostname or fully qualified domain name (FQDN). The Ping tool display shows the FQDN and its corresponding IPv6 address.

Using Nslookup: If the Ping tool is using the wrong IPv6 address:

You can use the Nslookup tool to determine the set of addresses as returned in the DNS Name Query Response message.

- 1 First flush the DNS resolver cache. You can use the command:
ipconfig /flushdns
- 2 At the Nslookup > prompt, use the: **set d2** command to display the maximum amount of information about the DNS response messages.
- 3 Use Nslookup to look up the desired FQDN. Use either:
 - **nslookup <ip address>**
 - **nslookup <hostname>**

Look for AAAA records in the detailed display of the DNS response messages.

Is there a problem with the IP addresses I am using? How can I double check them?

You can check you are using the correct IPv6 address for a device by running the command: **ipconfig**.

On a Win2K3 box enabled for IPv6, **ipconfig** returns three sets of IPv6 addresses, as seen in the following figure:

```
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix . : localdomain
    IP Address. . . . . : 192.168.6.154
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : 2001:db8:0:1:20c:29ff:fed4:5ab
    IP Address. . . . . : fe80::20c:29ff:fed4:5ab%4
    Default Gateway . . . . . : 192.168.6.2

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . :
    IP Address. . . . . : fe80::5445:5245:444f%5
    Default Gateway . . . . . :

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix . : localdomain
    IP Address. . . . . : fe80::5efe:192.168.6.154%2
    Default Gateway . . . . . :

C:\Documents and Settings\Administrator>
```

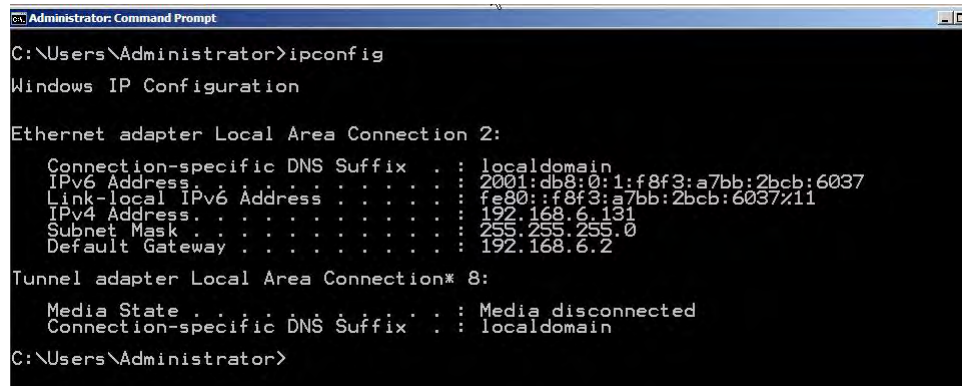
For the three IP Addresses, as circled in red (top to bottom), each is different:

- The address “2001:db8:0:1:20c:29ff:fed4:5ab” is the *global unicast IPv6 address* which can be used for *external communication*.
- The address “fe80::20c:29ff:fed4:5ab%4” is the *link-local address*. This address can be used for *communication with neighbors on the same subnet (link), only*. Link-local addresses are not forwarded by routers.
- The address “fe80::5efe:192.168.6.154%2” is the *IPv4-mapped v6 address*, which can be used for *tunneling*.

Note that a device can have multiple interfaces. You could issue the command: **interface ipv6 show address** to display the IPv6 address assigned to each interface.

On a Win2K8 box, the **ipconfig** command returns only two IPv6 addresses. Also, they are explicitly listed as **IPv6 Address** and **Link-local IPv6 Address**, as seen in the following image under the Ethernet adapter Local Area Connection 2:

From this listing, always use the **IPv6 Address** for external communication. :



```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : localdomain
    IPv6 Address . . . . .           : 2001:db8:0:1:f8f3:a7bb:2bcb:6037
    Link-local IPv6 Address . . . . . : fe80::f8f3:a7bb:2bcb:6037%11
    IPv4 Address. . . . .            : 192.168.6.131
    Subnet Mask . . . . .            : 255.255.255.0
    Default Gateway . . . . .        : 192.168.6.2

Tunnel adapter Local Area Connection* 8:

    Media State . . . . .            : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Users\Administrator>
```

Is it a problem with the network between my client and the server? Again, how can I validate that?

There might a lot of reasons for this. A few are listed below:

- The Firewall might be enabled on the client/ server machine. Please check this and disable the firewall.

- HPCA servers by default listen for both v4 and v6 connections. Client binding on v4 might have failed as server is not listening for v4 connections. On the server side, open a cmd prompt, type: **netstat -an**. This will display all the addresses and ports on which the server is listening.
- Server might be too busy to accept connections.

Index

Symbols

., 32

A

Acquire Microsoft Patches acquisition setting, 314

acquisition settings, 312

Active state of system tray, 415

AdaptiveBandwidth column, 412

adapt to traffic, 415

adding columns to Service List, 412

Additional Files advanced publishing mode option, 382

advanced programmable interrupt controller
See APIC

agent_os parameter, 245

agent_version parameter, 246

Agent Explorer, 396

AlertMessage column, 412

All Devices
group, 190

APIC, 191

Application Self-service Manager

accessing, 398

user interface, 397

Catalog List, 401

Global Toolbar, 400

installing software, 403

Menu Bar, 400

refreshing the catalog, 404

removing software, 405

Service List, 401

viewing information, 404

Author column, 412

AUTOPKG.PATCH instance, 244

AUTOPKG class, 244

Avis column, 412

B

bandwidth

reserving, 415

settings, adjusting, 407

slider, 407

throttling, 407, 414, 417

Bandwidth Control in Status window, 417

blade server reports, 209

boot server, 39

installation port, 39

Bulletins acquisition setting, 312

Button Bar of Status Window, 416

C

- ca-bundle.crt, 440, 442
- catalog
 - refreshing, 400
 - selecting, 401
 - virtual, 401
- Catalog List, 401
- CMI, configuring, 284
- Columns Available list box, 412
- Columns to show list box, 412
- compliance data
 - removing, 247
- Component Select publishing, 383
- CompressedSize column, 412
- configuration files, 423
- Configuration Server Database,
 - synchronizing, 243
- configuring
 - directory service, 272
 - LDAP, 274
- conmfiguring
 - CMI, 284
- Connection options, 414
- Connection Settings, 272
- console access, 255
- console user
 - creating, 256
 - deleting, 257
 - viewing and modifying details, 257
- Customize colors option, 410

D

- dashboard
 - panes, 84

- dashboards, 84
 - configuring, 318
 - HPCA Operations, 319
 - patch, 323
 - Vulnerability Management, 319
 - overview, 84
 - Patch Management, 134
 - Vulnerability Management, 96
- deployment
 - scenarios, os images, 189
- Description column, 412
- Device Resolution, 169
- devices
 - importing, 26
- directory service
 - Configuration Server, 272
 - ldap, 274
 - types, 273
- DISCOVER_PATCH instance, 294
- DISCOVER_PATCH Service, 244
- docked Status window, 408

E

- Embedded Linux, 192, 373
- ErrorCode column, 412
- Expand active catalog item, 412
- Expand active service item, 412

F

- Force acquisition setting, 313

G

Gateway Operations

- Cache Content Details, 250
- Export URL Requests, 250
- Import URL Requests, 251
- View Cache Statistics, 249

Gateway Settings, 289

Global Toolbar, 400

H

HAL, 190

Hardware Abstraction Layer See HAL

Hardware Management, 284

History button, 406

Home button, 400

HPCA Agent ID, 209

HPCA Application Self-service Manager

- user interface
 - repairing software, 406
 - verifying software, 406

HPCA Operations dashboard, configuring, 319

HPCA Status window, 416

HPCA System Tray icon, 415

HP Hardware reports, 210

HP SoftPaq SysIDs, 308

HTTPS, 442

I

Idle state of system tray, 415

ImageName.EDM, 368, 372, 375

Image Preparation Wizard

- using, 369, 372, 375

importing devices, 26

Information Panel of Status window, 416

InstalledDate column, 413

installing

- software using Application Self-service Manager user interface, 403

Internet proxy detection, 415

Inventory Management Reports, 209

IP networking

- dual stack, 445
- IPv4, 445
- IPv6, 445

IPv4 address, 446

IPv6 address, 446

- using brackets, 447

IPv6 support, 445

- Configuration Server, 451
- configuring, 451
- Core and Satellites, 449
- limitations, 448
- prerequisites, 450

J

Job Management, 158

Job States, 165

- Completed, 163, 165

L

LDAPS, 440, 442

Leaf Node Filter, 276

LocalRepair column, 413

Local Service Boot, 196

LOCATION Class, 34

log files, 425, 426

log files, downloading, 232

logs, viewing online, 247

M

- Management Options publishing option, 381
- Mandatory column, 413
- Menu Bar, 400
- Microsoft feed settings, 300
- Microsoft Security bulletins, 312
- Mode acquisition setting, 313
- MSSECURE.XML file, 300
- My Software button, 400

N

- Name column, 413
- Notify Templates, creating, 276
- nvd_attributename attribute, 243
- nvd_classname table, 243

O

- O/S Filter acquisition setting, 302
- operating system images, publishing, 385
- OS image Target Devices requirements, 190
- OS Management, 317
- Out, 314
- OwnerCatalog column, 413

P

- panes, 84
- patch management configuration, 287
- Patch Management Reports, 210
- Patch Manager Server logs, 247
- PATCHMGR domain, 243

- Patch Vulnerability dashboard, 134
 - configuring, 323

- Perform client connect after OS install check box, 370, 376

- Policy Management Wizard, 152
 - Policy Configuration, 152
 - Service Selection, 152
 - Summary, 153

- Preferences button, 400

- prepwiz.exe, 369, 372

- Price column, 413

- Properties publishing option, 382

- proxy
 - detecting, 415

- PublishedDate column, 413

- published services, viewing, 396

- Publisher
 - using, 379

- publishing
 - component select, 383
 - modes
 - additional files, 382
 - management options, 381
 - properties, 382
 - transforms, 382
 - software, 381

- PXE, 196

- PXE boot, 190

R

- Reboot column, 413

- Red Hat Security advisories, 312

- refreshing catalog, 400

- removing
 - columns from Service List, 412
 - software, 405

removing a device, 154
repairing software, 406
Replace acquisition setting, 313
report acquisition status, 242
RePublishedDate column, 413
Reserve Bandwidth, 415
ReservedBandwidth column, 413

S

S.M.A.R.T. Alerts
 reports, 209
Sample Notify Templates, 280
Sample SAP Instances for Two Satellites, 32
SAP Instance
 setting priority, 34
SAPPRI attribute, 34
ScheduleAllowed column, 413
SCSI, 191
server.crt, 441
server.key, 441
Server Access Profile, 31
Service Access Profile for Patch Gateway, 33
Service CD, 197
Service List, 401
 adding columns, 412
 options, 411
 removing columns, 412
Services, 153
 viewing, 153
 viewing details, 153
Show advanced operations, 412
Show Extended Information, 404
Show grid lines, 412

Size column, 413
small computer systems interface See SCSI
software
 publishing, 381
 removing, 405
 repairing, 406
 verifying, 406

SSL

Active Directory, 440
ca-bundle.crt, 440, 442
Certificate Authorities, 439
certificates, 439
Certificates file, 440
digital certificates, 440
generating certificates, 439
HTTPS, 442
LDAPS, 440, 442
Private Key, 441
private key files, 439
Public Certificate, 440
public key files, 439
server.crt, 441
server.key, 441
Server Certificate, 440, 441

SSL settings

Core Console, 441
Satellite Console, 441

Status Area of Status window, 416

Status button, 407

Status column, 413

Status Message Area of Status window, 417

Status Window

Information Panel, 416

- Status window
 - Bandwidth Control, 417
 - Button Bar, 416
 - docking, 408
 - Status Area, 416
 - Status Message Area, 417
 - undocking, 408
- support, 254
- SuSE security patch acquisition, 309
- SuSE Security patches, 313
- SystemInstall column, 413
- system requirements
 - target devices, 190
- system tray
 - active state, 415
 - idle state, 415

T

- target device
 - definition, 190
 - requirements, 190
- Thin client
 - prepare and capture images, 367
- thin client, 192
 - deploying factory OS images to, 192
- throttling, 414
 - adapt to traffic, 415
 - bandwidth, 415
- ThrottlingType column, 413
- transform file, 382
- Transforms publishing option, 382
- troubleshooting
 - Satellite log files, 426

U

- UIOption column, 413

- undocked Status window, 408
- UpgradedDate column, 413
- Url column, 414
- User Details window, 257
- user interface for Application Self-service Manager, 397
- Use system colors option, 410

V

- Vendor column, 414
- VerifiedDate column, 414
- verifying software, 406
- Version column, 414
- viewing
 - information in Application Self-service Manager user interface, 404
 - published services, 396
- virtual catalogs, 401
- virtual hosting servers, 173
- virtual machine
 - creating, 177
 - managing, 173
- Virtual Machine Creation Wizard, 178
- VMware ESX Server, 173
- Vulnerability Management
 - configure HP Live Network Settings, 30
- Vulnerability Management dashboard, 96
 - configuring, 319

W

- Windows 2003 Server, 25
- Windows CE, 192, 371
- Windows Installer files, 381
- Windows XPe, 367

Windows XP Embedded, 192

X

XPe, 192

