

HP Client Automation Enterprise Manager

for the Windows® operating system

Software Version: 7.50

User Guide

Manufacturing Part Number: None

Document Release Date: November 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 2005-2009 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Java™ is a US trademark of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER

Copyright © 1996-1999 Intel Corporation.

TFTP SERVER

Copyright © 1983, 1993 The Regents of the University of California.

OpenLDAP

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

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

OpenSSL License

Copyright © 1998-2001 The OpenSSLProject.

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

DHTML Calendar
Copyright Mihai Bazon, 2002, 2003

Documentation Updates

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

- Software Version number, which indicates the software version.
- 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.

The following table indicates changes made to this document since the last released edition.

Document Changes

Chapter	Version	Changes
All	7.20	HP Configuration Management (CM) was rebranded to HP Client Automation (HPCA).
Chapter 3	7.20	Information explaining how to configure the new dashboards and HP Live Network settings was added. Notify Job Template information was added.
Chapter 4	7.20	Notifying Devices process was updated to include new Notify Job Templates.
Chapter 5	7.20	New chapter discussing Vulnerability Management was added.
Chapter 6	7.20	Information was added describing the new HPCA Operations, Patch Management, and Vulnerability Management dashboards.

Document Changes

Chapter	Version	Changes
Chapter 7	7.20	Added new Vulnerability Management and Administrative reports.
Chapter 8	7.20	Added troubleshooting tips pertaining to using SSL with Internet Explorer 6 and a problem in ESX version 3.5 Update 2 that prevents Virtual Machines from starting.
Chapter 2	7.20	The version of Adobe Flash Player supported now correctly reads 9.0.124 or higher.
Chapter 4	7.50	Support for Distributed Task Management (DTM) jobs, OS Management, synchronizing satellites, and Out of Band (OOB) management added. Notify Job Templates were renamed Job Action Templates. They can be used for either DTM or Notify jobs.
Chapter 5	7.50	Compliance (SCAP) and Security Tools Management features added to existing Vulnerability Management offering.
Chapter 6	7.50	Added the Compliance Management and Security Tools Management dashboards, along with support for perspectives (Global, Mobile, and Virtual) and custom filters.
Chapter 7	7.50	Added Compliance Management and Security Tools reports.
Appendix A	7.50	Added information about enabling custom perspectives and filters.
Appendix B	7.50 November 2009	Added instructions for creating Distributed Task Management (DTM) jobs in an HPCA Enterprise (CAE) classic component-based installation.

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	15
	Audience	16
	Chapters Summary	16
	Variables and Abbreviations	17
	Related Documents	17
	Next Steps	18
2	Installing the Enterprise Manager	19
	System Requirements	20
	Platform Support	21
	Installation Tasks	21
	Post-Installation Steps	23
	Installation Troubleshooting	24
	MySQL Port Conflicts	25
	Enterprise Manager Port Conflicts	26
	Missing RMP or OS Deployment Jobs	28
3	Accessing and Configuring the Enterprise Manager	29
	Navigating the Enterprise Manager	30
	Signing in to the Enterprise Manager	30
	Enterprise Manager Tabs	31
	Online Help	32
	Basic Configuration	33
	Configure Directory Services	34
	Navigate the Directory Services Page	35
	View Directory Service Details	36
	Modify Directory Service Property Settings	38
	Configure a Connection to the Configuration Server Directory Service	38

Configure Connections to External Directory Services	40
Specify Console Settings.	43
Create Enterprise Manager Users	44
Create Job Action Templates	47
Create a New Template.	48
Sample Templates	50
Integrate the Reporting Server	51
Security and Compliance Management Configuration	52
Configure the HP Live Network Settings	53
Configure the Connection to the HP Live Network Server.	54
Configure the Database Settings	56
Configure the Live Network Updates.	59
Download the HP Live Network Connector	62
Test Your Live Network Settings	63
Configure the Dashboards	65
HPCA Operations	66
Vulnerability Management	67
Compliance Management	68
Security Tools Management	69
Patch Management	70
Configure Remote Control	72
Configure Event Auditing	73
Log Files	74
4 Managing the Enterprise	77
Managing Directory Policies	78
View an Object's Properties	80
Search for an Object	82
Manage Policy for Directory Objects	84
Service Information	87
Importing Devices	88
Managing Groups.	89
Deploying the HPCA Agent.	90
Managing Jobs	92
Current and Past Jobs	93
Jobs and Job Executions.	94

Targets	94
Schedules	95
Job Details for DTM Jobs	96
Job Details for Notify Jobs	97
Job Details for RMP Jobs	98
Job Execution Details	98
Job Execution States	99
Create a New DTM or Notify Job	100
Delete a Job	101
Device Resolution for Notify Jobs	101
Device Resolution for DTM Jobs	102
Removal of Old Job Execution Records	103
Managing Virtual Machines	104
Creating New Virtual Machines	108
Controlling Devices Remotely	111
Requirements for Remote Connections	112
Requirements for Windows Remote Desktop Connection	113
Requirements for VNC	113
Requirements for Windows Remote Assistance	114
Firewall Considerations	115
Remote Control Auditing	116
Managing Operating Systems	117
OS Management Terms	118
Prerequisites for OS Management	119
Deployment Scenarios	120
Requirements for Target Devices	121
Deploying Thin Client Factory Images	123
How it Works	124
View the OS Deployment State	124
Deploy an OS Image	125
OS Management Wizard	126
Using LSB	128
Using Network Boot	128
Using an ImageDeploy CD or DVD	128
Perform a One-Time Hardware Maintenance Operation	130
View the Status of OS Management Activities	131

Creating a CD/DVD for OS Deployment	131
5 Security and Compliance Management	135
Introduction	136
Vulnerability Management.	136
Compliance Management.	138
Security Tools Management.	141
HPCA and HP Live Network.	142
License Requirements	142
Software Prerequisites.	143
How Security and Compliance Management Works in HPCA	144
How HP Live Network Content is Updated	145
Scanning Services in Detail	149
Configuring Security and Compliance Management	152
Common Security and Compliance Management Tasks	152
Update HP Live Network Content.	152
Schedule or Trigger a Scan.	153
Entitle A Device for Scanning.	154
Create an HPCA Job to Schedule or Trigger a Scan	155
Start a Scan from a Target Device	156
View the Results of a Scan or Update	157
Find Vulnerability Remediation Information	157
Find Information about Compliance Failures	159
Find Information About Security Tools	161
Advanced Topics.	162
Use the Command Line Utility	162
Required Settings	163
Optional Settings.	165
Stored Settings.	167
Examples	167
Run the HP Live Network Connector Manually.	168
Next Steps	170
Move HP Live Network Content from a Test Environment to a Production Environment	170
More Information about Security and Compliance Management.	173

6	Using the Dashboards	175
	Dashboard Overview	176
	Dashboard Perspectives	180
	Dashboard Filters	182
	HPCA Operations Dashboard	182
	Client Connections	183
	Service Events	184
	12 Month Service Events by Domain	186
	Vulnerability Management Dashboard	188
	Vulnerability Impact by Severity (pie chart)	189
	Historical Vulnerability Assessment	191
	Vulnerability Impact	193
	HP Live Network Announcements	198
	Vulnerability Impact by Severity (bar chart)	199
	Most Vulnerable Devices	201
	Most Vulnerable Subnets	202
	Top Vulnerabilities	204
	Compliance Management Dashboard	207
	Compliance Status	208
	Compliance Summary by SCAP Benchmark	210
	Historical Compliance Assessment	211
	Top Failed SCAP Rules	213
	Top Devices by Failed SCAP Rules	215
	Security Tools Management Dashboard	217
	Security Product Status	218
	Security Product Summary	220
	Most Recent Definition Updates	222
	Most Recent Security Product Scans	223
	Patch Management Dashboard	226
	Device Compliance by Status (Executive View)	227
	Device Compliance by Bulletin	229
	Device Compliance by Status (Operational View)	230
	Microsoft Security Bulletins	231
	Most Vulnerable Products	232
7	Using Reports	235

Reports Overview	236
Navigating the Reports	238
Types of Reports	241
HPCA Management Reports	241
Inventory Management Reports	241
HP Hardware Reports	242
Patch Management Reports	242
Vulnerability Management Reports	243
Compliance Management Reports	244
Security Tools Management Reports	244
Drilling Down to Detailed Information	246
Filtering Reports	246
8 Troubleshooting	251
Browser Issues	252
Cannot Refresh Page Using F5	252
Cannot Enable HTTP 1.1 with Internet Explorer 6 and SSL	252
Browser Error Occurs when Using Remote Control	253
Job Issues	253
DTM Jobs Not Working Correctly / RMP Jobs Missing	253
Dashboard Issues	255
Delete Dashboard Layout Settings	255
Most Vulnerable Products Dashboard Pane Loads Slowly	255
Dashboard Pane Cannot Be Loaded	256
Dashboard Pane Cannot Be Loaded – Reporting Query Failed	256
Dashboard Panes in Perpetual Loading State	256
RSS Query Failed	257
Security and Compliance Issues	258
HP Live Network Connector Unable to Connect	258
Managed and Scanned Device Counts are Zero	259
SQL Server Connection Errors	259
Report Presentation is Slow	260
Other Issues	261
Cannot Open a Report	261
Additional Parameters Disregarded by the HPCA Job Wizard	262
Virtual Machines Will Not Start	263

Query Limit Reached	263
A Adding Custom Dashboard Filters and Perspectives	265
Add a Filter	265
Add a Perspective	266
B DTM Jobs in an HPCA Classic Installation	269
Requirements	269
Configuring Your Servers	270
Configure the Proxy Server	270
Configure the Server Access Profiles (SAPs)	272
Configure the Messaging Server	275
Test a DTM Job	277

1 Introduction

The HP Client Automation Enterprise Manager (Enterprise Manager) is a web-based agent management tool that enables you to quickly and easily manage software, patches, and inventory for devices in your environment.

This guide introduces the Enterprise Manager, shows you how to install and configure its components, and provides detailed information and instructions for using the Enterprise Manager. The following topics are included:

- [Accessing and Configuring the Enterprise Manager](#) on page 29
- [Managing the Enterprise](#) on page 77
- [Security and Compliance Management](#) on page 135
- [Using the Dashboards](#) on page 175
- [Using Reports](#) on page 235
- [Troubleshooting](#) on page 251



The Enterprise Manager is only available in a traditional (classic) component-based Client Automation Enterprise (CAE) installation. It is not available in a Core and Satellite installation. The HPCA Enterprise Console, which has many features in common with the Enterprise Manager, is used in Core and Satellite installations.

If your environment uses Core and Satellite servers, refer to the *HP Client Automation Core and Satellites Getting Started and Concepts Guide*.

Audience

This guide is intended for administrators who will be installing, configuring, and using the Enterprise Manager in a traditional (classic) component-based CAE installation.

Chapters Summary

This guide contains the following chapters in addition to this one:

- [Chapter 2, Installing the Enterprise Manager](#) includes information about the system requirements and installation instructions.
- [Chapter 3, Accessing and Configuring the Enterprise Manager](#) describes how to configure the Enterprise Manager for use in your enterprise.
- [Chapter 4, Managing the Enterprise](#) shows you how to use the Enterprise Manager to administer policy on your devices and monitor the Operations, Vulnerability Management, and Patch Management dashboards.
- [Chapter 5, Security and Compliance Management](#) presents an overview of the HPCA vulnerability management solution and instructions for related tasks.
- [Chapter 6, Using the Dashboards](#) describes the various dashboards available in the Enterprise Manager.
- [Chapter 7, Using Reports](#) shows you how to display and filter reports related to HPCA operations, vulnerability and compliance management, patch management, and auditing.
- [Chapter 8, Troubleshooting](#), provides tips for solving common problems.
- [Appendix A, Adding Custom Dashboard Filters and Perspectives](#), instructions for adding your own filters and perspectives to the dashboards
- [Appendix B, DTM Jobs in an HPCA Classic Installation](#), provides details you will need to set up and run DTM jobs in a classic (component-based) HPCA installation.

Variables and Abbreviations

Table 1 Abbreviations Used in this Guide

Abbreviation	Definition
HPCA	HP Client Automation
CAE	Classic (traditional) HPCA Enterprise environment installed from individual server components (not Core and Satellite)
CSDB	Configuration Server Database
Portal	HPCA Portal, formerly known as the Management Portal

Table 2 Variables Used in this Guide

Variable	Description	Default Value
<code><InstallDir></code>	Location where the Enterprise Manager is installed	Classic HPCA Enterprise installation: C:\Program Files\HP\HP BTO Software Core and Satellite installation: C:\Program Files\Hewlett-Packard
<code><DataDir></code>	Location where the Enterprise Manager stores data files	Classic HPCA Enterprise installation: C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software Core and Satellite installation: C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\HPCA

Related Documents

The following guides describe products related to the Enterprise Manager.
HP Client Automation Configuration Server User Guide

HP Client Automation Portal Installation and Configuration Guide

HP Client Automation Reporting Server Installation and Configuration Guide

Next Steps

Proceed to [Chapter 2, Installing the Enterprise Manager](#).

2 Installing the Enterprise Manager

This chapter contains the following information:

- [System Requirements](#) on page 20
- [Platform Support](#) on page 21
- [Installation Tasks](#) on page 21
- [Post-Installation Steps](#) on page 23
- [Installation Troubleshooting](#) on page 24



This chapter applies specifically to a traditional (classic) CAE installation.

If your environment uses Core and Satellite servers, use the Enterprise Console instead of the Enterprise Manager. Refer to the *HP Client Automation Core and Satellites Getting Started and Concepts Guide* for more information.

System Requirements

If you are using the classic (traditional) HP Client Automation (HPCA) installation process, you will need to install the following components in your enterprise in addition to the Enterprise Manager. You will also need to identify which ones will be used by the Enterprise Manager.

- HP Client Automation Configuration Server (Configuration Server)
- HP Client Automation Configuration Server Administrator (Administrator)
- HP Client Automation Reporting Server (Reporting Server)
- HP Client Automation Portal (Portal)
- HP Client Automation Messaging Server (Messaging Server)



The Reporting Server supplies the data that is used to populate the dashboards and provides the reports. If you do not have a Reporting Server installed and identified in your enterprise, you will not be able to use these features in your Enterprise Manager.

For information about installing and configuring the Reporting Server, refer to the *HP Client Automation Reporting Server Guide (Reporting Server Guide)*.

If you are using a Core and Satellite installation, the Enterprise Manager and the components on which it depends are automatically installed as part of the Core server installation.

The device on which the Enterprise Manager will be installed requires one of the following browsers:

- Microsoft Internet Explorer 6.x or 7.x, with patches applied. Internet Explorer 8.x is not currently supported.
- Mozilla Firefox 2 (or later)

Browsers require Adobe Flash Player version 9.0.124 (or later) to be installed. Refer to:

www.adobe.com/go/getflashplayer

For Enterprise Manager to properly display data, the following desktop display settings are minimum requirements:

- Screen Resolution: 1024x768

- Color Quality: Medium (16 bit)

Installation and execution of Enterprise Manager is not supported on servers that are configured to perform the role of Windows Terminal Server.

Platform Support

For information about the platforms that are supported in this release, see the accompanying release notes.

Installation Tasks



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

You will need to complete the following tasks to use all the features of the Enterprise Manager. Be sure to have the IP address, host name, and port for your Configuration Server, Portal, and Reporting Server.



The Enterprise Manager runs in an instance of the Tomcat application server. By default, Tomcat uses port 8080 for HTTP communication and port 8443 for HTTPS communication.

If the Enterprise Manager is installed behind a firewall, and you will be accessing it from outside the firewall, make sure that the firewall allows incoming network connections to Tomcat.

If this is not configured properly, you will not be able to access the Enterprise Manager from outside the firewall. If you require SSL (secure) access, the firewall must also be configured to allow incoming network connections on the secure Tomcat access port.

If you configure your Tomcat installation to use ports other than 8080 and 8443 as described here, you will need to modify the Enterprise Manager configuration accordingly. See [Enterprise Manager Port Conflicts](#) on page 26 for detailed instructions.

To install the Enterprise Manager and configure Portal settings:

- 1 From the installation media, navigate to the following directory:
Enterprise Manager\win32
- 2 Double-click the installation executable.
- 3 Select a language and click **OK**.
- 4 Follow the steps in the wizard, and provide the appropriate responses.
- 5 After installation, you will be prompted for your Portal settings:

Hostname:*	<input type="text" value="localhost"/> <i>e.g. cmportalserver.mycorp.com</i>
Port:*	<input type="text" value="3471"/> <i>e.g. 3471 or 443</i>
Protocol:*	<input type="text" value="http"/> ▼

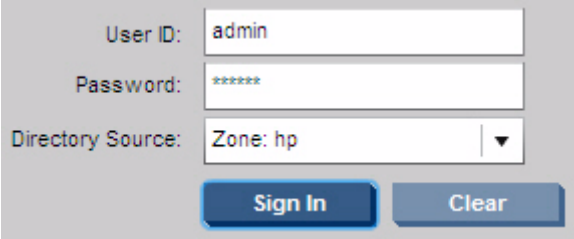
▶ If your web browser does not display this settings window, you will need to access it manually by opening a web browser and navigating to the following URL on the system where the Enterprise Manager is now installed:

CAE: **http://localhost:8080/em**

- 6 Type or select the correct settings, and click **Save**. The settings are then validated. If validation fails, an error is displayed.

If validation is successful, click **Close** to continue. You will be automatically redirected to the Enterprise Manager start page.

- 7 Sign in with a **User ID** of *admin* and a **Password** of *secret*. These are the defaults. For now, the directory source should be the zone you created when you installed the Portal.



The screenshot shows a sign-in form with the following fields and values:

- User ID: admin
- Password: *****
- Directory Source: Zone: hp

Below the fields are two buttons: "Sign In" and "Clear".

- ▶ You should change the admin user's password before using the Enterprise Manager in a production environment. See [Create Enterprise Manager Users](#) on page 44 for instructions.

- 8 Click **Sign In**.

The main screen of the Enterprise Manager is displayed and you are successfully signed in.

To remove the Enterprise Manager:

- From the **Add or Remove Programs** Control Panel applet, select the HPCA Enterprise Manager. Use the regular removal procedure for your operating system.

Post-Installation Steps

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 92.

To configure the Enterprise Manager to properly list all types of jobs:

- 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}3gM1spmbrGbcqVXNPDx8tWg==
```

```
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.

Installation Troubleshooting

This section includes information to help you troubleshoot an Enterprise Manager installation.

MySQL Port Conflicts

If you encounter a problem with conflicting port addresses, you may need to change the default port used by MySQL. Enterprise Manager installs MySQL using port 3479, by default. You can change this port number if another application is already using this port.

To change the MySQL port number:

- 1 For a CAE installation, stop the following service:

HP Client Automation Enterprise Manager

Stopping this service will also stop and restart the database service. This is required for the port change to take effect. This step is not necessary for a Core and Satellite installation.

- 2 Edit the following file:

CAE: `<InstallDir>\CM-EC\database\bin\opedb.ini`

Core and Satellite: `<InstallDir>\HPCA\database\bin\my.ini`

- 3 Find the line `port=3479`

Change this to match the port number you want to use. There will be two instances, one in the client section and one in the server section. Be sure to change both instances of the port declaration to the same value.

- 4 Save the file.

- 5 Edit the `hibernate.cfg.xml` file. To edit this file you will need to open the `ope-core-<version>.jar` file. You can open this file with an archive extraction tool such as WinZip. The file is located in this directory:

CAE: `<InstallDir>\CM-EC\tomcat\webapps\ope\WEB-INF\lib`

Core and Satellite:

`<InstallDir>\HPCA\tomcat\webapps\ope\WEB-INF\lib`

- 6 Locate the file `hibernate.cfg.xml` and open the file for editing.

- 7 Find the `hibernate.connection.url` value and change the port 3479 to the same port number configured in the `opedb.ini` file (or `my.ini` file) above.

- 8 Save the `hibernate.cfg.xml` file back to the `ope-core-<version>.jar` file.

- 9 Start the service that you stopped in Step 1.

To verify that the database is accessible with the new port configuration:

- 1 Locate the MySQL command line tool. It is located in the following directory:

CAE: `<InstallDir>\CM-EC\database\bin`

Core and Satellite: `<InstallDir>\HPCA\database\bin`

- 2 Run the following command:

```
mysql.exe -uope -pope ope -P<portNumber>
```

In this case `<portNumber>` is the port number that you specified in Step Find the line `port=3479` above. For example:

```
mysql.exe -uope -pope ope -P3479
```

This command tells the tool to use the login/password `ope/ope`, the database `ope`, and port `3479`. Be sure to specify the newly updated port number.

- 3 Once you are logged in, run the `status` command to display current database information.
- 4 Use `Exit` to close the tool.

Enterprise Manager Port Conflicts



The following information pertains only to classic (traditional) HPCA Enterprise (CAE) installations. For Core and Satellite installations, see the *HPCA Core and Satellites Getting Started Guide*.

By default, the Enterprise Manager uses Tomcat port 8080 for HTTP communication and port 8443 for HTTPS communication. If you change your Tomcat installation to use different ports, you must also change the Enterprise Manager ports.

To change the Enterprise port numbers:

- 1 Stop the following service:

CAE: HP Client Automation Enterprise Manager

Core and Satellite: HPCA Tomcat Server

- 2 Edit the following file:

```
<InstallDir>\CM-EC\tomcat\conf\server.xml
```

- 3 Find the following text:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->  
<Connector port="8080"
```

Change the port to match the port number that you want to use.

- 4 Also find the following text:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->  
<Connector port="8443"
```

Change this to match the port number that you want to use.

- 5 Save the `server.xml` file.

- 6 Edit the following file:

```
<InstallDir>\CM-EC\tomcat\webapps\em\WEB-INF\  
Console.properties
```

- 7 Find the following strings:

```
opeurl=http://localhost:8080/ope/resources
```

```
dtmurl=http://localhost:8080/ope/resources
```

If you are using SSL, the protocol will be `https` and the port will be 8443.

Change this to match the port number that you want to use.

- 8 Find the following string:

```
vulnerability_management_server_url=http://localhost:8080/  
vms/livecontent
```

If you are using SSL, the protocol will be `https` and the port will be 8443.

Change this to match the port number that you want to use.

- 9 Save the `Console.properties` file.

- 10 Start the service that you stopped in Step 1.

Missing RMP or OS Deployment Jobs

A manual post-installation step is required to configure the Enterprise Manager so that it properly displays RMP and OS Deployment jobs on the Current Jobs and Past Jobs pages. See [Post-Installation Steps](#) on page 23.

3 Accessing and Configuring the Enterprise Manager

This chapter contains information you can use to access, navigate, and configure the Enterprise Manager. This includes signing in, configuring user access, setting up Directory Services, establishing proxy settings, specifying the security and compliance settings, and creating templates for managing jobs. The following topics are discussed:

- [Navigating the Enterprise Manager](#) on page 30
- [Basic Configuration](#) on page 33
- [Security and Compliance Management Configuration](#) on page 52
- [Log Files](#) on page 74

Navigating the Enterprise Manager

The Enterprise Manager enables you to define the desired state for your enterprise by setting configuration policies in your enterprise directory services. In this section, you will learn how to sign in to the Enterprise Manager, and the purpose of each tab. The following topics are covered in this section:

- [Signing in to the Enterprise Manager](#) on page 30
- [Enterprise Manager Tabs](#) on page 31
- [Online Help](#) on page 32

Signing in to the Enterprise Manager

Before you can configure the Enterprise Manager, you must sign in.

To sign in to the Enterprise Manager

- 1 Double-click the Enterprise Manager icon on your desktop, or use the Windows programs group.

In a traditional (classic) CAE installation, you can also open a web browser and go to the following URL:

```
http://<EM_hostname>:8080/em
```

where <EM_hostname> is the name of the device where the Enterprise Manager has been installed.

To sign in to the Enterprise Manager using secure (SSL) communications, open a browser and go to:

```
https://<EM_hostname>:8443/em
```

A default truststore containing a temporary certificate is included in the Enterprise Manager. If you wish to use SSL to access the Enterprise Manager, you will be prompted to accept or reject this default certificate. Acceptance of this certificate will allow you to use the Enterprise Manager; however, you should replace this temporary truststore with one containing a valid certificate for your server. For more information about creating a permanent truststore, see the *HP Client Automation SSL Implementation Guide (SSL Guide)*.

If you changed the Enterprise Manager port, be sure to use the new port number in this URL instead of 8080.

Sign in with the Enterprise Manager user name and password (by default, these are *admin* and *secret*.) If you have not already done so, you should change the default user's password. See [Create Enterprise Manager Users](#) on page 44 for instructions.

▶ Do not use non-ASCII characters when entering passwords.

- 2 Select the directory source. Until you have completed other configurations, the directory source should be the zone you created when you installed the Portal.
- 3 Click **Sign In**.

▶ If the Enterprise Manager is installed behind a firewall, and you will be accessing the Enterprise Manager from outside the firewall, make sure that the firewall allows incoming network connections to Tomcat (default port is 8080). If it does not, you will not be able to access the Enterprise Manager from outside of the firewall. If you need SSL (secure) access, then the firewall must also be configured to allow incoming network connections to Tomcat (default port is 8443).

Your current session credentials are displayed in the upper right corner of the Enterprise Manager.

[To sign out of the Enterprise Manager](#)

In the upper right corner of the Enterprise Manager page, click **Sign Out**.

Enterprise Manager Tabs

The following tabs are available in a fully configured Enterprise Manager installation:

- **Home:** Use this tab to view the following dashboards:
 - HPCA Operations
 - Vulnerability Management
 - Compliance Management


- Security Tools Management
- Patch Management


See [Using the Dashboards](#) on page 175 for more information. Note that the dashboards are not functional until the Reporting Server is integrated into the Enterprise Manager.

- **Management:** Use this tab to view and manage devices in your environment. See [Managing the Enterprise](#) on page 77 for more information.
- **Reporting:** Use this tab to see reports about your environment. These reports are provided by the Reporting Server. To use this tab, you must enable Reporting in the Enterprise Manager (see [Integrate the Reporting Server](#) on page 51). See the *HP Client Automation Reporting Server Installation and Configuration Guide (Reporting Server Guide)* for more information.
- **Configuration:** Use this tab to configure the Enterprise Manager, including directory services, user accounts, HP Live Network settings, and dashboards. Any account in the internal zone (non-LDAP accounts) has access to the Configuration tab. See [Create Enterprise Manager Users](#) on page 44 for more information.

Online Help







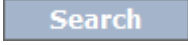
Context sensitive online help is available throughout the Enterprise Manager.

To open the help window, click the  (online help) button in the upper right corner of the page.

In a dashboard pane, you must first click the  (quick help) button in the lower right corner of the pane to make the quick help panel visible. Then, click the online help button to open the help window.

In the online help window, you can use the following buttons to find the information that you need:

Table 3 Online Help Navigation Tools

Button	Description
	Show the table of contents panel, and highlight the location of the current topic in the table of contents.
	Move one topic “up” in the table of contents.
	Move one topic “down” in the table of contents.
	Print the help topic currently displayed.
	Display the table of contents.
	Display the alphabetical index of help topics.
	Search all online help topics for a keyword or phrase.

Basic Configuration

At a minimum, you will need to complete the following tasks to finish configuring the Enterprise Manager:

- Decide which directory services you will use.
- Decide which directory services you will use for administrator authentication to the console.
- Decide which directory services will be used for assigning policy.

These tasks are described in [Configure Directory Services](#) on page 34 and [Specify Console Settings](#) on page 43.

Depending on the additional Enterprise Manager features that you want to use, you may also need to do the following:

- [Create Enterprise Manager Users](#) on page 44
- [Create Job Action Templates](#) on page 47
- [Integrate the Reporting Server](#) on page 51
- [Security and Compliance Management Configuration](#) on page 52
- [Configure the Dashboards](#) on page 65
- [Configure Remote Control](#) on page 72
- [Configure Event Auditing](#) on page 73

Configure 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 Enterprise Manager
- 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 Enterprise Manager.

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 Enterprise Manager. 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 35

[Configure a Connection to the Configuration Server Directory Service](#) on page 38

[Configure Connections to External Directory Services](#) on page 40








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 4 Directory Services Toolbar Buttons

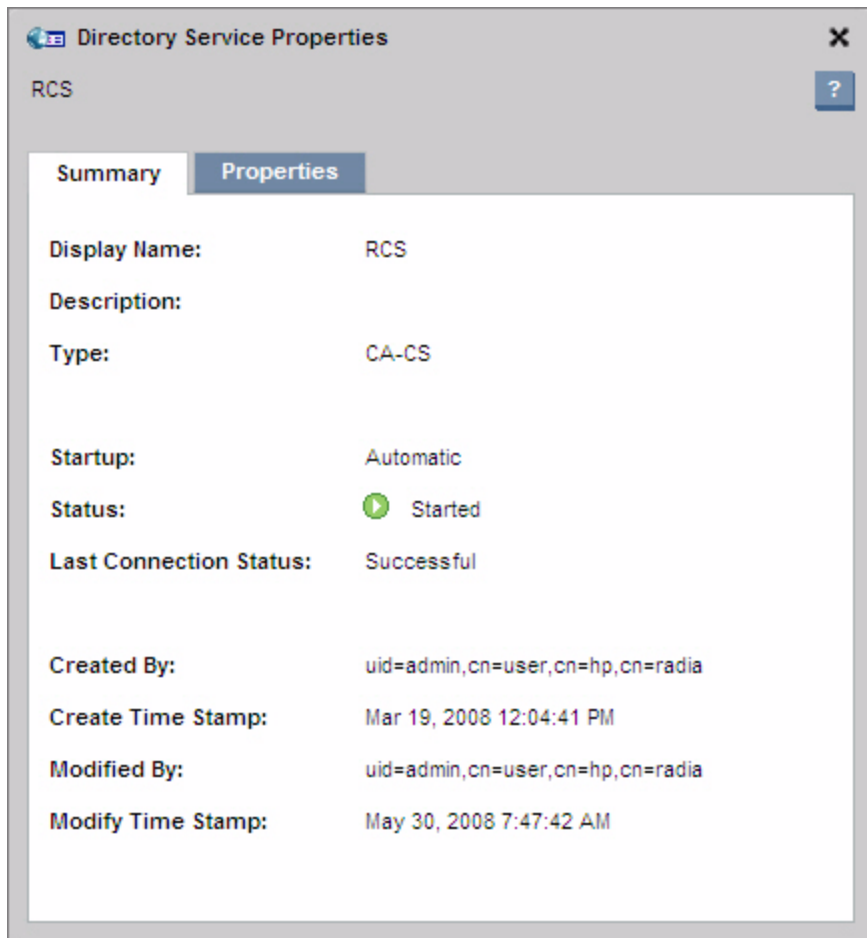
Icon	Toolbar Button Name	Description
	Refresh Data	Refreshes the Directory Services list.
	Show/Hide Filter Input	Use to show or hide the filter toolbar. You can filter Directory Services data by using a text string and narrow the search by selecting individual Directory Services columns to include in 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 38
 - [Configure Connections to External Directory Services](#) on page 40
- 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 Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager 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 38.

You can administer LDAP policies through the Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager.
- 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 Enterprise Manager 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 Enterprise Manager for policy management.
- **Used for Authentication:** When enabled, this directory service becomes enabled as a sign-in option on the Enterprise Manager 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 Enterprise Manager. Any user that is a member of this group will be enabled to sign in to the Enterprise Manager.
 - **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.

Specify Console Settings

Use Console Settings to set advanced options for the Enterprise Manager user interface.

To configure your Enterprise Manager console settings:

- 1 From the Configuration tab, click **Console Settings**.
- 2 Set the following options. All parameters marked with an asterisk (*) are required.
 - Use **Maximum Cache Age (Minutes)** to set the threshold for when the cache should expire for a given set of data. This value is in minutes.
 - Use **Directory Search Attributes** to specify a default set of attributes for the drop-down filter in the Directory Search dialog.

The data queried from the Portal database – for example, Children or Services displayed in tables – are cached by the Enterprise Manager. Maximum cache age indicates when the given set of data should be expired.

Consult your directory service’s documentation for valid attributes.

- Specify the **Operational Process Engine URL** to specify the location of the Operational Process Engine (OPE), including the port on which it listens. The OPE is an internal HPCA component responsible for executing Notify commands. Its default HTTP port is 8080.
 - Select **Enable HTTP Proxy Support** if there is a proxy server that will be used for outbound communication from the Enterprise Manager, such as a Real Simple Syndication (RSS) feed in the dashboard. If you select this option, you must also specify the following:
 - **Proxy Server Host**: network addressable name of the proxy server
 - **Port**: port on which the proxy server listens
- 3 Click **Save** to implement your changes.
 - 4 Click **Close** to acknowledge the dialog.

Create Enterprise Manager Users

Use the Configuration tab to configure the internal users who have access to this Enterprise Manager.

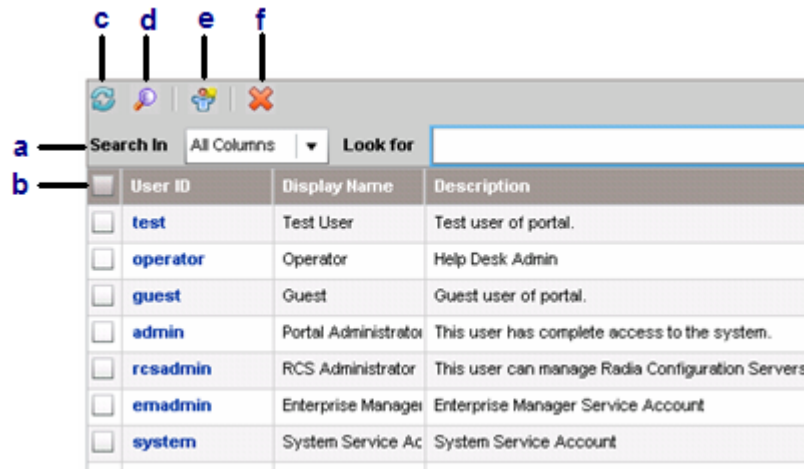
When you create a user from the Enterprise Manager, you are creating a user for the Portal who has administrative access to the internal data store, but may not have access to the directory source depending on the configuration of the directory source. If you do not want to use—or do not have LDAP servers to use for authentication—you will need to create an Enterprise Manager user.

The following User IDs are included, by default, in a classic (traditional) CAE installation:


- test
- operator
- guest
- admin
- rcsadmin
- emadmin
- system

The list is slightly different for a Core and Satellite installation.

Figure 1 User List



Legend

- a Filter toolbar. This does not appear until you click the Filter  button.
- b Select all users.
- c Refresh User list.
- d Show/Hide Filter toolbar.
- e Show New User wizard.
- f Delete User.

To create an Enterprise Manager user:

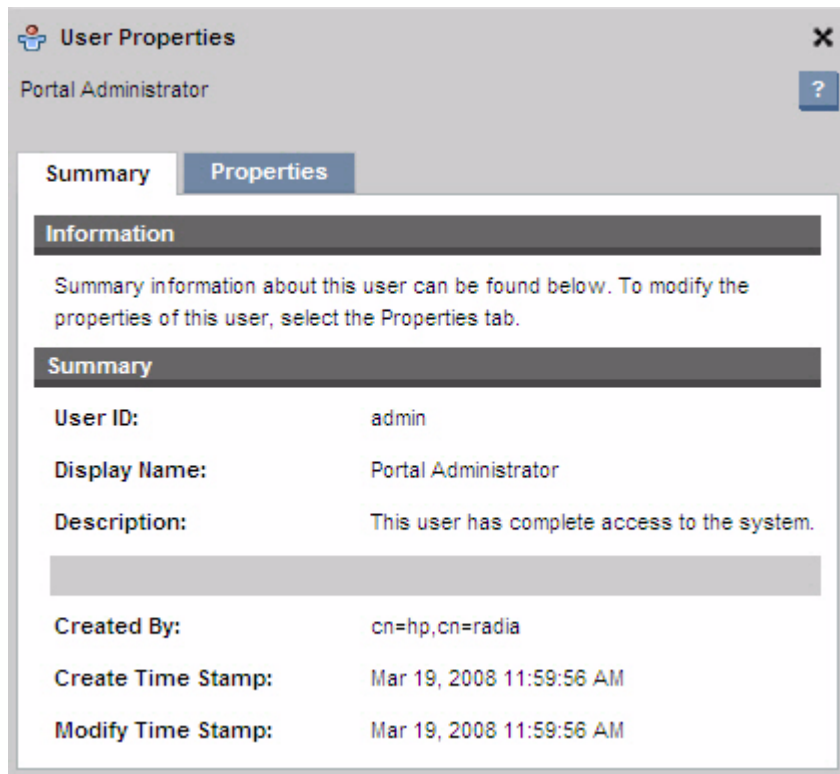
- 1 From the Configuration tab, click the **Users** button in left pane.
- 2 From the Users section, click the **New User** button. The **User Creation Wizard** starts.
- 3 You have the following configuration options. All parameters marked with an asterisk (*) are required.
 - Create a **User ID**.
 - Create a **Display Name**.

- Type a meaningful **Description** for the user.
 - Use **Password** to specify the password for the user. Retype the password in **Confirm Password**.
- 4 Click **Next**.
 - 5 Review the Summary screen. If all properties are correct, click **Commit**.
 - 6 Click **Close** to acknowledge the dialog.

If the user already exists, you may want to view its properties or change the password.

To view user details:

- 1 From the Configuration tab, click **Users** in the left pane.
- 2 Click the name of a user. The following screen capture shows a sample User Properties window.



- 3 Click the **Summary** tab to see basic information about the user. You cannot modify these properties.
- 4 Click the **Properties** tab to see the display name and description of the user. You can modify these properties.
- 5 Click **Save** if you make any modifications.
- 6 Click **Close** to acknowledge the Execution Status dialog.
- 7 Click the **X** in the upper right corner to close the User Properties window.

To change a password:

- 1 From the Configuration tab, click the **Users** button in the left pane.
- 2 Click the name of the user whose password you want to change.
- 3 Click the **Properties** tab to see the display name and Description of the user.
- 4 Click **Change Password**.
- 5 Type in the new password. All parameters marked with an asterisk (*) are required.



If you are changing the password for the user who is currently signed in, this session will be invalidated, and you will need to sign in again.

- 6 Click **Commit**.
- 7 Click **Close** to close the Execution Status dialog.
- 8 Click the **X** in the upper right corner to close the User Properties window.

The password has been changed.

Create Job Action Templates

Job Action Templates enable you to pre-define parameters used when creating new jobs.

Job Action Templates are managed in the Jobs 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 48 for detailed instructions.

The following Job Action Templates are provided when you install the Enterprise Manager:


- Patch Connect
- Security Connect
- Software Connect

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.

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 **Jobs**.
- 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 50.
 - 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 to 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 92 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.

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.

Integrate the Reporting Server

The Reporting Server enables you to view and filter information about devices in your enterprise. When the Reporting Server is integrated into the Enterprise Manager, you can access the Reporting Server by clicking the Reporting tab.



To use this feature, you must already have a Reporting Server configured for your enterprise. For information on installing and configuring the Reporting Server, see the *Reporting Server Guide*.

To integrate the Reporting Server

- 1 From the Configuration tab, click **Reporting**.
- 2 Click **Enable Integration**.
- 3 In the **HPCA Reporting URL** box, type the URL for your Reporting Server. Enter the fully qualified host name in the configuration box.

Do not use `localhost` even if the Reporting Server is on the same computer as the Enterprise Manager.

For a Core and Satellite installation, this is automatically configured. The value is `http://<HPCACoreServer>:3466/rrs`

- 4 Click **Save**.
- 5 Click **Close**. At this point, you must log out of the Enterprise Manager to complete the integration.

Click **OK** to log out of the Enterprise Manager. When you log in again, the Reporting tab will be visible.

Security and Compliance Management Configuration

You can use the Live Network configuration page in the Enterprise Manager to configure your HPCA security and compliance management solution.

- The **Settings** tab enables you to provide the URL for your HP Live Network content server, your HP Live Network login credentials, and proxy server information.

Proxy server information is required only if there is a proxy server between the system hosting your HPCA security and compliance management solution and the Internet.

From the **Settings** tab, you can also download the HP Live Network Connector. Because the Connector is installed with HPCA and is self-updating, however, this is rarely necessary.

- The **Databases** tab enables you to specify information about your Configuration Server and Reporting database.
- The **Schedule Updates** tab enables you to configure security and compliance management content updates.
- The **Update Now** tab enables you to immediately update the security and compliance management content from the source specified on that tab.

The HPCA Reporting features must be properly configured to enable security and compliance management reporting. The `vm.kit`, `compliance.kit`, and `stm.kit` report packs must be present. To optimize report generation speed, you may also want to enable report caching.

Brief instructions are provided here. For detailed information about reporting and report packs, refer to the *Reporting Server Installation and Configuration Guide*.

To configure security and compliance management reporting:

- 1 Open a web browser and type the following URL:

CAE Install: `http://<ReportingHost>/reportingserver/setup.tcl`

Core Install: `http://<ReportingHost:3466>/reportingserver/setup.tcl`

where `<ReportingHost>` is the host name or IP address of the system where the Reporting Server is installed.

The configuration file page opens.

- 2 In the left navigation menu, click **Vulnerability Management Configuration**.
- 3 For the **Enable VM Reports** option, choose “1” from the drop-down list.
- 4 *Optional:* If you want to optimize the speed with which vulnerability management reports are generated and displayed, follow these steps:
 - 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.
- 5 Click **Apply**.
- 6 In the left navigation menu, click **Compliance Management Configuration**.
- 7 Repeat [step 3](#) – [step 5](#) for Compliance Management
- 8 In the left navigation menu, click **Security Tools Management Configuration**.
- 9 Repeat [step 3](#) – [step 5](#) for Security Tools Management.

Configure the HP Live Network Settings

There are three steps required to configure the Enterprise Manager security and compliance management features:

- [Configure the Connection to the HP Live Network Server](#) on page 54
- [Configure the Database Settings](#) on page 56
- [Configure the Live Network Updates](#) on page 59

The tabs on the Live Network configuration page contain the settings required to perform these steps. On the Settings and Databases tabs, you can test your configuration settings before you save them.

Passwords entered on the Live Network configuration tabs are encrypted.



Some of the configuration steps described in this section are not necessary in a Core and Satellite installation. All steps are required in a classic (traditional) CAE installation, however.

Configure the Connection to the HP Live Network Server

Use the Settings tab 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.
- Your HP Passport login credentials.
- Name, port, and authentication credentials for the Internet proxy server, if one exists, between the Enterprise Manager and the HP Live Network content server.

▶ For your security and convenience, the HP Live Network content server uses HP Passport authentication. HP Passport is a single sign-in service that enables you register with all HP Passport-enabled web sites using a single user ID and password. To set up your HP Passport profile, go to:

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

Make sure that your HP Passport profile includes the 12-digit service agreement identifier (SAID) associated with your HPCA support contract. This SAID must include entitlement to HP BSA Essentials so that you can access the HP Live Network content server. For assistance, contact your HP Software sales representative.

▶ Passwords entered on this tab are encrypted.

You can test your configuration information before you save it. When you request a test, the Enterprise Manager 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 63 for details.

To specify the HP Live Network connection settings:

- 1 On the Configuration tab, click **Live Network**.
- 2 Click the **Settings** tab.
- 3 Specify the following information. All parameters marked with an asterisk (*) are required.
 - **HP Live Network User ID**—your HP Passport user ID.

- **HP Live Network Password**—your HP Passport password.
- **HP Live Network Content URL**—the location of the HP Live Network content server for vulnerability definitions and scanners (URL filled in by default).
- **HP Live Network Connector**—the path to the Live Network Connector executable on the system hosting the Enterprise Manager (path filled in by default).

For more information, see [Run the HP Live Network Connector Manually](#) on page 168 and [Download the HP Live Network Connector](#) on page 62.

- **HTTP Proxy Server**—URL and port for the proxy server, if one is used, that will facilitate Internet communication between the Enterprise Manager and the HP Live Network content server.

Specify this URL in the following format:

[http|https]://server:port

For example: **https://webproxy.mycompany.com:8088**

Be sure to specify the correct protocol, name, and port in the URL for your proxy server. The Enterprise Manager does not validate this URL. If it is not correct, you will be unable to update your HP Live Network content.

- **Proxy User Name**—the user name for proxy server access. This is only required if the proxy server requires authentication.
 - **Proxy Password**—the password for proxy server access. This is only required if the proxy server requires authentication.
- 4 To test the settings that you have specified, click **Test**. See [Test Your Live Network Settings](#) on page 63 for more information.
 - 5 Click **Save** to implement your changes.



The Enterprise Manager 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 tab, 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.

Configure the Database Settings

Use the Database tab to specify where the security and compliance management information downloaded from HP Live Network should be published:

- Reporting Database

The latest HP Live Network vulnerability definitions are published to the Reporting database. These definitions are then used to populate various reports (see [Using Reports](#) on page 235) and dashboard panes (see [Using the Dashboards](#) on page 175).

This is the same database as the Inventory Database. Therefore, the database information used to connect to the Reporting database will be the same information that was required to set up the ODBC DSN to the Inventory Database. This step would have been performed as part of the installation and configuration of a Core and Satellite installation.

For a traditional HPCA Enterprise installation, refer to the *Configuration Server Guide* and the *Messaging Server Guide*. For a Core and Satellite installation, refer to the *HPCA Core and Satellites Getting Started Guide*.

- Configuration Server Database

The latest HP Live Network scanners and data are published to the Configuration Server. The Configuration Server then pushes this content to the scanner services in the SECURITY Domain in the Configuration Server Database (CSDB). The most recent scanners and data are deployed to managed client devices whenever a vulnerability or compliance scan is performed.

Passwords entered on this tab are encrypted.

You can test your configuration information before you save it. When you request a test, the Enterprise Manager attempts to connect to the databases that will store your vulnerability and compliance management content. If the connection succeeds, you know that your configuration information is valid.

To specify the database settings:

- 1 From the Configuration tab, click **Live Network**.

- 2 Click the **Databases** tab.
- 3 Under Reporting database Configuration, specify the following information. All parameters marked with an asterisk (*) are required.
 - **Database Type**—select `oracle` or `sqlserver` from the list.
 - **Database Server**—specify the fully qualified host name or IP address of the system where the Reporting database is located.

If you are using SQL Server, and it is configured to use something other than the default database instance, you must append the instance to the server name. For example:

```
mydbserver.mycompany.com\myinstance
```

You must also specify the database name in the **Database Name** field.
 - **Port**—specify the port used to access the Reporting Server. The default is 1521 for Oracle and 1433 for SQL Server.

Some databases, such as SQL Server, may use a dynamic port unless specifically set up within the database management software to use a static port. If the database is set to use dynamic ports, leave this field empty.
 - **Database Name**—specify the name of the Reporting database. For Oracle, this is the same as the SID of the database.
 - **Database User**—specify the user name that will be used to access the Reporting database.
 - **Password**—enter the password for the Reporting database user you specified above.
- 4 Under Configuration Server, specify the **Password** for the CSDB service account ID listed.

The other Configuration Server parameters shown here are configured on the Directory Services page under the Configuration tab.
- 5 To test the settings that you have specified, click **Test**.
- 6 Click **Save** to implement your changes.



The Enterprise Manager 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 tab, 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.

Configure the Live Network Updates

Use the Schedule Updates and Update Now tabs 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 62 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
```

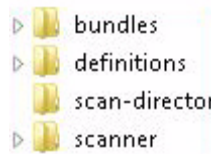
This path is configured automatically by HPCA. You do not need to specify this path unless you have downloaded a new copy of the HP Live Network Connector and installed it in a different location.

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 Enterprise Manager 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 168.

- **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 170.

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 Configuration tab, 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:
 - **Schedule**—Select Once, Hourly, Daily, Weekly, or None

None is what the Enterprise Manager 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.

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 Configuration tab, 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.

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

Security Tools Management > Product Reports > All Products



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:

CAE installation:

```
<InstallDir>\VulnerabilityServer\logs\vms-server.log
```

Core server in a Core and Satellite installation:

```
<InstallDir>\HPCA\VulnerabilityServer\logs\vms-server.log
```

There will be no other indication in the Enterprise Manager that the update has failed, however.

If the Reporting database is not properly configured on the Databases tab, there may not be any records in this report, and you will have to use the log file. For more information about reports, see [Using Reports](#) on page 235.

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, click **Live Network**.
- 2 Click the Settings tab.

- 3 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.
- 4 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
```

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 Enterprise Manager first confirms that all required settings are specified and that all settings have the proper format. It then takes the following actions:

- Settings tab

The Enterprise Manager 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 this tab 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**.

- Databases tab

The Enterprise Manager attempts to first connect to the Reporting Database and then to the Configuration Server using the settings specified.

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. For the Databases tab, the results for the Reporting Database and Configuration Server tests are shown separately.

Table 5 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). • The database information for the Reporting Database is incorrect. • The password for the Configuration Server is incorrect. <p>Other errors may also be reported by the Reporting Database or Configuration server.</p>

Table 5 Live Network Settings Test Results

Icon	Outcome	Explanation and Suggested Action
	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 Enterprise Manager 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 (see [Log Files](#) on page 74).



You must click the **Save** button to save your settings—even if the test is successful. The Enterprise Manager does not automatically save your settings.

Configure the 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 183

[Service Events](#) on page 184


The Executive View also includes the following pane:

[12 Month Service Events by Domain](#) on page 186

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 182.

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 189
- [Historical Vulnerability Assessment](#) on page 191
- [Vulnerability Impact by Severity \(bar chart\)](#) on page 199
- [Vulnerability Impact](#) on page 193

The Operational View includes the following four information panes:

- [HP Live Network Announcements](#) on page 198
- [Most Vulnerable Devices](#) on page 201
- [Most Vulnerable Subnets](#) on page 202
- [Top Vulnerabilities](#) on page 204

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 188.




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 server

Currently 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 210
- [Compliance Status](#) on page 208
- [Historical Compliance Assessment](#) on page 211

The Operational View includes the following information panes:

- [Top Failed SCAP Rules](#) on page 213
- [Top Devices by Failed SCAP Rules](#) on page 215


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 207.

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 218
- [Security Product Summary](#) on page 220

The Operational View includes the following information panes:

- [Most Recent Definition Updates](#) on page 222
- [Most Recent Security Product Scans](#) on page 223


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 217.

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 227
- [Device Compliance by Bulletin](#) on page 229

The Operational View includes three information panes:

- [Device Compliance by Status \(Operational View\)](#) on page 230
- [Microsoft Security Bulletins](#) on page 231
- [Most Vulnerable Products](#) on page 232

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 226.

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.

Configure Remote Control

The Enterprise Manager 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 Enterprise Manager 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 112 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 111.

Related Topic:

[Configure Event Auditing](#) on page 73

Configure Event Auditing

If you want to be able to log security and compliance data acquisition and remote control operations, you must ensure that the HPCA event auditing subsystem is properly configured. The following requirements must be met:

- The HPCA Messaging Server “Core” data delivery agent (`core.dda`) must be enabled and configured. This triggers the creation of the auditing tables.
 - For a Core and Satellite installation, this component is installed automatically and simply needs to be configured by specifying the Messaging settings in the HPCA Core Console.
 - For a classic (traditional) CA Enterprise installation, you must select the `core.dda` and configure it as part of the Messaging Server installation.

For detailed instructions, refer to the *Core and Satellite Getting Started Guide* or the *Messaging Server Installation and Configuration Guide*.

- The HPCA Reporting Server must be installed and properly configured to enable HPCA Management reporting. The HPCA Management Report Pack (`admin.kit`) must be present. To optimize report generation speed, you may also want to enable HPCA Management report caching.

Brief instructions are provided below. For detailed information about reporting and report packs, refer to the *Reporting Server Installation and Configuration Guide*.

- The Vulnerability Management subsystem must be configured. The Auditing subsystem uses the same database connection settings that the Vulnerability Management subsystem uses. See [Configuring Security and Compliance Management](#) on page 152.

To configure the HPCA Management reports:

- 1 Open a web browser and type the following URL:

CAE Install: `http://<ReportingHost>/reportingserver/setup.tcl`

Core Install: `http://<ReportingHost:3466>/reportingserver/setup.tcl`

where `<ReportingHost>` is the host name or IP address of the system where the Reporting Server is installed.

The configuration file page opens.

- 2 In the left navigation menu, click HPCA Management Reports Configuration.
- 3 For the **Enable HPCA Management Reports** option, choose “1” from the drop-down list.
- 4 *Optional:* If you want to optimize the speed with which Administration Reports are generated and displayed, follow these steps:
 - a For the **Enable HPCA Management Report Caching** option, choose “1” from the drop-down list.
 - b Specify the **HPCA Cache Lifetime** in seconds. For example, 1200 seconds is 20 minutes.
- 5 Click **Apply**.

Log Files

If you are having issues with connecting or using features of the Enterprise Manager, you may need to access the log files. Enterprise Manager log files are stored in the following location by default:

CAE: `<InstallDir>\CM-EM\tomcat\logs`

Core and Satellite: `<InstallDir>\HPCA\tomcat\logs`

The Enterprise Manager stores information in multiple log files:

- `catalina.<date>.log` contains the Enterprise Manager server log messages. Multiple server logs may be found in the default log directory with `<date>` specified (for example: `catalina.2007-10-22.log`).
- `OvCMEEmTomcat`
Contains messages related to installing, stopping, and starting Tomcat service.
- `ope.log` contains the Enterprise Manager job process engine messages. Default log settings allow for a maximum of 10 backup log files, each no greater than 5 MB. The initial log file is `ope.log` and subsequent backup

log files are appended with a number, for example, `ope.log.1`, `ope.log.2`. After 10 backup files have been generated, the oldest file is replaced the next time that the current log file is backed up.

Security and compliance management log files are stored in the following location:

CAE: `<InstallDir>\VulnerabilityServer\logs`

Core and Satellite: `<InstallDir>\HPCA\VulnerabilityServer\logs`

- `vms-server.log` contains vulnerability management server messages. Default log settings allow for a maximum of five backup log files, each no greater than 5 MB. The initial log file is `vms-server.log` and subsequent backup log files are appended with a number: `vms-server.log.1`, `vms-server.log.2`, etc.
- `vms-commandline.log` contains status and error messages logged by the `content-update.bat` command. See [Update HP Live Network Content](#) on page 152 for more information. Default log settings allow for a maximum of 5 backup log files, each no greater than 5 MB.

The same file naming convention used for `vms-server.log` is used for `vms-commandline.log`. In both cases, after 5 backup files have been generated, the oldest file is replaced the next time that the current log file is backed up.

You can change the vulnerability management server log levels – for example, INFO or DEBUG – without restarting the server. The log levels are specified in the following files:

`log4j-server.properties`

`log4j-commandline.properties`

Both files are located here: `<InstallDir>VulnerabilityServer\conf`

If you change the log level, the change will be reflected in the log file messages approximately 60 seconds after you save the pertinent file.

You are not expected to understand all of the contents of the logs, but you should be aware of them for the following reasons:

- To be able to look for entries labeled **SEVERE**, **FATAL**, or **ERROR**.
- To access the files under the direction of HP Support

4 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:

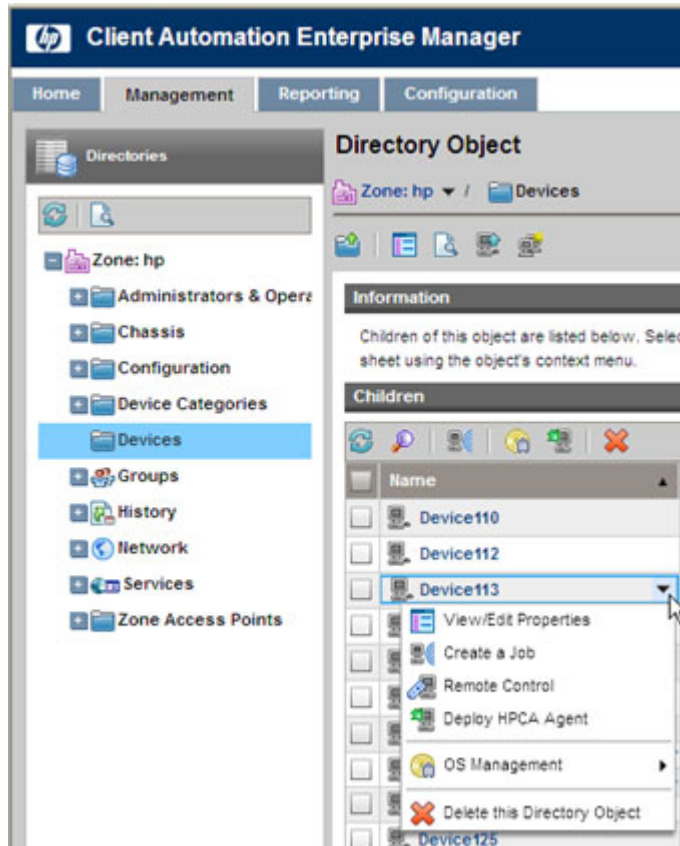
- [Managing Directory Policies](#) on page 78
- [Service Information](#) on page 87
- [Managing Groups](#) on page 89
- [Deploying the HPCA Agent](#) on page 90
- [Importing Devices](#) on page 88
- [Managing Jobs](#) on page 92
- [Managing Virtual Machines](#) on page 104
- [Controlling Devices Remotely](#) on page 111
- [Managing Operating Systems](#) on page 117

Managing Directory Policies

From the Directories tree on the Management tab, you can view the objects in your configured directory services. See [Configure Directory Services](#) on page 34. You can view the properties of an object, create its policies, and view its entitlementments.







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 2 Directory Object View



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

Table 6 Actions Available from the Drop-Down Menu

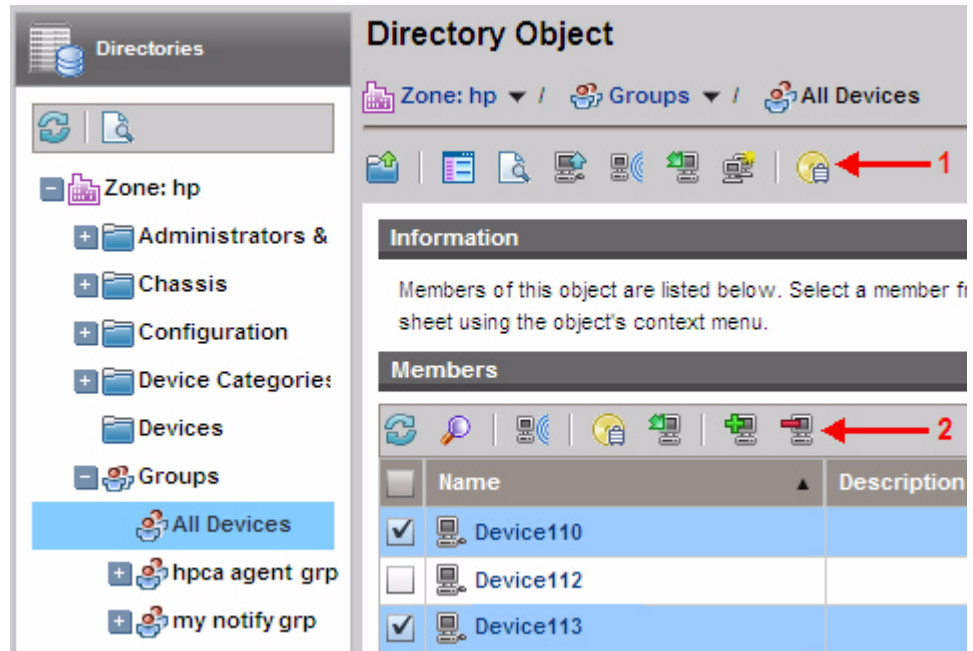
Icon	Action	Description
	View/Edit Properties	View or edit the properties of this child object in a new browser window. See Directory Object View on page 78.
	Create a Job	Create a Notify or DTM job for this object. See Managing Jobs on page 92.
	Remote Control	Access a managed device remotely. See Controlling Devices Remotely on page 111
	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 90.
	OS Management	Deploy an operating system, or perform a one-time hardware maintenance operation. See Managing Operating Systems on page 117.
	Delete this Directory Object	Delete this object from the HPCA database. See Importing Devices on page 88.

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 3](#) on page 80, the All Devices group is selected.

Figure 3 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 4](#) on page 81).

Figure 4 Directory Object Properties Window

Directory Object [?]


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 94 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 104.

Search for an Object


The Enterprise Manager 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:

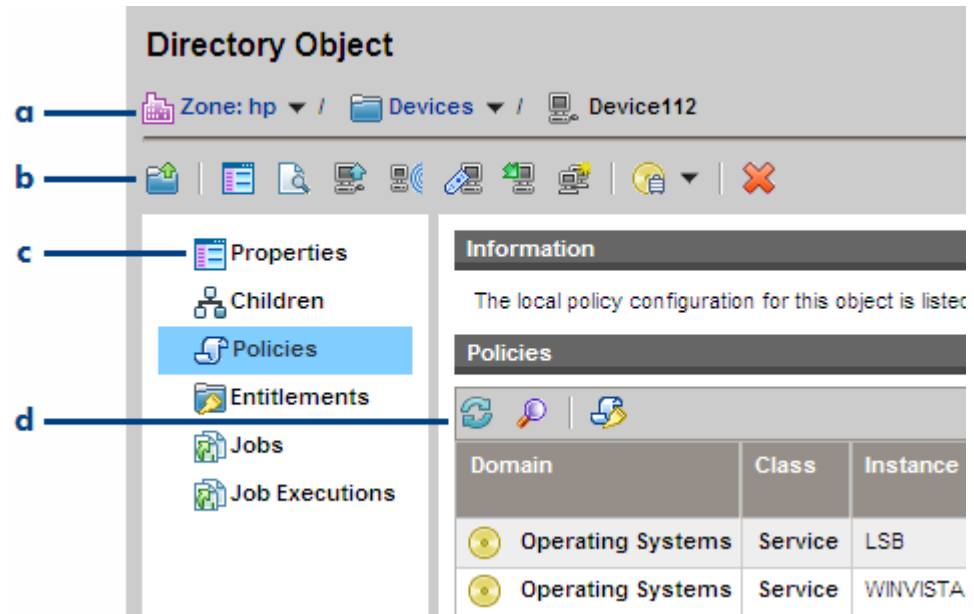
- 1 From the Management tab, **Directories** area, click the Search Directories  button.
- 2 From the Directory Search box, you can define the following parameters:
 - Specify the distinguished name (DN) for the search by selecting an item in the left navigation menu.
 - Select the **Scope** of the search: 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. To configure the list of available attributes, see [Specify Console Settings](#) on page 43.

 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 4](#) on page 81), you can manage the local policy configuration for an object.


Figure 5 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 80)

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.

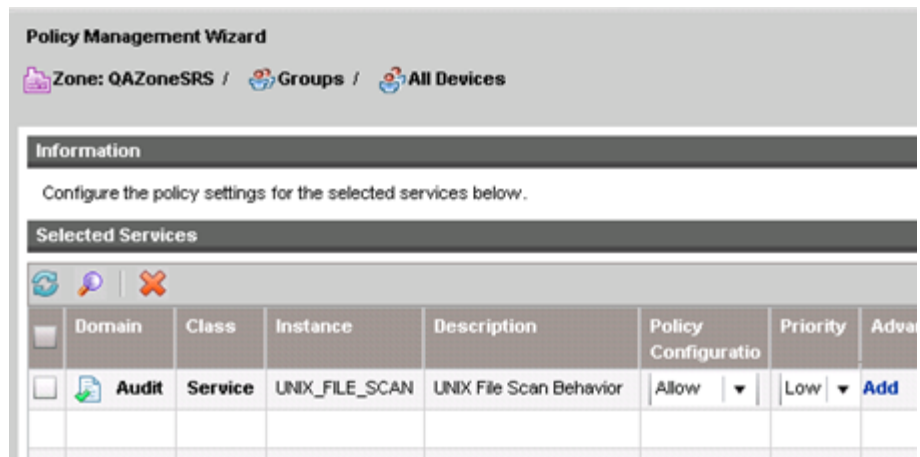
In our example we will create a policy for one device.

[Figure 5](#) on page 84 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 Enterprise Manager 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 Enterprise Manager, 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.

You will only see information here if you have enabled Reporting Server Integration. To do this, see [Integrate the Reporting Server](#) on page 51. For information on the reports, see the *Reporting Server Guide*.




For the Reporting tab to show summary reports, you must enable **Use Portal for Logon Authentication** on the Reporting Server. This option is disabled by default.


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 104.
- 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 Enterprise Manager 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 92) 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 Enterprise Manager users.
- The **My Jobs** category lists jobs submitted by the Enterprise Manager 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 Enterprise Manager:

Table 7 Types of Jobs

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



In an HPCA Core installation, you can create and manage DTM jobs by using the Enterprise Console. This capability is automatically configured and is available out of the box.

In an HPCA Enterprise (CAE) classic component-based installation, however, special configuration steps are required. See [DTM Jobs in an HPCA Classic Installation](#) on page 269 for more information.

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 Enterprise Manager 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 8 Jobs Table Controls

Icon	Description
	Refresh data
	Show/Hide filter input
	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 100 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 94

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 95.

- 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 98.

The Job Details window contains slightly different information for Notify jobs. See [Job Details for Notify Jobs](#) on page 97.

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 9 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 94

- 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 98.

The Job Details window contains slightly different information for DTM jobs. See [Job Details for DTM Jobs](#) on page 96.

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 97).

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 99.

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 10 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 97 or [Job Details for DTM Jobs](#) on page 96 for additional information. See [Job Execution States](#) on page 99 for additional information about the status of each job.

Job Execution States

Enterprise Manager 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 11 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

Table 11 Job Execution State Descriptions


State	Description
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 90. To create a new OS deployment job, see [Managing Operating Systems](#) on page 117.

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 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 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 [Create Job Action Templates](#) on page 47 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 95 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.

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 server. Target devices that already have the deleted job can still execute the job until they synchronize with the HPCA server.

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.

CAE installation: C:\Program Files\HP\HP BTO Software\CM-EC\tomcat

Core and Satellite: 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 Enterprise Manager 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 12 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
rmpPort	3466	Portal server port to which to connect
rmpUser	SYSTEM	
rmpPassword		Not shown here for security
userDS	""	User directory to which to connect

Table 12 Parameters for Device Resolution Service for DTM Jobs

Parameter	Default Value	Comment
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.

CAE installation: C:\Program Files\HP\HP BTO Software\CM-EC\tomcat

Core and Satellite: 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.

Managing Virtual Machines

The Enterprise Manager 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 4](#) on page 81.
- 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 Enterprise Manager 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 7](#) on page 107.

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

Figure 6 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 7 List of Virtual Machines Hosted by an ESX Server

Information

Virtual Machines available on this Virtual Hosting Server are displayed below. Use the toolbar options below for additional management options.

Virtual Machines

Name	Operating System	# CPUs	Memory Size (MB)	Status	VM Tools Status
vm1	Microsoft Windows 2000 Advanced Server	1	828	Powered on	Not running
vm2	Microsoft Windows Server 2003, Standard Edition	4	16384	Powered on	Current version running
vm3	Red Hat Enterprise Linux 3	1	2048	Powered on	Not running
vm4	Microsoft Windows Server 2003, Enterprise Edition	1	10228	Powered off	Not installed
vm5	Microsoft Windows 2000 Advanced Server	1	1052	Powered off	Not running
vm6	Novell NetWare 5.1	1	408	Suspended	Not running
vm7	Microsoft Windows Server 2003, Standard Edition	1	4096	Suspended	Not installed
vm8	Microsoft Windows Server 2003, Standard Edition	1	4076	Powered off	Not installed

8 of 8 records shown

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













Table 13 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 14 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 104 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 Enterprise Manager 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 Enterprise Manager 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 72 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 112 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 Enterprise Manager 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 112

[Configure Remote Control](#) on page 72

[Remote Control Auditing](#) on page 116

Requirements for Remote Connections

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

- 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 Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager 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 Enterprise Manager (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 Enterprise Manager, 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 Enterprise Manager 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 Enterprise Manager and the target devices must be joined to the same domain.
- The system where you are accessing the Enterprise Manager (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 Enterprise Manager 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 Enterprise Manager, 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 – Enterprise Manager 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 Enterprise Manager

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 111

[Configure Event Auditing](#) on page 73

[Using Reports](#) on page 235

Managing Operating Systems

You can use the operating system (OS) management features of the Enterprise Manager 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 118
- [Prerequisites for OS Management](#) on page 119
- [Deployment Scenarios](#) on page 120
- [How it Works](#) on page 124
- [Deploy an OS Image](#) on page 125
- [View the Status of OS Management Activities](#) on page 131
- [Creating a CD/DVD for OS Deployment](#) on page 131

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 Enterprise Manager, 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.
- The Proxy Server used to deploy the service containing the operating system images to the target devices is installed and properly configured.

Refer to the *HPCA Proxy Server Installation and Configuration Guide* for more information about installing this server and how to co-locate it with the Configuration Server.

- The HPCA OS Manager must be installed and properly configured.

Refer the *HPCA OS Manager System Administrator User Guide* for additional information.

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 Enterprise Manager 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 15 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.

Table 15 Deployment Scenarios

Device State	Instructions for deployment
Bare-metal (no OS installed)	<p>If the device was previously managed (for hard drive recovery, for example):</p> <ul style="list-style-type: none">• 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 93).

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 Enterprise Manager:

- 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 90.

- 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 119 and [Deployment Scenarios](#) on page 120.

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 128.
 - **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 128.
 - **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 128.
- 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 92).

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 120 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 120 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 120 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 Enterprise Manager:
 - a On the Management tab, follow the instructions for [Deploy an OS Image](#) on page 125
 - 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 Enterprise Manager, 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 92).

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 93).

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 124.

Creating a CD/DVD for OS Deployment



This topic pertains only to an HPCA Classic installation.

You can use the following script to download operating system image services that have been uploaded to the Configuration Server database:

```
<OSMInstallDir>\OSManagerServer\modules\osm-download.tcl
```

In this case, `<OSMInstallDir>` is the installation directory for the OS Manager. By default, this is:

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

These services can then be used to create a CD or DVD for operating system deployment.

The script syntax is as follows:

```
nvdkit.exe <script-location>\osm-download.tcl -host  
<hostname> -cspport <CS-port> -port <Proxy-port> -user  
<userID> -pass <password> -logfile <logfile> -outdir  
<out-dir> -service <services>
```

- `<script-location>`: OS Manager Server installation \modules directory (see above)
- `-host <hostname>`: Configuration Server hostname (default localhost)
- `-cspport <CS-port>`: Configuration Server port (default 3464)
- `-port <Proxy-port>`: CA Proxy server port (default 3466). Downloading resources from a Proxy server will take additional time.
- `-user <userID>`: Configuration Server user ID
- `-pass <password>`: Configuration Server user password
- `-outdir <out-dir>`: Output folder for the downloaded service
- `-logfile <logfile>`: Log file for this script. By default, this is:
.\osm-download.log
- `-service <services>`: A space separated list of services. At least one service is required. Service name must be in the following format:

PRIMARY.OS.ZSERVICE.SERVICENAME

For example:

PRIMARY.OS.ZSERVICE.EMCPET5 PRIMARY.OS.ZSERVICE.MY_OS

The executable, `nvdkit.exe`, is located in the default OS Manager Server installation directory:

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

The following example will use the default installation location and default Configuration Server user name credentials to run the script and download the EMCPET5 and MY_OS services to the `c:/tmp/CDDeploy/out` directory.

```
nvdkit.exe "C:\Program  
Files\Hewlett-Packard\HPCA\OSManagerServer\modules\osm-download.  
tcl" -host localhost -port 3466 -user admin -pass secret -logfile  
c:/tmp/CDDeploy/osm-download.log -outdir c:/tmp/CDDeploy/out  
-service PRIMARY.OS.ZSERVICE.EMCPET5 PRIMARY.OS.ZSERVICE.MY_OS
```

The executable nvdkit.exe and the script osm-download.tcl can be copied to another device, if required. Running the script and connecting to a Configuration Server with a CA Proxy Server enabled will take much longer to download resources than downloading directly from the Configuration Server database.

5 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 136
- [HPCA and HP Live Network](#) on page 142
- [License Requirements](#) on page 142
- [Software Prerequisites](#) on page 143
- [How Security and Compliance Management Works in HPCA](#) on page 144
- [Configuring Security and Compliance Management](#) on page 152
- [Common Security and Compliance Management Tasks](#) on page 152
- [Advanced Topics](#) on page 162
- [More Information about Security and Compliance Management](#) on page 173

Introduction

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

- [Vulnerability Management](#) on page 136
- [Compliance Management](#) on page 138
- [Security Tools Management](#) on page 141

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 16 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 16 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 16 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 17 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 17 Compliance Management Terms

Term	Definition
SCAP	<p data-bbox="468 256 1262 453">Security Content Automation Protocol (pronounced ess-kap) 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 data-bbox="468 465 1043 493">SCAP incorporates the following specifications:</p> <ul data-bbox="468 513 1262 944" style="list-style-type: none"><li data-bbox="468 513 1129 541">• CVE (see Vulnerability Management on page 136)<li data-bbox="468 562 715 590">• CCE (see above)<li data-bbox="468 611 1262 701">• Common Platform Enumeration (CPE), a naming convention for hardware, operating system (OS), and application products<li data-bbox="468 722 1248 847">• Extensible Configuration Checklist Description Format (XCCDF), an XML specification for structured collections of security configuration rules used by OS and application platforms<li data-bbox="468 868 1143 895">• OVAL (see Vulnerability Management on page 136)<li data-bbox="468 916 1143 944">• CVSS (see Vulnerability Management on page 136) <p data-bbox="468 965 1262 1020">Because SCAP uses XML-based standards, SCAP content is both human and machine readable.</p> <p data-bbox="468 1038 1248 1128">NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD).</p> <p data-bbox="468 1142 1219 1170">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 Enterprise Manager—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 [Configure the HP Live Network Settings](#) on page 53 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.
- Your Reporting Server must be properly configured to provide the reports used to populate the dashboards.
- Reporting must be enabled in the Enterprise Manager. See [Integrate the Reporting Server](#) on page 51.
- 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.

- To use the Patch Management dashboards and reports, you must also install the HPCA Patch Manager in your environment. Refer to the *HP Client Automation Patch Manager Installation and Configuration Guide (Patch Manager Guide)* for more information.



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 8](#) on page 147.

You can use the Enterprise Manager 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 Enterprise Manager 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 175.

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

Table 18 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 62.



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 Reporting 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 Reporting database.

Figure 8 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 Reporting 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 170).

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 the Reporting Server 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.

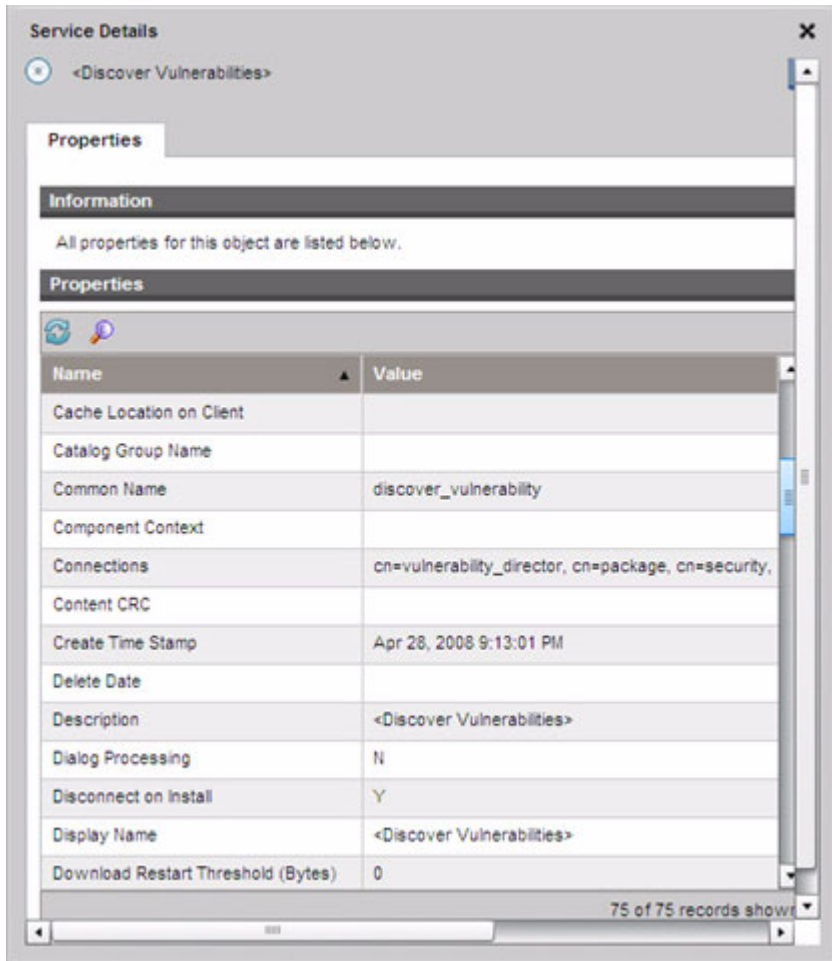
Although the name of the service changes, any entitlements that you have established do not change.

To view the scanning services:

- 1 Sign in to the Enterprise Manager.
- 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 87.






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 155. 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 153 for more information.

Configuring Security and Compliance Management

See [Security and Compliance Management Configuration](#) on page 52 .

Common Security and Compliance Management Tasks

This section contains information about the following tasks:

- [Update HP Live Network Content](#) on page 152
- [Schedule or Trigger a Scan](#) on page 153
- [View the Results of a Scan or Update](#) on page 157
- [Find Vulnerability Remediation Information](#) on page 157
- [Find Information about Compliance Failures](#) on page 159
- [Find Information About Security Tools](#) on page 161

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 configuration page to configure the Enterprise Manager to periodically download updated content, or use the Update Now tab to initiate an immediate update from the HP Live Network subscription site.

See [Configure the Live Network Updates](#) on page 59 for detailed instructions.

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

See [Use the Command Line Utility](#) on page 162 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 Enterprise Manager 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 154.

- 2 Schedule or trigger a scan from the Enterprise Manager by creating a job using the Security Connect job action template. See [Create an HPCA Job to Schedule or Trigger a Scan](#) on page 155.


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 156.

For information about how HPCA performs a scan, see [Scanning Services in Detail](#) on page 149.

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 Enterprise Manager, 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 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 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 95 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 92.

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 Enterprise Manager 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 235 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 175 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 246 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 HP Client Automation Patch Manager to entitle the pertinent devices to that patch. Refer to the *HP Client Automation Patch Manager Installation and Configuration Guide (Patch Manager Guide)* for detailed instructions.

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 19

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 217
- [Security Tools Management Reports](#) on page 244

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 162
- [Run the HP Live Network Connector Manually](#) on page 168
- [Move HP Live Network Content from a Test Environment to a Production Environment](#) on page 170

Use the Command Line Utility

As an alternative to using the HP Live Network page under on the Configuration 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:

CAE: `<InstallDir>\VulnerabilityServer\bin`

Core and Satellite: `<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 167). 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 [Log Files](#) on page 74 for more information.

See [Examples](#) on page 167 for typical uses of the `content-update.bat` command.

Required Settings

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

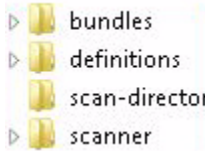


Any values that you specify on the command line override the stored configuration settings that were specified elsewhere (see [Stored Settings](#) on page 167). If you do not specify a value for a particular setting, the stored configuration setting is used.

Table 20 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 Configure the HP Live Network Settings on page 53.</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 NetworkUpdates tab on the Live Network configuration page. See Configure the HP Live Network Settings on page 53.</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 162.</p>

Table 20 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 167). If you do not specify a value for a particular setting, the stored configuration setting is used.

Table 21 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: CAE: C:\Program Files\HP\HP BTO Software\LiveNetwork Core and Satellite: 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.

Table 21 Optional Settings for content-update.bat

Setting	Description
livenetwork_proxy_ http_server	HTTP proxy server used to connect to the HP Live Network download site. This option must have the following form: <http https>://<host>:<port>
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 oracle or sqlserver). 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 tabs are used by default:

Table 22 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>	Databases tab
<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>	Settings tab
<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>	Databases tab

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 server hosting the Enterprise Manager 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 server hosting the Enterprise Manager. 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 server hosting the Enterprise Manager.
- 4 Update the HP Live Network content from the file system on the server hosting the Enterprise Manager. See [Update HP Live Network Content](#) on page 152.

When you execute the HP Live Network Connector, it creates the folder structure described under `content_path` in [Table 20](#) on page 163 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 Enterprise Manager.

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://bsaen-dist.hp.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 Enterprise Manager 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 Enterprise Manager. 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 configuration page Settings 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 145.

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.
 - ▶ This process will not work unless the Reporting database Configuration and Configuration Server Information on the Databases tab of the Live Network configuration page in the Enterprise Manager are correct.

There are two ways to do this:

- **Method 1:** Use the Enterprise Manager
 - a Click the **Configuration** 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 [Configure the HP Live Network Settings](#) on page 53 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 162 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 Enterprise Manager:

- [Using the Dashboards](#) on page 175
- [Using Reports](#) on page 235
- [Configure the HP Live Network Settings](#) on page 53

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>

6 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 176
- [HPCA Operations Dashboard](#) on page 182
- [Vulnerability Management Dashboard](#) on page 188
- [Compliance Management Dashboard](#) on page 207
- [Security Tools Management Dashboard](#) on page 217
- [Patch Management Dashboard](#) on page 226

Dashboard Overview

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

- The [HPCA Operations Dashboard](#) on page 182 shows you how much work is being done by the HPCA infrastructure.
- The [Vulnerability Management Dashboard](#) on page 188 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 207 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 217 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 226 shows you information about any patch vulnerabilities that are detected on the devices in your network

Each dashboard includes two views:

Table 23 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 [Configure the Dashboards](#) on page 65 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 the Reporting Server displays the report.


- ▶ The information displayed in the dashboards comes from HPCA reports. Your Reporting Server must be properly configured to provide these reports. In a Core and Satellite installation, this is done automatically. If you are using a CAE installation, you must execute the Oracle or SQL Server prerequisite scripts (refer to the Reporting Server Guide for instructions).

Also, Reporting must be enabled in the Enterprise Manager. See [Integrate the Reporting Server](#) on page 51.

- ▶ Before you can view data in the dashboards, you must enable the following report packs on the Reporting Server: Patch Management, Inventory Management, Vulnerability Management, Compliance Management, and Security Tools Management. Refer to the *Reporting Server Guide* for instructions.

- ▶ The information displayed in the Patch Management dashboard comes from the Patch Manager. Both the Patch Manager and the Inventory Manager must be properly configured and operational before the Patch Management dashboard can display data. Refer to the *Patch Manager Guide* and *Inventory Manager Guide* for additional information.

- ▶ Patch Manager features are only available for customers who purchase a license for Patch Manager or a bundle or suite that includes Patch Manager.

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 9 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. For more information, refer to the *Reporting Server Guide*.

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 24 Dashboard Pane Actions













Icon	Description
	Display the information in chart format.
	Display the information in grid format.
	Display the legend for this chart.
	Refreshes the data from its source. Click the refresh icon in an individual pane to refresh the data for that pane. Click the refresh icon in the upper right corner of the dashboard to refresh all panes. The dashboard panes are not automatically refreshed if your Enterprise Manager 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 on the Reporting Server. 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.

Table 24 Dashboard Pane Actions

Icon	Description
	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 10 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 Enterprise Manager. 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 255 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 Enterprise Manager. See [Cannot Refresh Page Using F5](#) on page 252 for more information.

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

Table 25 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 189, 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

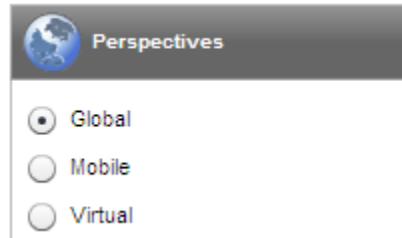
Perspectives enable you to limit the information displayed in the dashboard panes to certain types of devices. The following three perspectives are available by default:

- 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 Filters and Perspectives](#) on page 265 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.

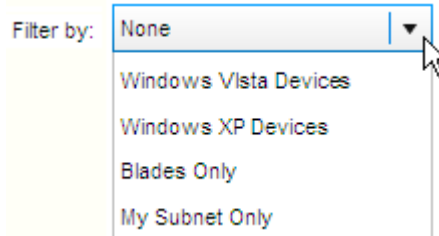
The following dashboard panes are not affected by perspectives:

- [Historical Vulnerability Assessment](#) on page 191
- [Historical Compliance Assessment](#) on page 211
- [Microsoft Security Bulletins](#) on page 231
- [HP Live Network Announcements](#) on page 198

When you select a perspective, it is applied to all the dashboard panes in the Enterprise Manager 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 Filters and Perspectives](#) on page 265.

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 183

[Service Events](#) on page 184

The Executive View also includes the following pane:

[12 Month Service Events by Domain](#) on page 186

All of these panes are visible by default. You can configure the dashboard to show or hide any of these panes. See [Configure the Dashboards](#) on page 65 .

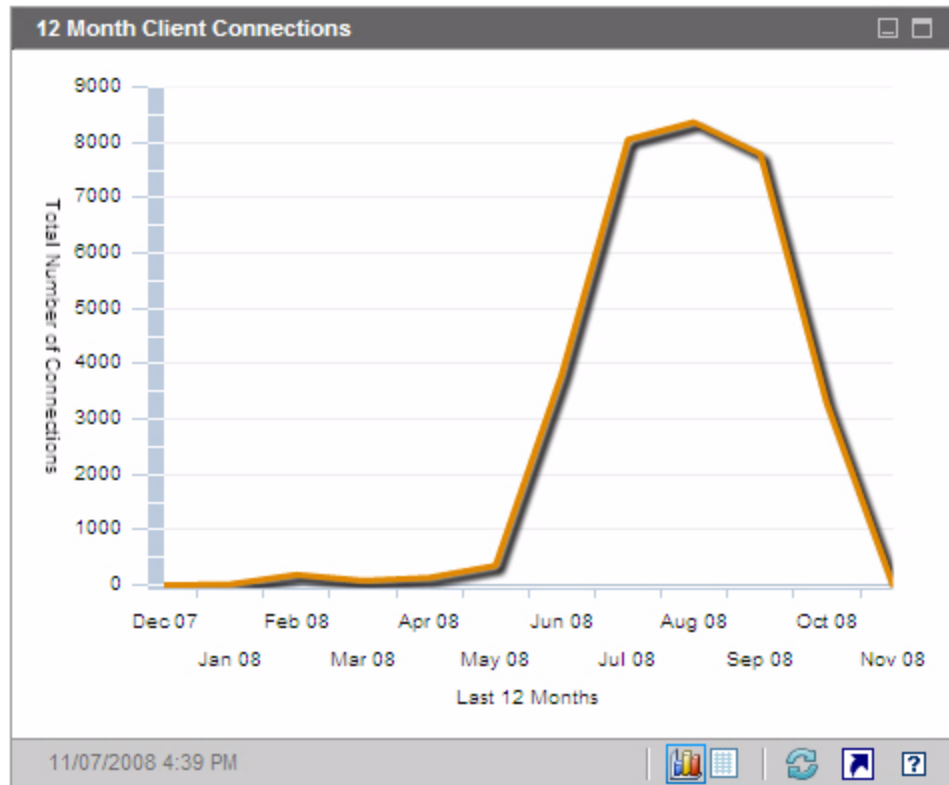


When you click HPCA Operations in the left navigation pane, the HPCA Operations home page is displayed. This page contains statistics and links to pertinent reports.

Client Connections

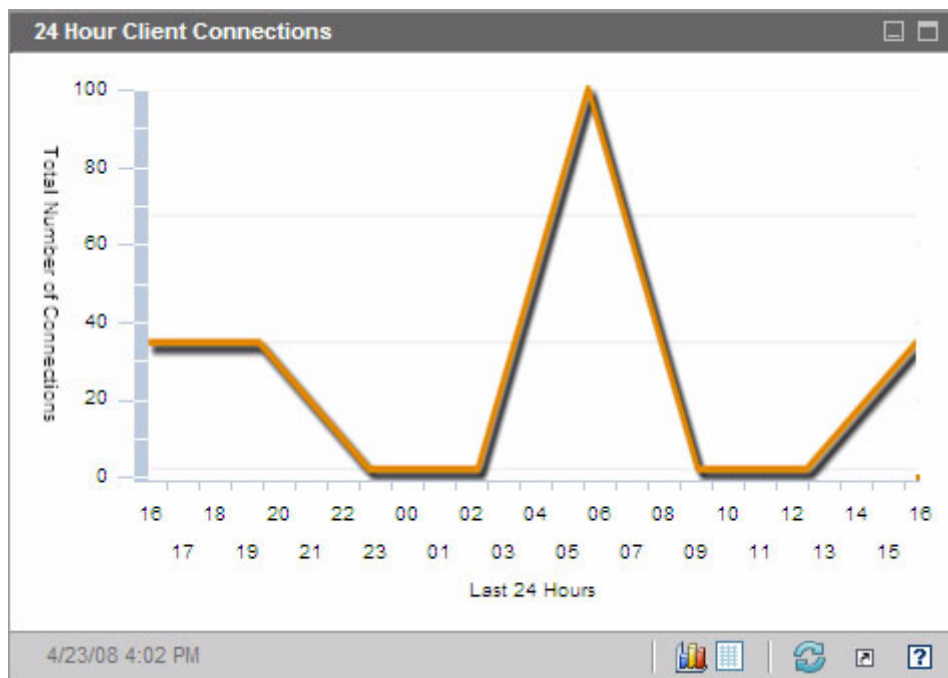
The chart view of this pane shows you the number of HPCA agent client connections that have occurred over the last twelve months (Executive View) or 24 hours (Operational View). When you rest the cursor on a data point, you can see the total number of connections for that month or hour.

Figure 11 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 12 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. For more information, refer to the *Reporting Server Guide*.

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

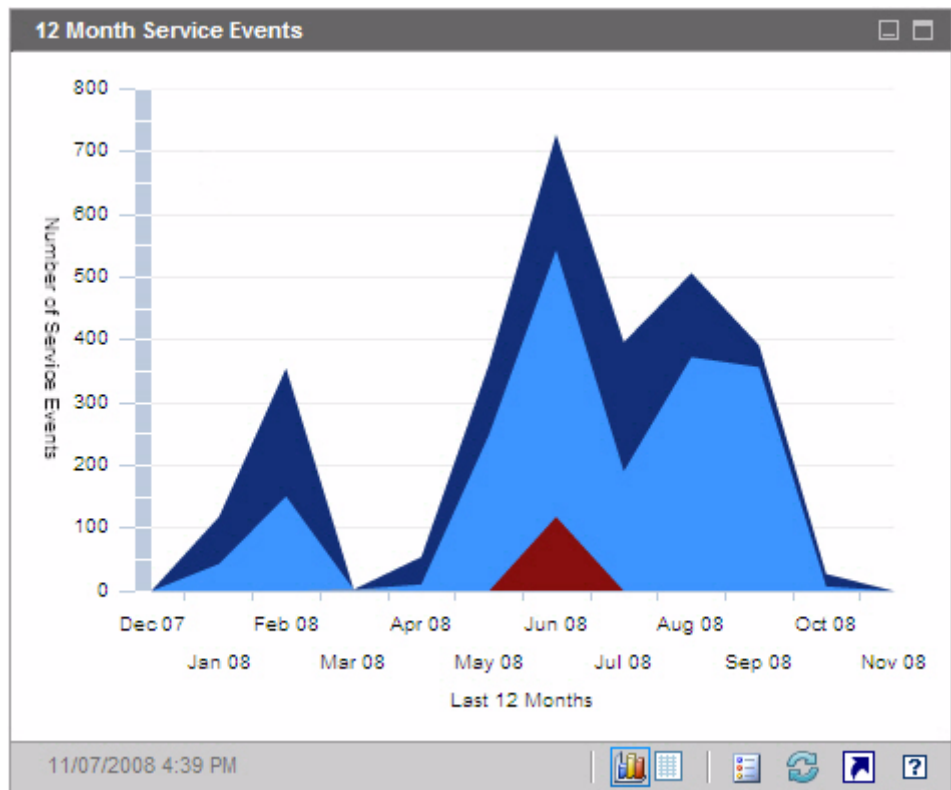
Service Events

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

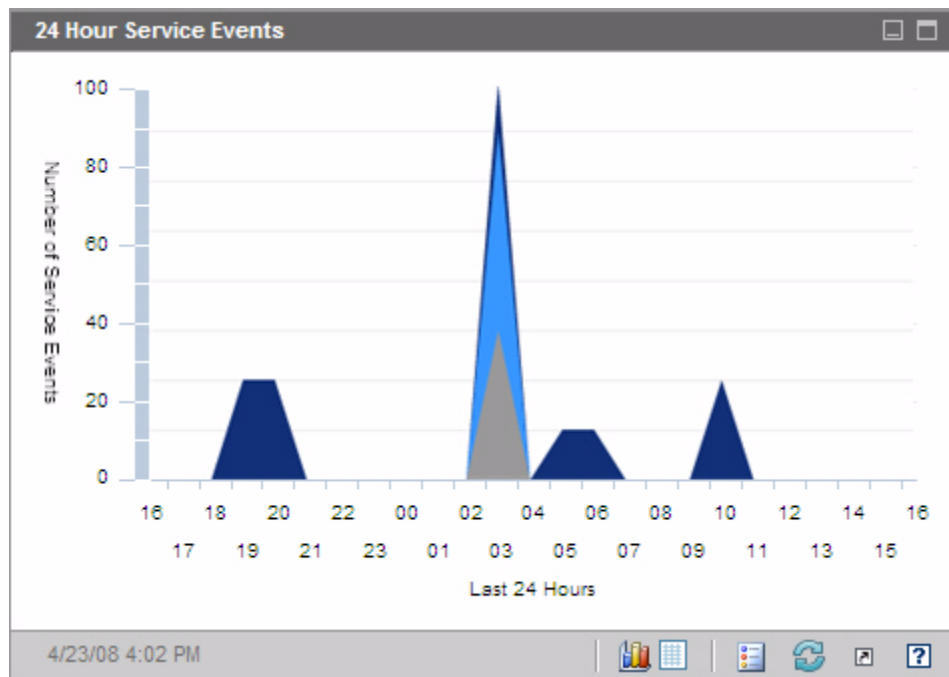
When you rest the cursor on a data point, you can see the number of service events that were completed during a particular month or hour.

Figure 13 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 14 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. For more information, refer to the *Reporting Server Guide*.

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

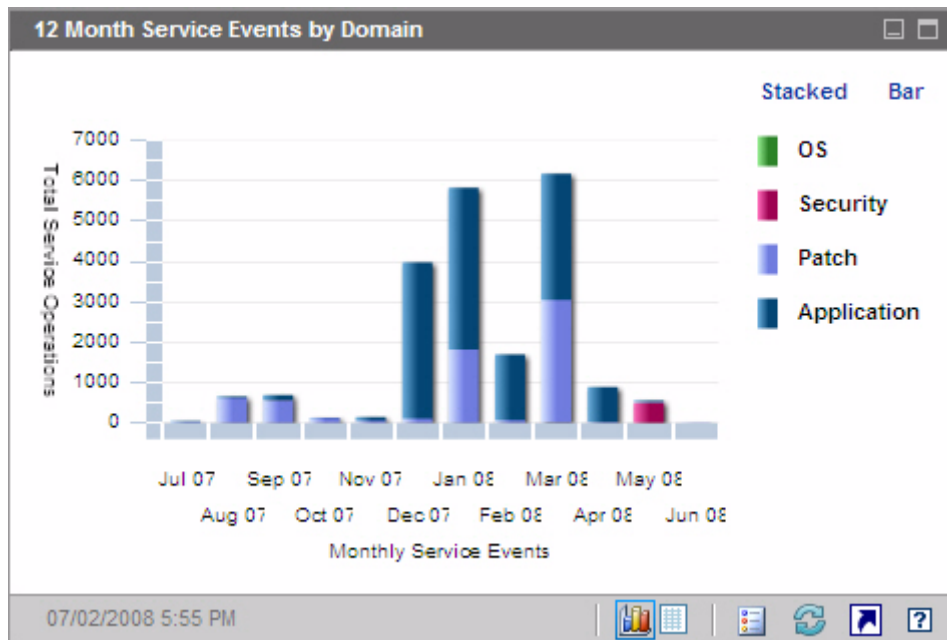
The chart view of this pane shows you how many of each of the following services that HPCA performed during each of the last 12 months:

- 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 15 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 135.

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 26 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 189
- [Vulnerability Impact by Severity \(bar chart\)](#) on page 199
- [Vulnerability Impact](#) on page 193
- [Historical Vulnerability Assessment](#) on page 191

The Operational View includes the following four information panes:

- [HP Live Network Announcements](#) on page 198
- [Most Vulnerable Devices](#) on page 201
- [Most Vulnerable Subnets](#) on page 202
- [Top Vulnerabilities](#) on page 204

You can configure the dashboard to show or hide any of these panes. See [Configure the Dashboards](#) on page 65.



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)

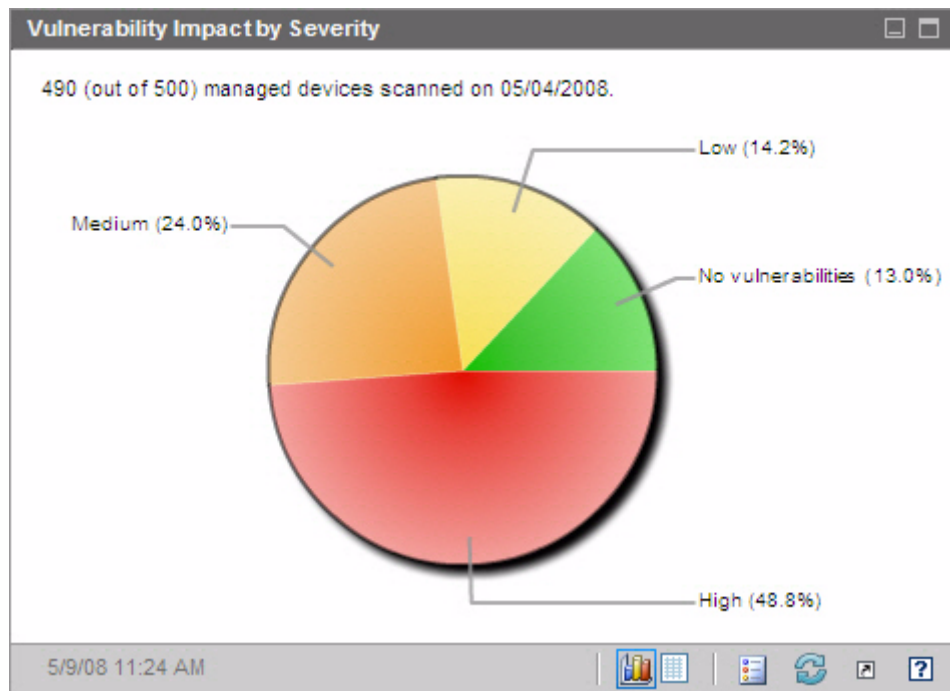
The chart view for this pane shows you the percentage of scanned devices in the enterprise that fall into each of the following five categories based on the highest severity vulnerability detected on each device:

- High (red)

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

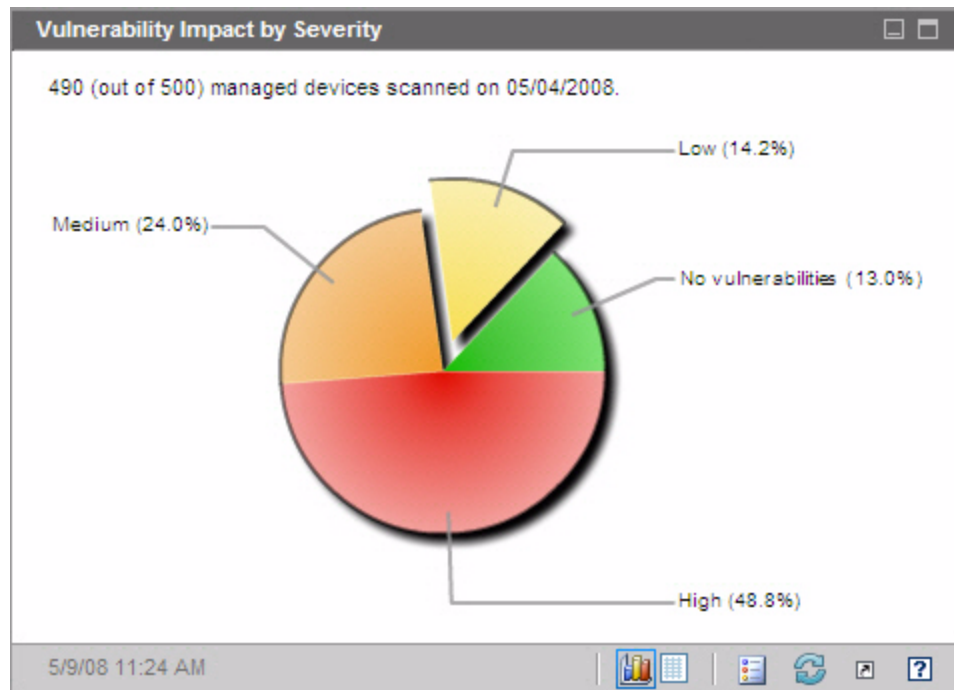
To see the number of devices in each severity category, rest the cursor on the corresponding sector of the pie chart.

Figure 16 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 by the Reporting Server. 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 17 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 175

[Vulnerability Management Dashboard](#) on page 188

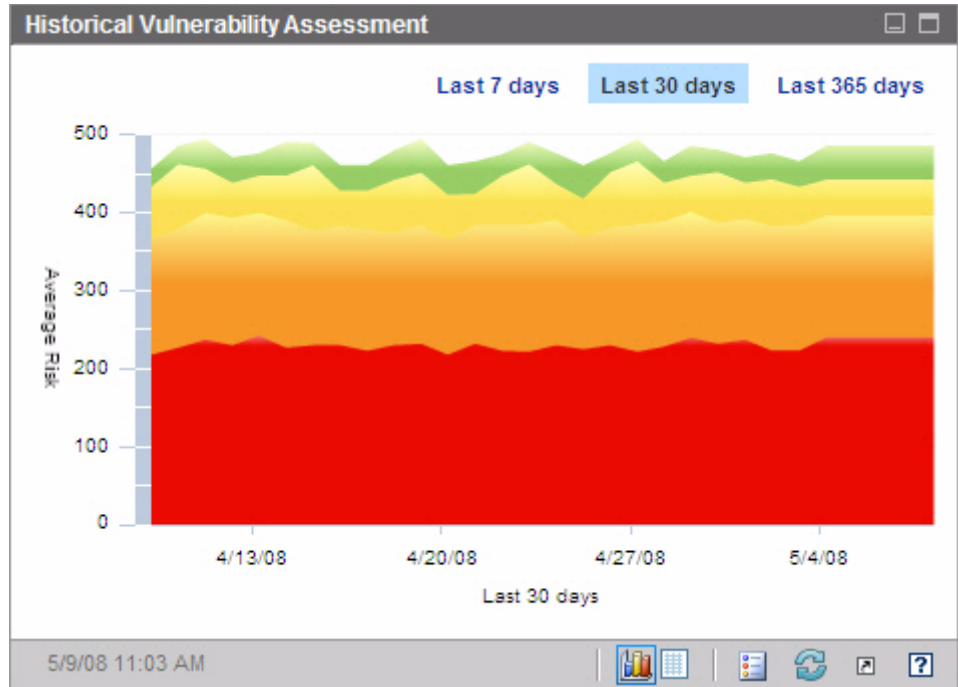
[Security and Compliance Management](#) on page 135

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 18 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 19 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 175

[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

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.

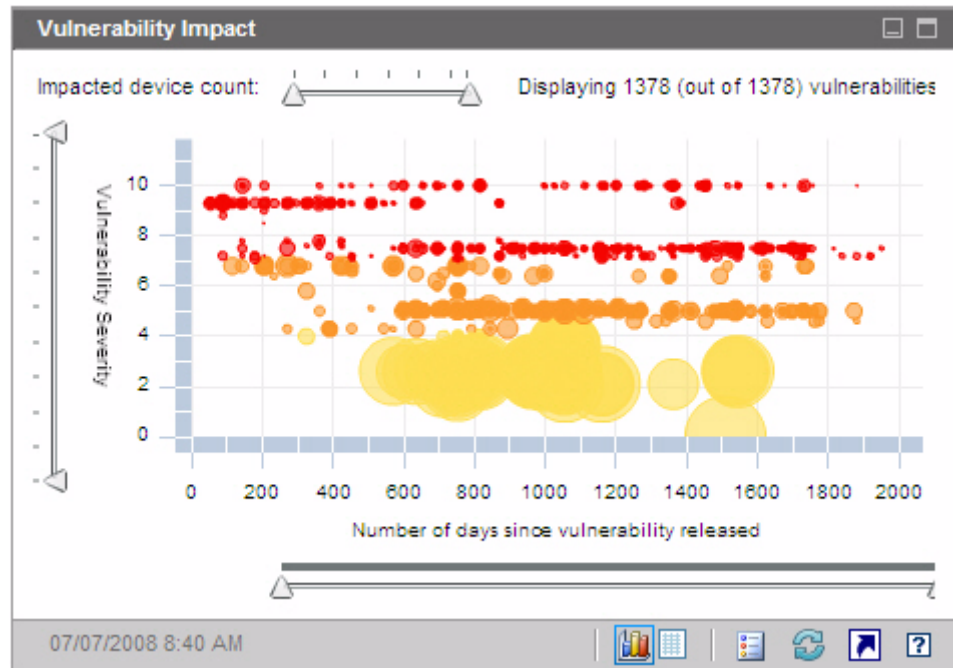
- Small yellow circles in the lower left portion represent issues that are of low severity, affect a smaller number of devices, and were published in the NVD relatively recently.
- An ideal chart would have no red bubbles in the upper right corner. This would imply that severe vulnerabilities are dealt 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 by the Reporting Server. 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 20 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.

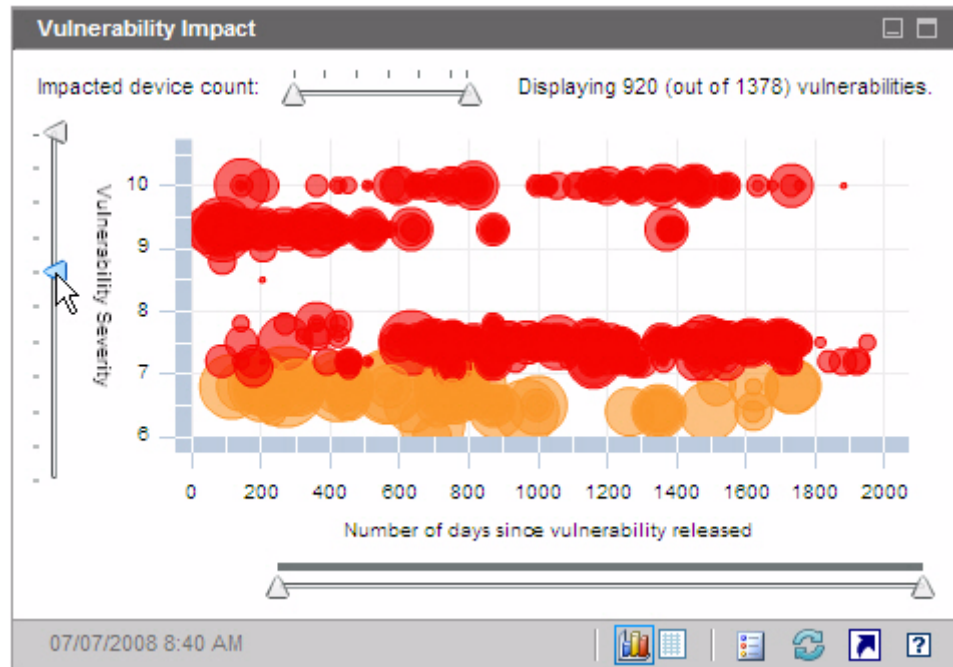
By default, the age span displayed is 45 days. You can specify this default value when you configure the Vulnerability Management dashboard. See [Configure the Dashboards](#) on page 65.

When the triangles (\triangle) 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.

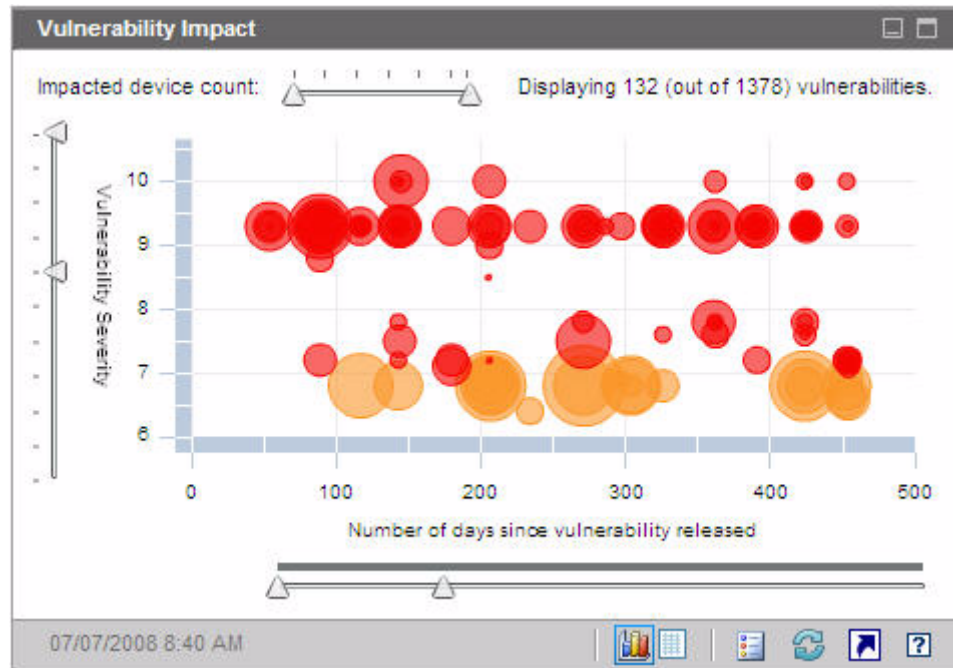
In the following example, vulnerabilities with a CVSS base score of 6 or greater are shown:

Figure 21 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 22 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 175

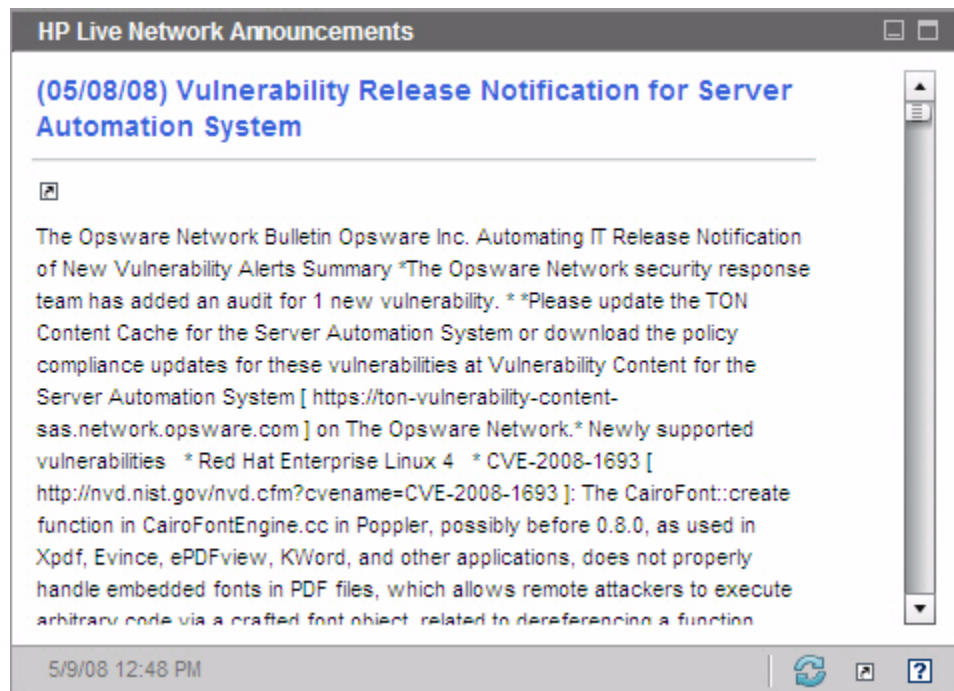
[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

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 [Configure the Dashboards](#) on page 65 for information about configuring your HP Live Network credentials.

Figure 23 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 [Configure the Dashboards](#) on page 65). You may also need to enable a proxy server (see [Configure the Connection to the HP Live Network Server](#) on page 54).

Related Topics:

[Using the Dashboards](#) on page 175

[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

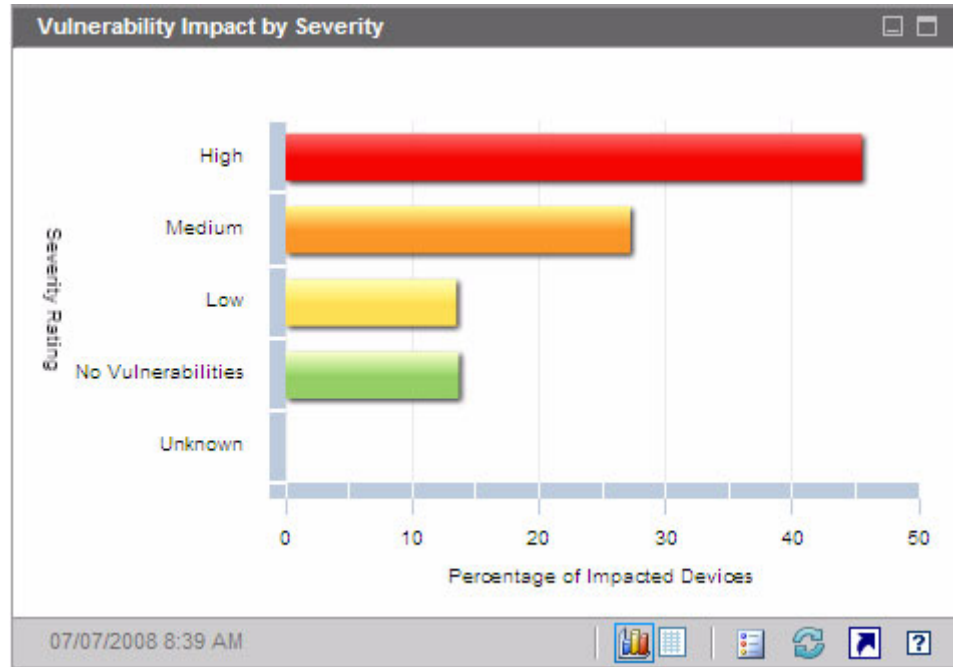
Vulnerability Impact by Severity (bar chart)

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 24 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 by the Reporting Server. 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 175

[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

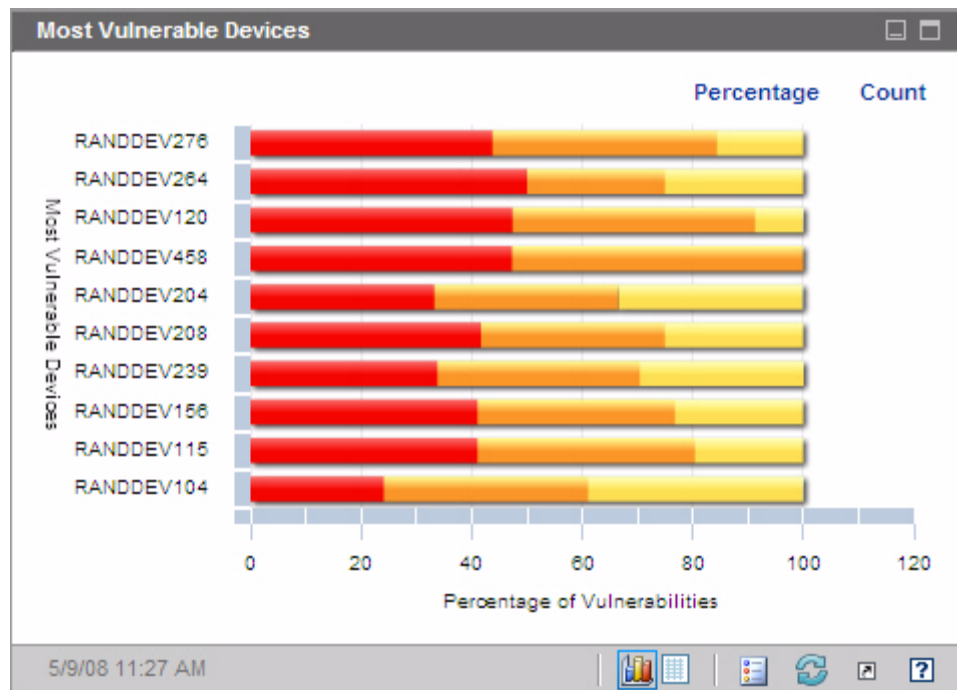
Most Vulnerable Devices

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 25 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 by the Reporting Server. 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 175

[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

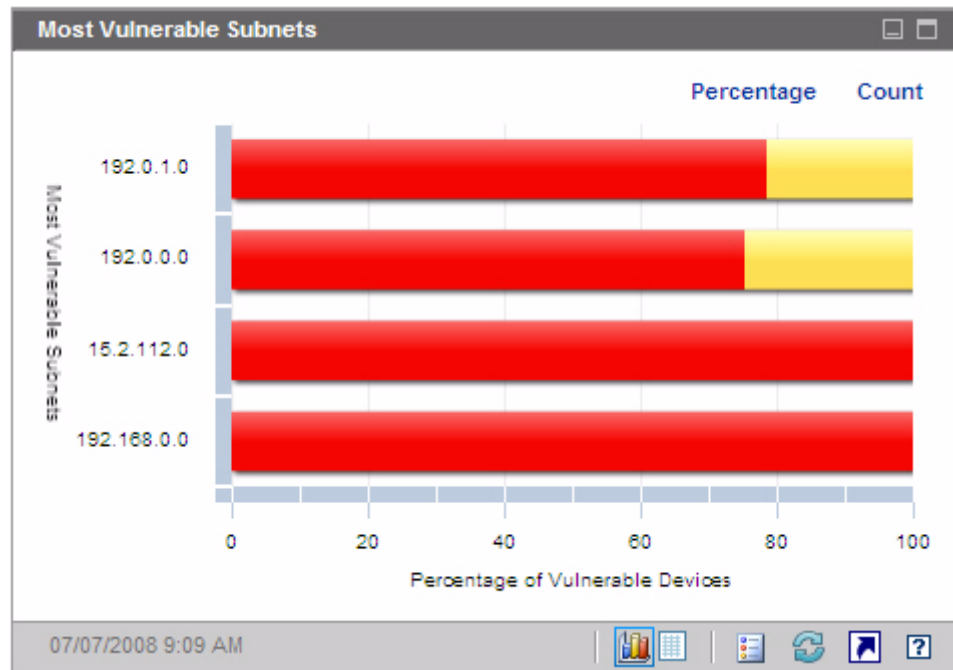
Most Vulnerable Subnets

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 [Configure the Dashboards](#) on page 65.

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 26 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 175

[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

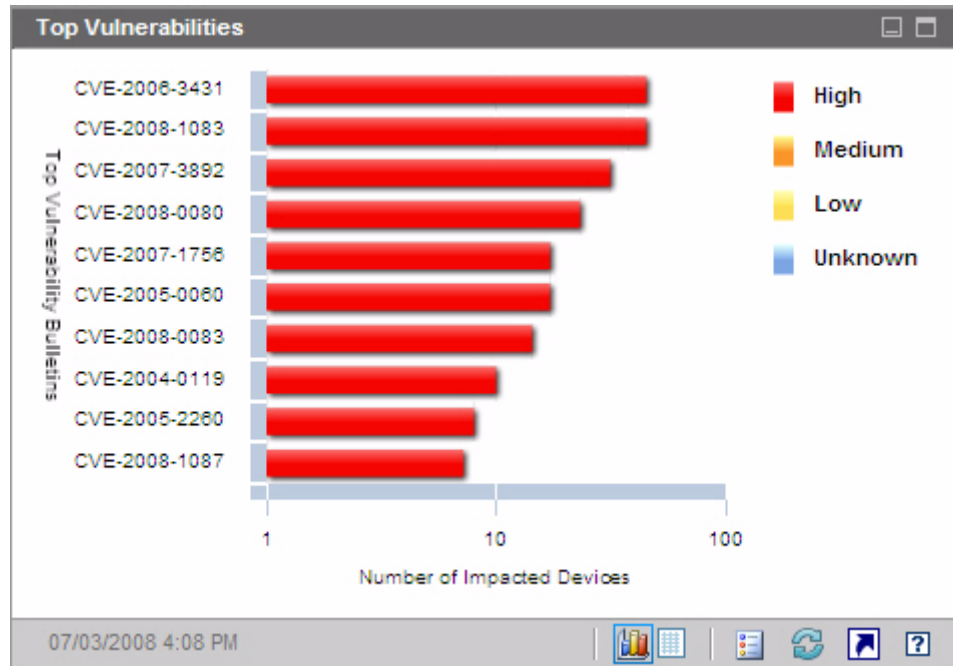
Top Vulnerabilities

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 27 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 28 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 by the Reporting Server. 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 175

[Vulnerability Management Dashboard](#) on page 188

[Security and Compliance Management](#) on page 135

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 135.

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 210
- [Compliance Status](#) on page 208
- [Historical Compliance Assessment](#) on page 211

The Operational View includes the following information panes:

- [Top Failed SCAP Rules](#) on page 213
- [Top Devices by Failed SCAP Rules](#) on page 215

You can configure the dashboard to show or hide any of these panes. See [Configure the Dashboards](#) on page 65 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.

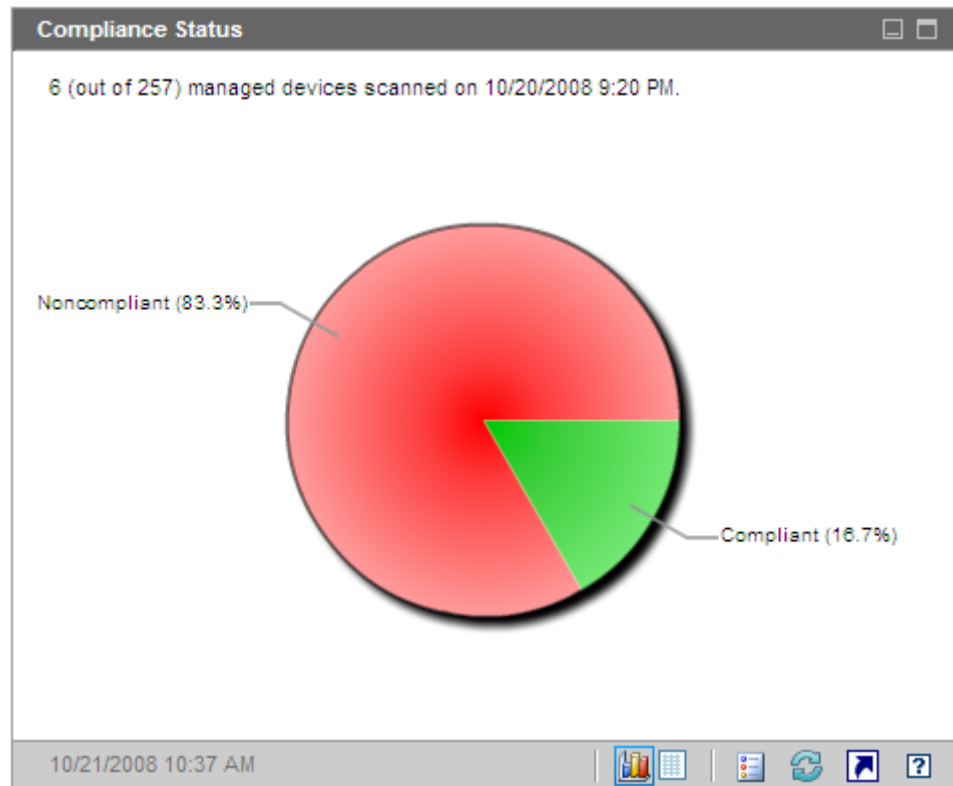
Compliance Status

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.

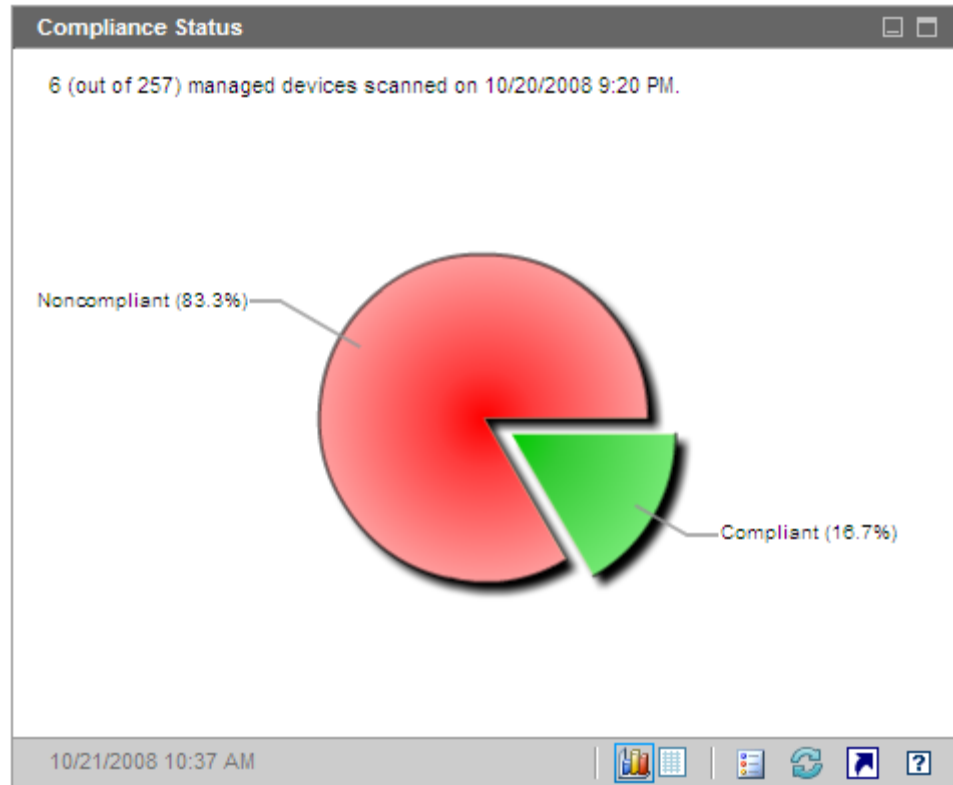
Figure 29 Compliance Status



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 by the Reporting Server. 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 30 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 175

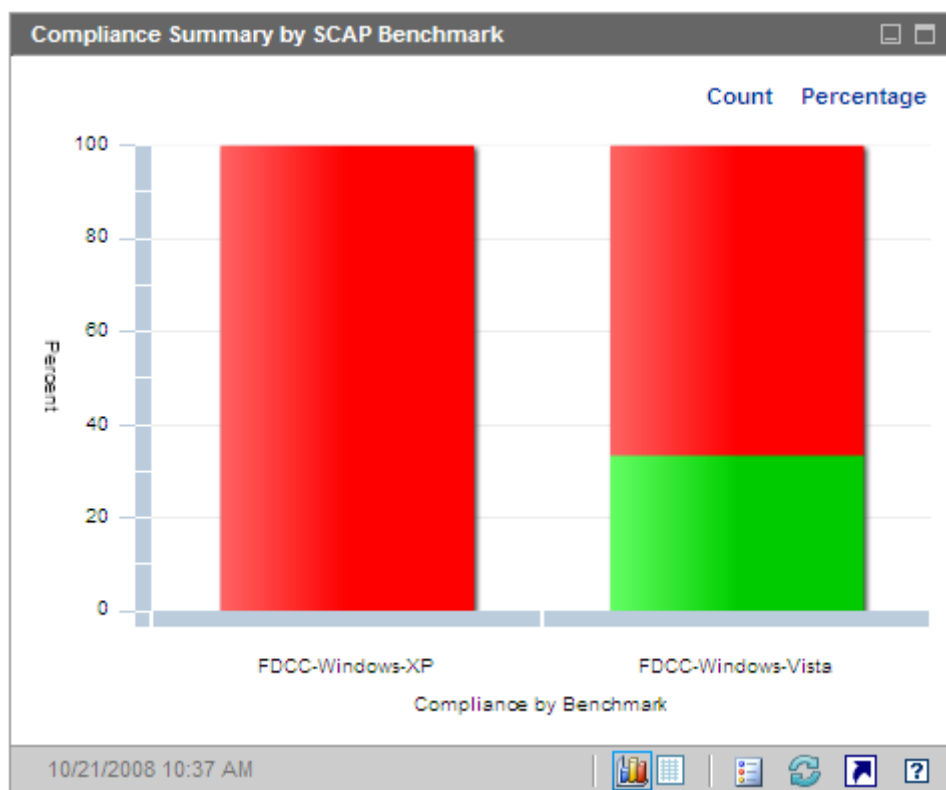
[Compliance Management Dashboard](#) on page 207

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:

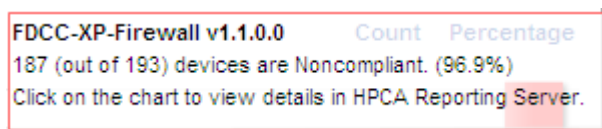
- Compliant devices (green)
- Noncompliant devices (red)

Figure 31 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 32 Tooltip



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 by the Reporting Server. 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 175

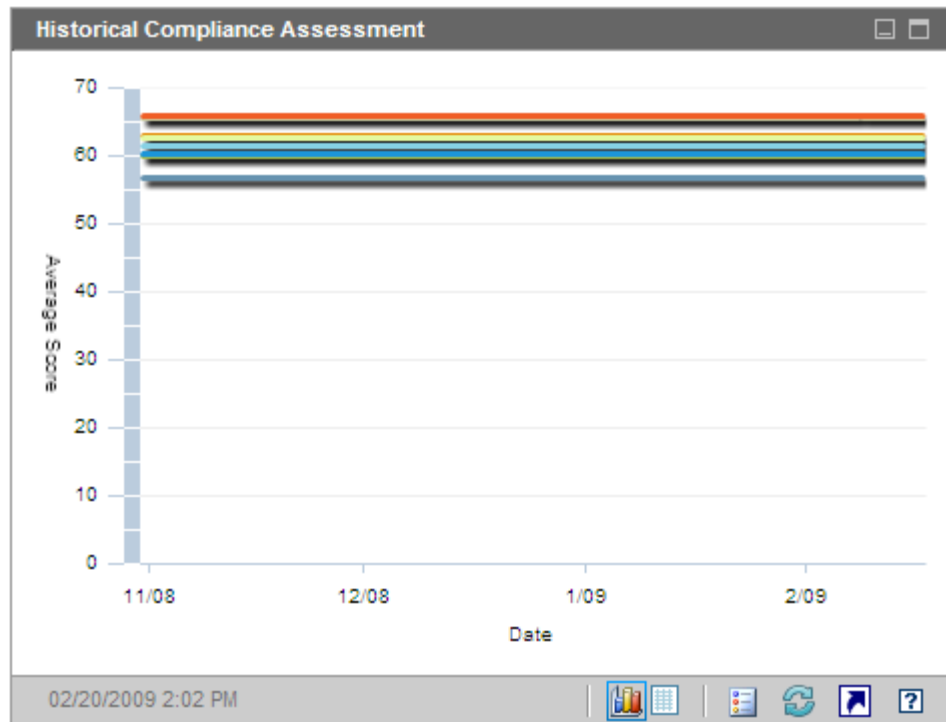
[Compliance Management Dashboard](#) on page 207

[Security and Compliance Management](#) on page 135

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 33 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 175

[Compliance Management Dashboard](#) on page 207

[Security and Compliance Management](#) on page 135

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 34 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 by the Reporting Server. 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 175

[Compliance Management Dashboard](#) on page 207

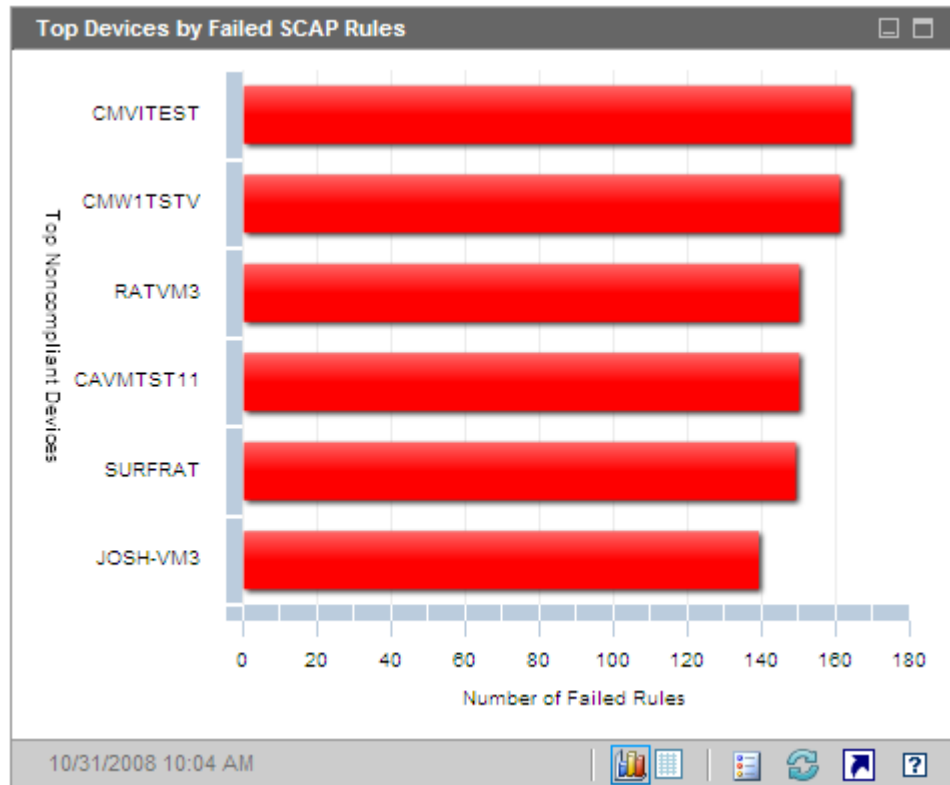
[Security and Compliance Management](#) on page 135

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 35 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 by the Reporting Server. 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 175

[Compliance Management Dashboard](#) on page 207

[Security and Compliance Management](#) on page 135

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 218
- [Security Product Summary](#) on page 220

The Operational View includes the following information panes:

- [Most Recent Definition Updates](#) on page 222
- [Most Recent Security Product Scans](#) on page 223

You can configure the dashboard to show or hide any of these panes. See [Configure the Dashboards](#) on page 65 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 152 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 27 Security Tool Detection States





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

Table 27 Security Tool Detection States

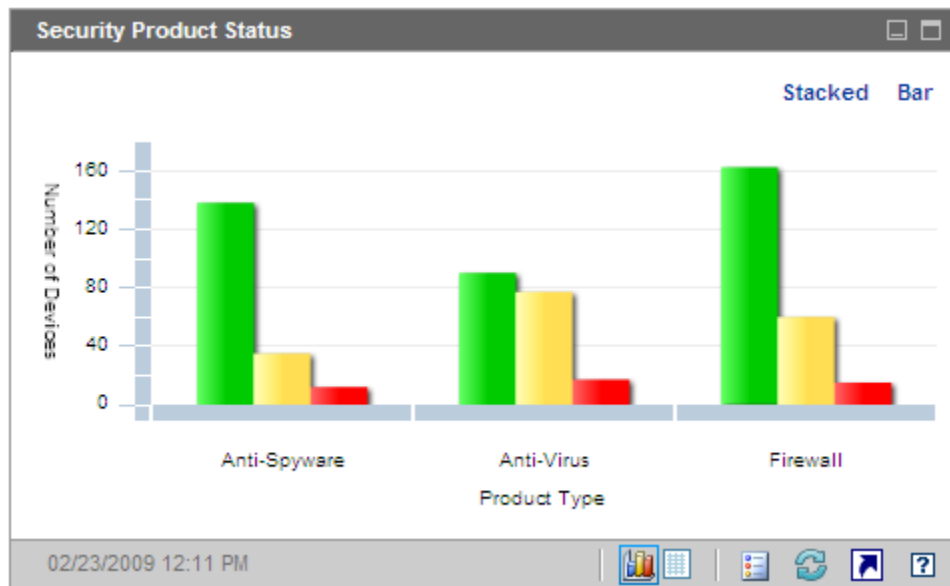
Color		Interval
	Red	Product was not detected.
	Blue	Unknown

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

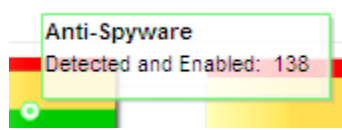
- The HP Live Network security tools scanner looked for this tool but was unable to determine its state.
- The scanner looked for this tool, but no scan records were found.
- The scanner did not look for this tool.

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

Figure 36 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 on the Reporting Server. 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 175

[Security Tools Management Dashboard](#) on page 217

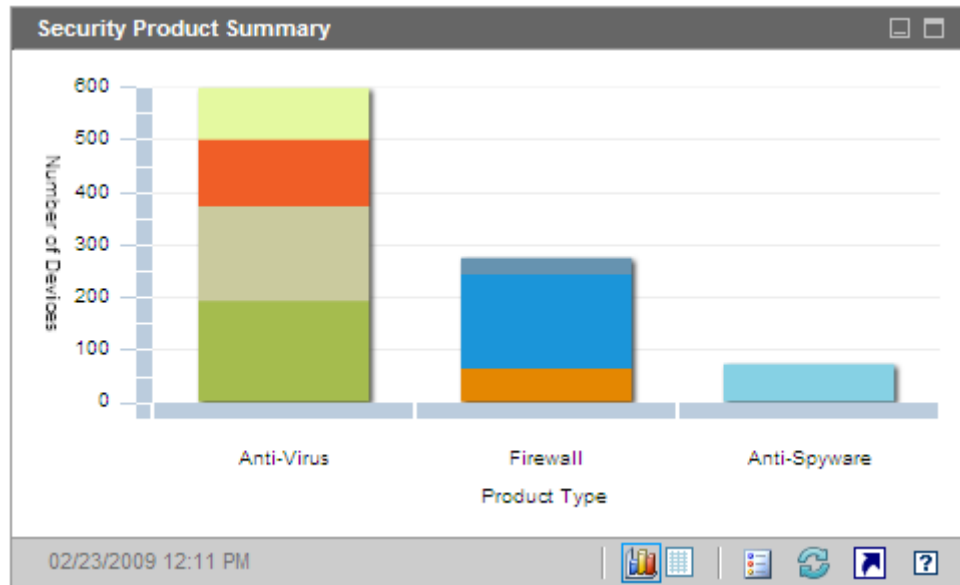
[Security and Compliance Management](#) on page 135

Security Product Summary

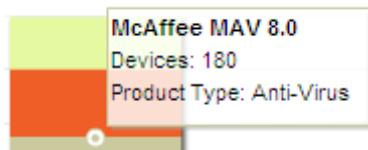
The chart view for this pane shows you which specific security products were detected on your managed client devices. The vertical axis shows the number of devices where each product was detected, and the horizontal axis shows the types of security tools detected.

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

Figure 37 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 by the Reporting Server. 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 175






[Security Tools Management Dashboard](#) on page 217

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:

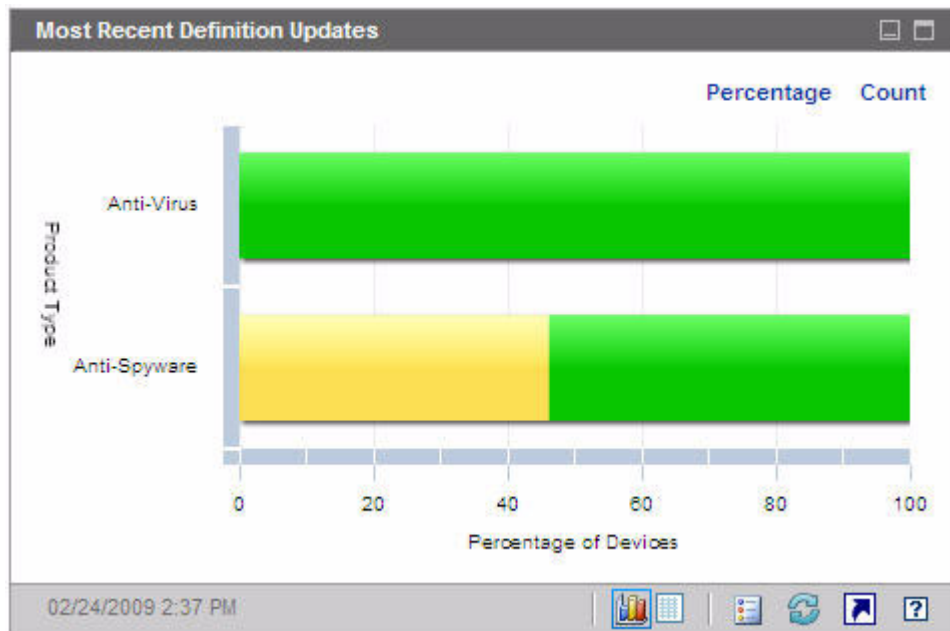
Table 28 Update Intervals

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 38 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 by the Reporting Server. 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 175

[Security Tools Management Dashboard](#) on page 217






[Security and Compliance Management](#) on page 135

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:

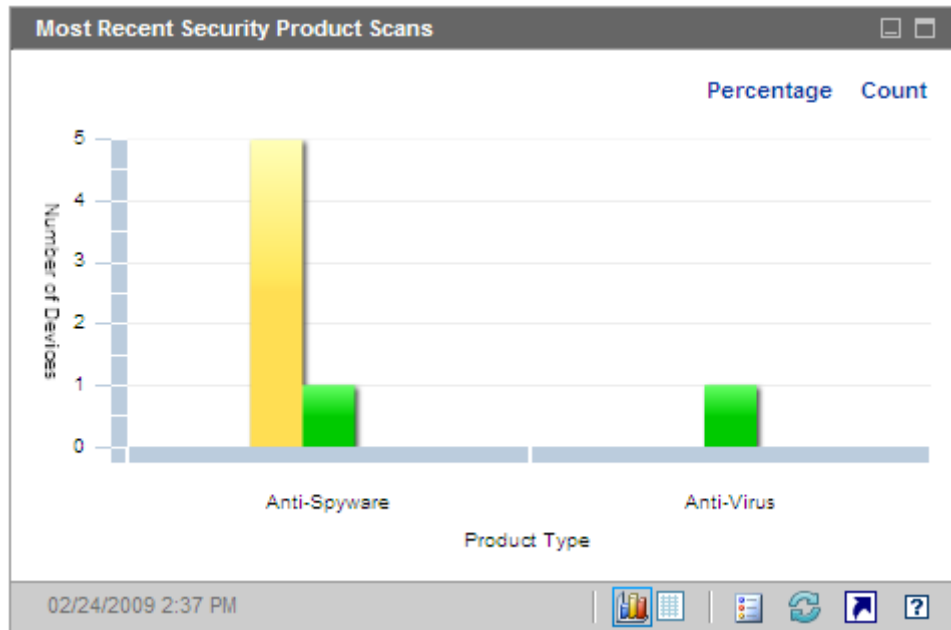
Table 29 Scan Intervals

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 39 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 by the Reporting Server. 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 175

[Security Tools Management Dashboard](#) on page 217

[Security and Compliance Management](#) on page 135

Patch Management Dashboard

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



This dashboard is disabled by default. To enable it, see [Configure the Dashboards](#) on page 65.

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

- [Device Compliance by Status \(Executive View\)](#) on page 227
- [Device Compliance by Bulletin](#) on page 229

The Operational View includes three information panes:

- [Device Compliance by Status \(Operational View\)](#) on page 230
- [Microsoft Security Bulletins](#) on page 231
- [Most Vulnerable Products](#) on page 232

You can configure the dashboard to show or hide any of these panes. See [Configure the Dashboards](#) on page 65.



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.

The information displayed in the Patch Vulnerability dashboard comes from the Patch Manager via the Reporting Server. Refer to the *Patch Manager Guide* for additional information.

The following items must be properly configured before this dashboard can display data:

- 1 The Reporting Server must be configured. Refer to the *Reporting Server Guide*.
- 2 The Patch Report Pack must be enabled on the Reporting Server. Also refer to the *Reporting Server Guide*.
- 3 Reporting Integration must be enabled and configured. See [Integrate the Reporting Server](#) on page 51.

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:

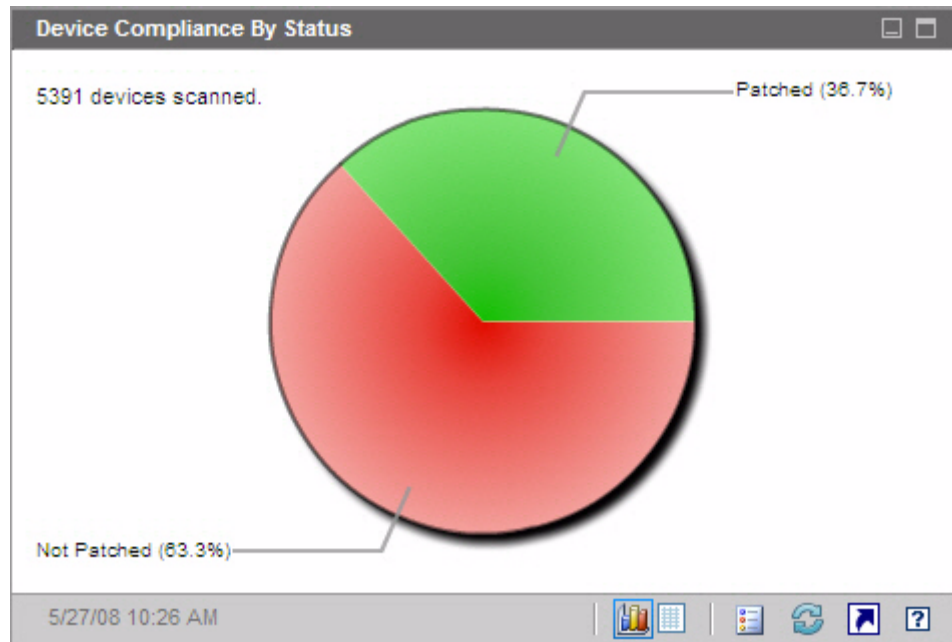
- Patched (green)
- Not patched (red)

The [Device Compliance by Status \(Operational View\)](#) on page 230 is similar but has finer-grained detail:

Table 30 Device Compliance By Status Views

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

Figure 40 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 by the Reporting Server. 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

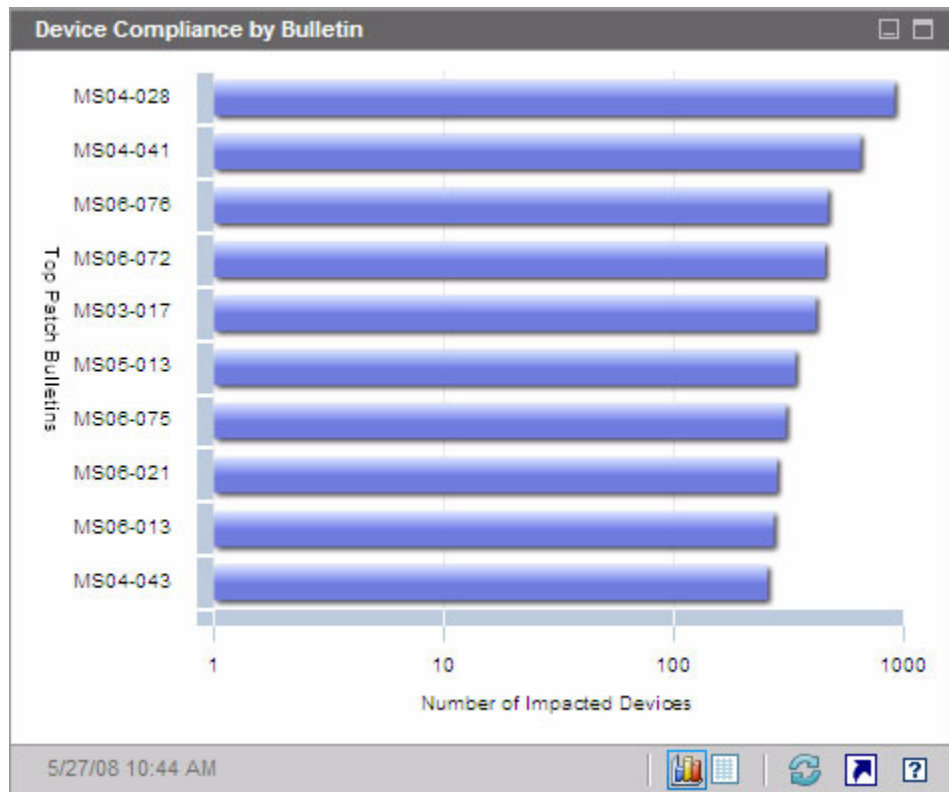
The chart view of this pane shows you the ten patch vulnerabilities that affect the greatest number of devices in your network. The vertical axis lists the patch bulletin numbers for these vulnerabilities. The horizontal axis represents the number of devices affected and uses a logarithmic scale.



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 41 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 by the Reporting Server. 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.

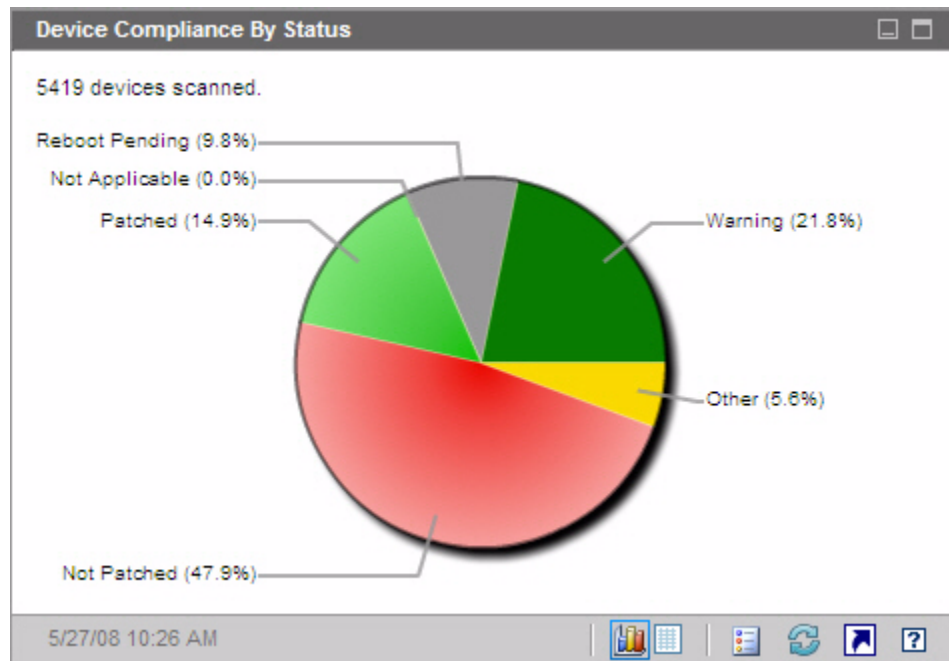
Device Compliance by Status (Operational View)

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 42 Device Compliance by Status (Operational View)



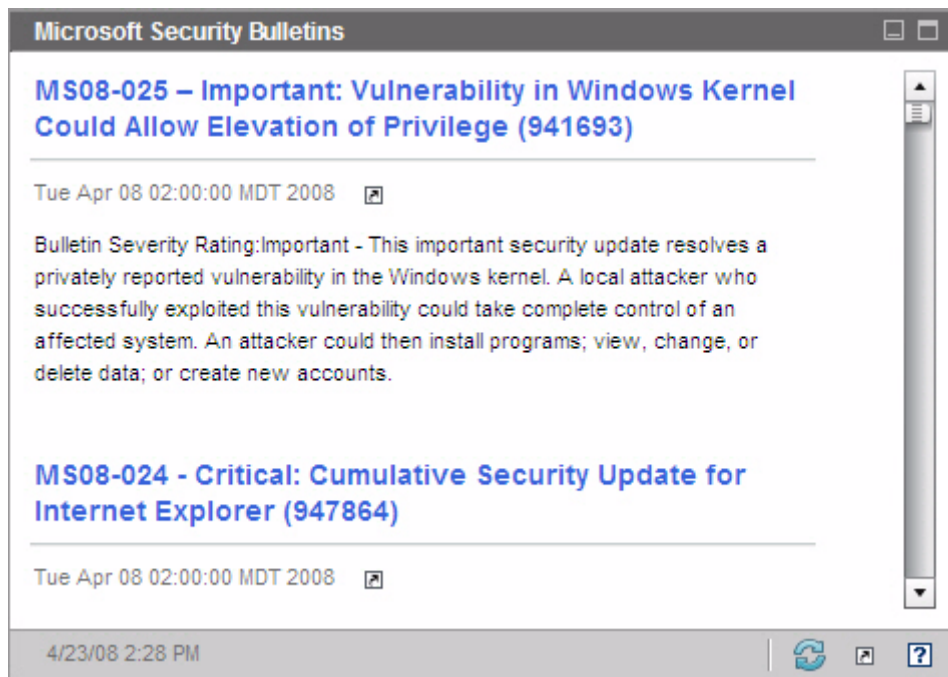
If you click one of the colored wedges in the pie chart, a new browser window opens, and a filtered report is displayed by the Reporting Server. The report lists all devices in the patch compliance status corresponding to the wedge that you clicked.


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 [Configure the Dashboards](#) on page 65).

Figure 43 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 [Configure the Dashboards](#) on page 65.

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

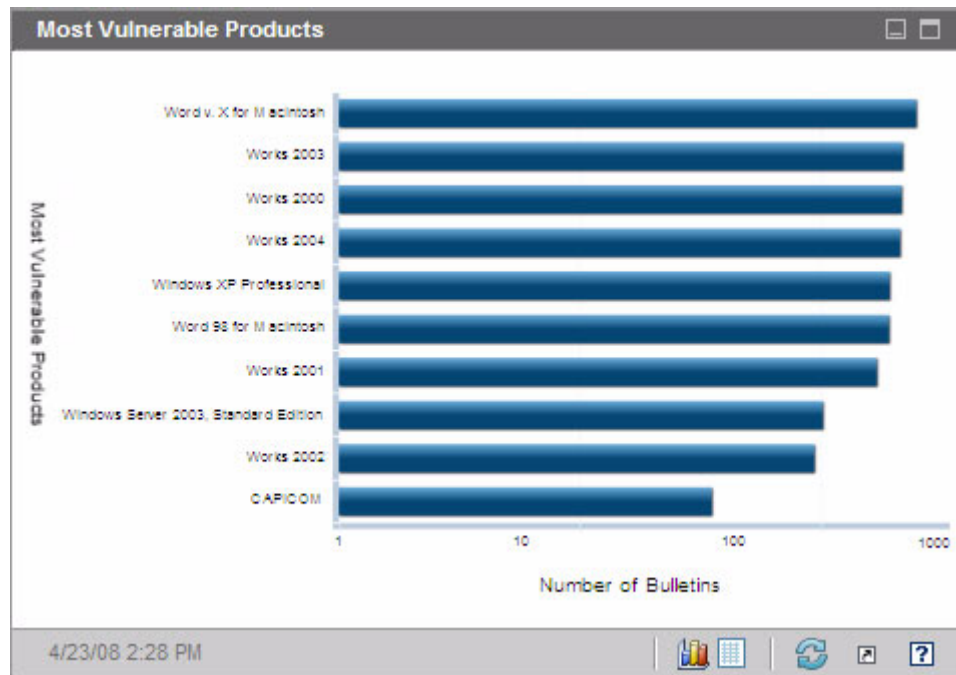
- 10 managed devices require all 6 of these patches
- 20 managed devices require 3 of these patches
- 50 managed devices only require 1 of the patches

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

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 44 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.

7 Using Reports

The Reporting area contains summary and detailed reports of many kinds. The specific reports available to you depends on the type of HPCA license that you have. The following topics are discussed in this chapter:

- [Reports Overview](#) on page 236
- [Navigating the Reports](#) on page 238
- [Types of Reports](#) on page 241
 - [HPCA Management Reports](#) on page 241
 - [Compliance Management Reports](#) on page 244
 - [Inventory Management Reports](#) on page 241
 - [Patch Management Reports](#) on page 242
 - [Vulnerability Management Reports](#) on page 243
 - [Security Tools Management Reports](#) on page 244
- [Filtering Reports](#) on page 246

Reports Overview

On the Reporting tab in the Enterprise Manager, 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.

These reports are provided by the Reporting Server, which must be properly installed and configured. Also, Reporting integration must be enabled in the Enterprise Manager. See [Integrate the Reporting Server](#) on page 51.

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

For additional information about report packs, refer to the *Reporting Server Guide*.



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 quicklinks for 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 quicklinks for 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", "Reset", and "?" 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 quicklinks for 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 quicklinks for View OVAL Definitions, View Scanned Devices, and View Top Vulnerabilities.
- Patch Information:** Shows Compliance Summary with Managed Devices: 0, Managed Bulletins: 1, and Last Acquisition: 2009-01-29 14:22:56. Includes quicklinks for View Device Compliance, View Bulletin Compliance, and View Acquisition Summary.



In a classic CAE installation, you must explicitly enable reporting on the Configuration tab. If the Reporting tab is not visible, follow the instructions under [Integrate the Reporting Server](#) on page 51.

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 31 Report Actions














Icon	Description
	Go back one page in the reports view.
	Return to the Reports home page.
	Refresh the data from the Reporting Server. 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.

Table 31 Report Actions

Icon	Description
	Print this report.
	Collapses the data portion of the report view.
	Expands the data portion of the report view.
	Show the graphical view of this report
	Show the grid (detailed) view of this report.
	Export report contents to a comma-separated value (CSV) file. The data in this file is actually delimited by tabs, not commas. The file extension is CSV, however.
	Export report contents to a Web query (IQY) file.

Items that appear in **blue text** in a report have various functions:

- Show Details – drill down to greater detail pertaining to this item
- Launch this Reporting View – open a new report based on this item
- Add to Search Criteria – apply an additional filter to the current report based on this item
- Go to Vendor Site – go to the web site of the vendor who posted this bulletin

When you rest your mouse over a **blue text** item, the tool tip tells you what will happen when you click the item.



By default, the reports use Greenwich Mean Time (GMT). Individual report packs can be configured to use either GMT or local time. For more information, refer to the *Reporting Server Guide*.

Types of Reports

The following types of reports are available in the Enterprise Manager:

- [HPCA Management Reports](#) on page 241
- [Compliance Management Reports](#) on page 244
- [Inventory Management Reports](#) on page 241
- [Patch Management Reports](#) on page 242
- [Vulnerability Management Reports](#) on page 243
- [Security Tools Management Reports](#) on page 244

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 Enterprise Manager 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 220 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 246 for more information.

These reports are displayed by the Reporting Server for which your Enterprise Manager is configured. 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 159 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 246 for more information.

These reports are displayed by the Reporting Server for which your Enterprise Manager is configured. Some of these reports are also available from the [Compliance Management Dashboard](#).

For more information, see [Configuring Security and Compliance Management](#) on page 152.

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 by the Reporting Server for which your Enterprise Manager is configured. 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 161 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 246 for more information.


These reports are displayed by the Reporting Server for which your Enterprise Manager is configured. Some of these reports are also available from the [Security Tools Management Dashboard](#).


For more information, see [Configuring Security and Compliance Management](#) on page 152.

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 157
- [Find Information about Compliance Failures](#) on page 159
- [Find Information About Security Tools](#) on page 161

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:

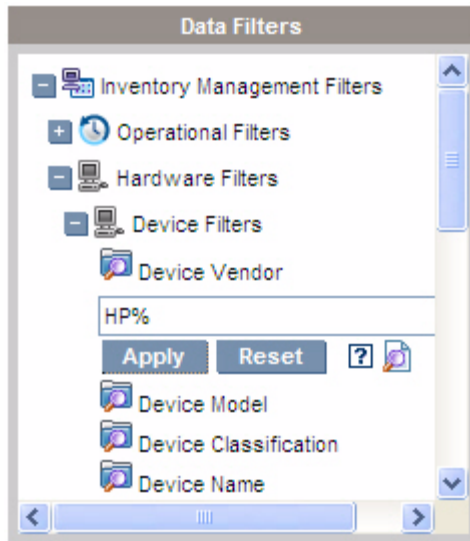
- 1 In the Data Filters section of the left navigation tree, expand the filter group that you want to use.
- 2 *Optional:* For the specific filter that you want to apply, click the  (show/hide) button to show the filter controls:
- 3 Specify the filter criteria in the text box, or click the  (criteria) 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 41 Special Characters and Wildcards

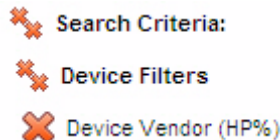
Character	Function	Device Vendor Filter Example	Records Matched
* or %	Matches all records containing a specific text string	HP*	All records that begin with “HP”
		%HP%	All records that contain “HP”
? or _	Matches any single character	Not?book	All records that begin with “Not” and end with “book”
		Note_ook	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.

8 Troubleshooting

This section contains information you can use to troubleshoot problems you encounter while using the Enterprise Manager. Each topic in this section describes a particular problem and provides a solution or workaround. The following areas are addressed:

- [Browser Issues](#) on page 252
- [Job Issues](#) on page 253
- [Dashboard Issues](#) on page 255
- [Security and Compliance Issues](#) on page 258
- [Other Issues](#) on page 261

Browser Issues


The following troubleshooting tips pertain to issues that may arise with your browser:

- [Cannot Refresh Page Using F5](#) on page 252
- [Cannot Enable HTTP 1.1 with Internet Explorer 6 and SSL](#) on page 252

Cannot Refresh Page Using F5

If you press the **F5** function key while using the Enterprise Manager, 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 Enterprise Manager 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 Enterprise Manager:

```
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](#) on page 253

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 92.

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}3gM1spnbrGbqVXNPDx8tWg==  
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 255
- [Most Vulnerable Products Dashboard Pane Loads Slowly](#) on page 255
- [Dashboard Pane Cannot Be Loaded](#) on page 256
- [Dashboard Pane Cannot Be Loaded – Reporting Query Failed](#) on page 256
- [Dashboard Panes in Perpetual Loading State](#) on page 256
- [RSS Query Failed](#) on page 257

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 [Configure the Dashboards](#) on page 65.

Dashboard Pane Cannot Be Loaded

This message is displayed when the Reporting Server is not integrated.

Solution:

See [Integrate the Reporting Server](#) on page 51 or your HP Software support representative.

Dashboard Pane Cannot Be Loaded – Reporting Query Failed

This message is displayed when the Reporting Server URL is not correct.

Solution:

See [Integrate the Reporting Server](#) on page 51 or your HP Software support representative.

Dashboard Panes in Perpetual Loading State

If the Enterprise Manager accesses a Reporting Server that 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 the Reporting Server 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 Reporting Server.

RSS Query Failed

If an HPCA dashboard pane cannot connect to the RSS feed that provides its content, the following error message is displayed in the pane:

Connection to RSS feed {*URL for RSS feed*} has failed. Make sure that the proxy server settings for HPCA Enterprise Manager have been properly configured, you have subscribed to the RSS feed, and that the RSS feed is accessible.

To determine the specific type of connection failure that has occurred, hover your mouse over the **RSS query failed** message in the lower left corner of the dashboard pane. One of the following messages will be displayed in a tool tip:

Table 42 Possible RSS Feed Failure Types

Failure Reason	Text Displayed
Proxy is not set	Error processing refresh: connection timed out: connect
Live Network password is invalid	Error processing refresh: Invalid Response: Login failed
You have not registered for the feed	Error processing refresh: Error on line -1: premature end of file

Solution:

Check the following things:

- 1 Make sure that the URL for the RSS feed is correct.
- 2 Paste the URL for the RSS feed site into a browser, and make sure that the site is accessible.

- 3 Make sure that your proxy settings for the Enterprise Manager are specified correctly.
- 4 For the HP Live Network Announcements feed:
 - a Make sure that your HP Live Network subscription is current.
 - b Make sure that your Live Network credentials are specified correctly.
- 5 Make sure that you have registered for the RSS feed, if necessary. To register for the feed, click the URL displayed in the error message.

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 258
- [Managed and Scanned Device Counts are Zero](#) on page 259
- [SQL Server Connection Errors](#) on page 259
- [Report Presentation is Slow](#) on page 260

HP Live Network Connector Unable to Connect

The most likely cause of this issue is an incorrect proxy server setting for HP Live Network. If the system where the Enterprise Manager is installed requires a proxy to access the Internet, you must specify a proxy server on the Settings tab on the Live Network configuration page. The proxy setting must be in the following format:

```
http|https://<servername>:<portNumber>
```

The `http` or `https` is required as well as the port. For example:

```
http://web-proxy.mycompany.com:8088
```

The Enterprise Manager does not perform any type of validation of the **Proxy Server** field on the Settings 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 the Reporting Server has not yet been integrated.

Solution:

For more information, see [Integrate the Reporting Server](#) on page 51, or contact your HPCA administrator.

SQL Server Connection Errors

If either the `vms-server.log` or `vms-commandline.log` file contains a message that includes the string `com.microsoft.sqlserver.jdbc.SQLServerException` and additional text about being unable to connect to SQL Server, it is possible that the settings specified on the Live Network configuration page are not correct.

Solution:

Check the following Live Network configuration settings:

- On the Databases tab, the **Database Server** should be the hostname of the system where the Reporting database resides. For example:

```
mydbserver.mycompany.com.
```

If the SQL Server setup uses something other than the default database instance, the instance needs to be appended to the server name. For example:

```
mydbserver.mycompany.com\HPCA
```

The **Database Name** field must reflect the specific Database Name in that instance.

- In SQL Server, the default static port is 1433. However, it is possible that the SQL Server installation is set up with a different static port or with a dynamic (non-specified) port.

Verify your SQL Server port settings, and update the SQL Server port information on the Database tab. If SQL Server is using a dynamic port, set the Live Network Reporting database port to be blank.

- Check your authentication settings in SQL Server. You must use SQL Server Authentication when connecting to the HPCA database from the HPCA CoreEnterprise Manager. Windows authentication is not supported in this context. If you change your authentication settings in SQL Server, be sure to update your Live Network Database configuration settings appropriately.

Report Presentation is Slow

If your vulnerability, compliance, or security tools management reports display slowly in the Enterprise Manager, you should enable report caching.

Solution:

- 1 Open a web browser and type:

```
http://ReportingHost:/reportingserver/setup.tcl
```

where *ReportingHost* is the host name or IP address of the system where the Reporting Server 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 261
- [Additional Parameters Disregarded by the HPCA Job Wizard](#) on page 262
- [Virtual Machines Will Not Start](#) on page 263
- [Query Limit Reached](#) on page 263

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 Server 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 Server behavior is to display the home page.

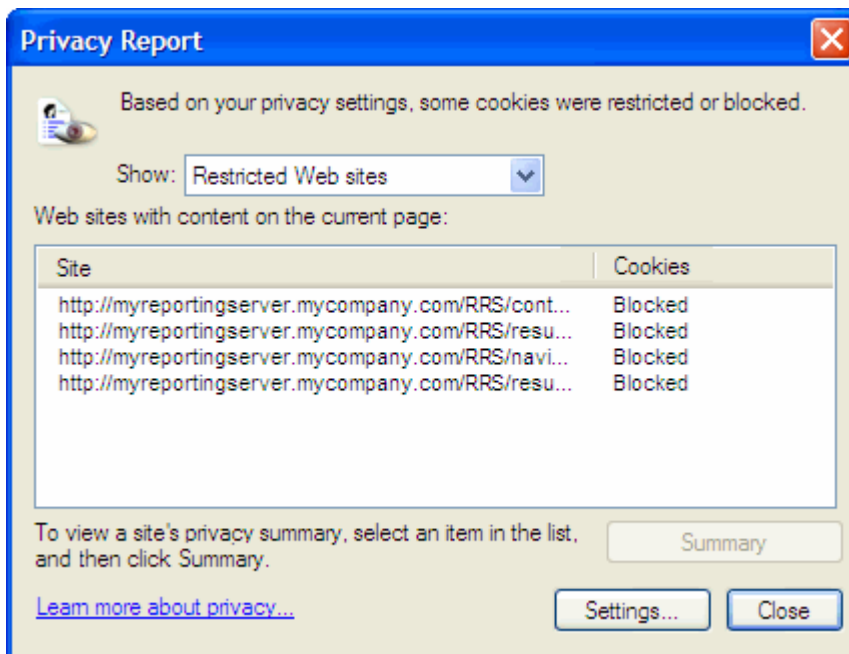
This behavior is most prevalent with Internet Explorer 6 and 7 on the Windows 2003 Server platform. It can, however, happen on any supported platform.

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:



- 2 Using your browser privacy settings, add the URL for the report that you want to view to the **Allowed** cookies list.

Additional Parameters Disregarded by the HPCA Job Wizard

If you want to specify “additional parameters” when using the HPCA Job Creation Wizard, you must specify them in the following format:

```
option=value
```

If you do not use this format, the additional parameters are ignored. On the confirmation page (the last page of the wizard), be sure to verify that your additional parameters are included in the command line.

Virtual Machines Will Not Start

A licensing defect in ESX version 3.5 Update 2 (build number 103908) prevents Virtual Machines from being started after a certain date.

If you are running this ESX build, and you attempt to start a Virtual Machine from the Enterprise Manager, 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](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 Enterprise Manager. 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 Enterprise Manager. This file is located in the following directory:

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

By default, `<tomcatDir>` is as follows.

CAE installation: `C:\Program Files\HP\HP BTO Software\CM-EC\tomcat`

Core and Satellite: `C:\Program Files\Hewlett-Packard\HPCA\tomcat`

After modifying the `Console.properties` file, be sure to restart the HPCA Enterprise Manager service.



Modifying the `directory_object_query_limit` property may negatively impact performance of the Enterprise Manager.

A Adding Custom Dashboard Filters and Perspectives

This appendix contains instructions for making custom dashboard filters and perspectives available in the Enterprise Manager.

Filters and perspectives are configured for use in the Enterprise Manager in the following file:

```
<InstallDir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties
```



In an HPCA Core installation, there are very few settings in this file initially. After you change and save the console configuration settings, however, the file contains much more information.

For information about using dashboard filters and perspectives, see [Using the Dashboards](#) on page 175.

Add a Filter

You can add any number of custom dashboard filters to the Enterprise Manager.



Dashboard filters consist of DEVICELIST filters implemented in the `rim.kit` report pack. Creating filters in the HPCA report packs is an advanced task. If you do not know how to do this, contact your HP Software Support representative for assistance.

To add a custom filter:

- 1 Implement the customizable DEVICELIST filter in the RIM report pack. This requires two steps:
 - a Create the filter.

To add a custom perspective:

- 1 Open the following file in a text editor:

```
<InstallDir>\CM-EC\tomcat\webapps\em\WEB-INF\Console.properties
```

- 2 Add the new perspective name using the following format:

```
global_perspective_N_displayname=displayName  
global_perspective_N_filter=filterName.filter
```

In this case, *displayName* is the name of the filter that will appear in the Perspectives box in the upper left corner of the Enterprise Manager, and *N* is either 4 or 5 (unless you are replacing the default perspectives, in which case *N* can also be 1, 2, or 3).

For example:

```
global_perspective_4_displayname=MyCustom  
global_perspective_4_filter=myfilter.filter
```

- 3 Save the `Console.properties` file.
- 4 Restart the following service:
HP Client Automation Enterprise Manager
- 5 Start the Enterprise Manager and verify that the new perspective is available in the Perspectives box.

B DTM Jobs in an HPCA Classic Installation

In an HPCA Core and Satellite installation, you can create and manage Distributed Task Management (DTM) jobs by using the Enterprise Console. This capability is automatically configured and is available out of the box.

In an HPCA Enterprise (CAE) classic component-based installation, however, special configuration steps are required. This appendix contains instructions for configuring your HPCA Enterprise (CAE) classic installation to accept DTM jobs.

For general information about DTM jobs, see [Managing Jobs](#) on page 92.

Requirements

Your CAE classic installation must meet the following requirements:

- Your HPCA Proxy Server must use the Apache-based Enterprise Proxy Server. The older Integration Server-based proxy server module will not work for DTM jobs. For more information, refer to the *Enterprise Proxy Server Installation and Configuration Guide*.
- The Enterprise Manager, Messaging Server, and Proxy Server components must all be installed on the same system.
- The DATA Service Access Profiles (SAPs) in your Configuration Server database (CSDB) must be configured as shown in [Configure the Server Access Profiles \(SAPs\)](#) on page 272.

For more information about SAPs, refer to the *Application Manager and Application Self-Service Manager Installation and Configuration Guide*.



In a classic 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. See [Job Issues](#) on page 253.

Configuring Your Servers

There are three steps required to configure your CAE to accept DTM jobs:

- [Configure the Proxy Server](#) on page 270
- [Configure the Server Access Profiles \(SAPs\)](#) on page 272
- [Configure the Messaging Server](#) on page 275

Each of these steps is discussed in detail in this section.

Configure the Proxy Server

The first step in configuring your CAE classic installation to manage DTM jobs is to configure your Proxy Server.

To configure the Proxy Server for DTM job management:

- 1 Open the following file in a text editor:

```
ApacheProxyServerInstallDir/conf/httpd.conf
```

By default, *ApacheProxyServerInstallDir* is:

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

- 2 Scroll to the end of the file.
- 3 Locate the following section:

```
<IfDefine DYNAMIC>
  LoadModule proxy_module modules/mod_proxy.so
  <IfModule mod_proxy.c>
    LoadModule proxy_http_module modules/mod_proxy_http.so
    ProxyPass          /RESOURCE http://
    @@ProxyUpstreamHost@@: @@ProxyUpstreamPort@@/RESOURCE
    ProxyPassReverse  /RESOURCE http://
    @@ProxyUpstreamHost@@: @@ProxyUpstreamPort@@/RESOURCE
    ...
  </IfModule>
</IfDefine>
```

- 4 Move the two `LoadModule proxy_` statements immediately before the `<IfDefine DYNAMIC>` statement:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

```

<IfDefine DYNAMIC>
  <IfModule mod_proxy.c>
    ProxyPass          /RESOURCE http://
    @@ProxyUpstreamHost@@: @@ProxyUpstreamPort@@/RESOURCE
    ProxyPassReverse  /RESOURCE http://
    @@ProxyUpstreamHost@@: @@ProxyUpstreamPort@@/RESOURCE
    ...
  </IfDefine>

```

- 5 Add the following to the end of the `httpd.conf` file. Be sure to change `MyServer` to the server name (or IP address) where the Enterprise Manager, Configuration Server, and Messaging Server are installed:

```

#EM URL
ProxyPass          /em http://MyServer:8080/em
ProxyPassReverse  /em http://MyServer:8080/em

#DTM and OPE server URL
ProxyPass          /ope/resources http://MyServer:8080/ope/resources
ProxyPassReverse  /ope/resources http://MyServer:8080/ope/resources

# DTM agent targets this URL
ProxyPass          /proc/msg http://MyServer:3461/proc/msg
ProxyPassReverse  /proc/msg http://MyServer:3461/proc/msg

# ROMS targets this URL
ProxyPass          /proc/appeventxml http://MyServer:3461/proc/
appeventxml
ProxyPassReverse  /proc/appeventxml http://MyServer:3461/proc/
appeventxml

# Legacy RMS URLs
ProxyPass          /proc/core          http://MyServer:3461/proc/core
ProxyPassReverse  /proc/core          http://MyServer:3461/proc/core
ProxyPass          /proc/patch         http://MyServer:3461/proc/patch
ProxyPassReverse  /proc/patch         http://MyServer:3461/proc/patch
ProxyPass          /proc/wbem          http://MyServer:3461/proc/wbem
ProxyPassReverse  /proc/wbem          http://MyServer:3461/proc/wbem
ProxyPass          /proc/inventory     http://MyServer:3461/proc/inventory
ProxyPassReverse  /proc/inventory     http://MyServer:3461/proc/inventory

# Used by WinCE/ThinClient support
ProxyPass          /proc/xml/obj       http://MyServer:3461/proc/xml/obj
ProxyPassReverse  /proc/xml/obj       http://MyServer:3461/proc/xml/obj

```

- 6 Restart the HPCA Proxy Server service.

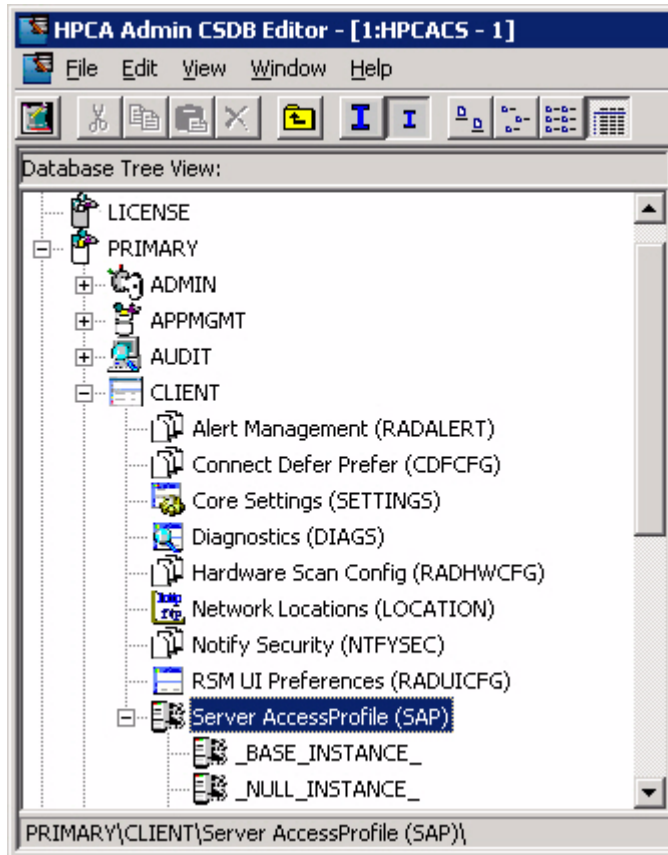
Configure the Server Access Profiles (SAPs)

The next step in configuring your CAE classic installation to manage DTM jobs is to create and configure the Service Access Profiles (SAPs) that enable the agents to communicate with the CAE server components.

A Server Access Profile (SAP) is simply a generic way to define all possible data access points for a service. A SAP can be a Configuration Server, Proxy Server, or CD-ROM drive.

To configure the SAPs:

- 1 Open the CSDB Editor.
- 2 Expand the PRIMARY.CLIENT.SAP entry.




















- 3 Add a new SAP instance of type RCS:
 - a In the Database Tree View, right-click Server Access Profile (SAP).
 - b Select **New Instance**.
 - c For both the display name and the instance name, specify RCS.
 - d Click **OK**.
 - e In the Database Tree View, right-click your new SAP.
 - f Select **Edit Instance**.
 - g For the Universal Resource Identifier attribute, specify the name (or IP address) of the server where the Configuration Server is installed.
 - h Specify the values of the remaining attributes as shown here:

Server AccessProfile class RCS Instance Attributes:	
Attribute Description	Value
Expression Resolution Method	
Expression Resolution Method - 001	
Friendly Name	RCS
Type [RCS/DATA/ROM/PMG]	RCS
Universal Resource Identifier	tcp://myserver.mycompany.com:3464
RCS Role A,O,S,M,R,D,Z	OSMR
Enable SAP [Y/N]	Y
Communications Timeout (0-3200)s	
Push Back (0-999 retries)	0
Throttle [NONE/ADAPTIVE/RESERVE...]	
Bandwidth Percentage (1-99)	
Enable Streaming [Y/N]	N
Internet Proxy URI	
Selection Priority	&(LOCATION.SAPPRI)
Product Filter	
Filter Expression [Obj.Var = Value]	
Network Time To Live (0-999)	

UTF-8 6/9/2009 11:38 AM

- i Click **OK** to save your changes.

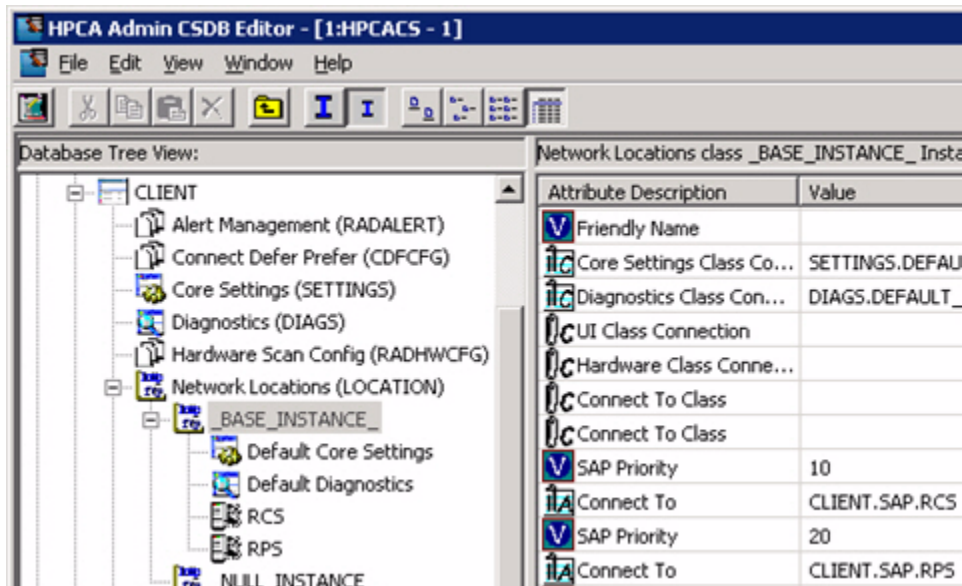
- 4 Following the same process, add a new SAP instance called RPS:

Server AccessProfile class RPS Instance Attributes:	
Attribute Description	Value
 Expression Resolution Method	
 Expression Resolution Method - 001	
 Friendly Name	RPS
 Type [RCS/DATA/ROM/PMG]	DATA
 Universal Resource Identifier	http://myserver.mycompany.com:3466
 RCS Role A,O,S,M,R,D,Z	PDZ
 Enable SAP [Y/N]	Y
 Communications Timeout (0-3200)s	
 Push Back (0-999 retries)	0
 Throttle [NONE/ADAPTIVE/RESERVE...]	
 Bandwidth Percentage (1-99)	
 Enable Streaming [Y/N]	N
 Internet Proxy URI	
 Selection Priority	&(LOCATION.SAPPRI)
 Product Filter	
 Filter Expression [Obj.Var = Value]	
 Network Time To Live (0-999)	

For the Universal Resource Identifier, specify the name (or IP address) of the server hosting the Proxy Server.

Specify the values for the remaining attributes as shown here.

- 5 Connect the two new SAPs to the BASE_INSTANCE of the CLIENT.LOCATION, as shown here:



Configure the Messaging Server

The final step in configuring your CAE classic installation to manage DTM jobs is to configure your Messaging Server.

To configure the Messaging Server:

- 1 Open the following file in a text editor:

MessagingServerInstallDir\etc\rms.cfg

By default, *MessagingServerInstallDir* is:

C:\Program Files\Hewlett-Packard\CM\MessagingServer

- 2 Locate the msg::register httpd section.
- 3 Add the following statement at the end of this section:

URL /proc/msg

The section should now look like this:

```

msg::register httpd {
    TYPE          HTTPD

    PORT          3461
    USE           default

    URL           /proc/rim/default
    URL           /proc/xml/obj
    URL           /proc/msg }

```

4 Locate the `msg::register router` section.

5 Add a DTM route, as shown here:

```

msg::register router {
    TYPE          ROUTER

    ROUTE        {
        TO        CORE.RIM
        USE       rim
    }
    ...
    ROUTE        {
        TO        DTM
        USE       dtm
    }
}

```

6 Add a new `msg::register dtm` section

```

msg::register dtm {
    TYPE          HTTP

    ADDRESS      {
        PRI       10
        URL       http://localhost:3466/ope/resources/jobruns
    }
}

```

7 Restart the HPCA Messaging Server service.

Test a DTM Job

To test your new DTM job capability, you will need to do the following:

- Create a Notify job to download your new SAPs to a target device.
- Create a DTM job (or multiple jobs) for that agent to run.
- Create another Notify job to force the agent on that target device to synchronize its DTM job schedules.

This process is briefly described here. For general information about creating and tracking DTM jobs, see [Managing Jobs](#) on page 92.

To test your DTM job setup:

- 1 Under Jobs on the Configuration tab, open the Software Connect job action template.
- 2 In the **Parameters** box for this template, specify the name (or IP address) of your server. For example:

```
dname=software, cop=y, ip=MyServer
```

Here, *MyServer* is the system where the Configuration Server is installed.

- 3 Create a Notify job for a target device using the Software Connect job action template.

This job will ask the agent on that device to connect to the Configuration Server and download the new SAPs

- 4 To determine whether the SAPs were successfully downloaded to the agent, check to see if the following file exists on the target device:

```
AgentDir\Lib\SAP.EDM
```

By default, *AgentDir* is:

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

- 5 Create one or more DTM jobs for your target device.
- 6 Create a Notify job for your target device using the Refresh DTM Schedules job action template.

After this job runs, you agent should have downloaded the DTM jobs that you assigned to it. These jobs will be listed in the following file:

AgentDir\Lib\dtm.xml

7 Check *AgentDir*\Log\dtm.log to see if your DTM job ran correctly.



To manually run a DTM job, go to the *AgentDir* on the target device, and execute the following command:

```
dtm run -jobid jobId -timerid timerId
```

You can find the values for *jobId* and *timerId* in the dtm.xml file on the target device.

Index

A

Adobe Flash Player, 20
advanced programmable interrupt controller
 See APIC
All Devices
 group, 121
APIC, 122

B

blade server reports, 241

C

Catalina log file, 74
Configuration tab, 32
configuration tasks, 33
configuring
 directory service, 39
 Enterprise Manager, 22
 LDAP, 41
Connection Settings, 39
Console Settings, 43
creating users, 44

D

dashboard
 panes, 176

dashboards, 176
 configuring, 65
 HPCA Operations, 66
 patch, 70
 Vulnerability Management, 67
 overview, 176
 Patch Management, 226
 Vulnerability Management, 188

deployment
 scenarios, os images, 120
Device Resolution, 101
Directory Search Attributes, 43, 44
directory service
 Configuration Server, 39
 ldap, 41
 types, 40

E

Embedded Linux, 123
Enterprise Manager
 configuring, 22
 creating users, 44
 installing, 22
 logging on, 30
 navigating, 30
 removing, 23

F

Flash Player, 20

H

HAL, 122
Hardware Abstraction Layer See HAL
Home tab, 31
HPCA Agent ID, 241
HPCA Operations dashboard, configuring, 66
HP Hardware reports, 242

I

installing Enterprise Manager, 22
integrating Reporting Server, 51
Inventory Management Reports, 241

J

Job Management, 92
Job States, 99
 Completed, 97, 99

L

Leaf Node Filter, 43
Local Service Boot, 128
log files, 74
logging in, 30
logon page, 22

M

Management tab, 32
Maximum Cache Age, 43

N

navigating Enterprise Manager, 30
Notify Templates, creating, 47

O

ope.log, 74
OS image Target Devices requirements, 121
OvCMEEmTomcat, 74

P

panes, 176
Patch Management Reports, 242
Patch Vulnerability dashboard, 226
 configuring, 70
platform support, 21
Policy Management Wizard, 86
 Policy Configuration, 86
 Service Selection, 86
 Summary, 87
PXE, 128
PXE boot, 122

R

related documents, 17
removing a device, 88
Reporting Server, integrating, 51
Reporting tab, 32

S

S.M.A.R.T. Alerts reports, 241
Sample Notify Templates, 50
SCSI, 122
Service CD, 128
Services, 87
 viewing, 87
 viewing details, 87

small computer systems interface See SCSI
SSL, 30
system requirements, 20
 target devices, 121

X

XPe, 123

T

target device
 definition, 121
 requirements, 121
thin client, 123
 deploying factory OS images to, 123

U

User IDs, default, 44
users, creating, 44

V

virtual hosting servers, 104
virtual machine
 creating, 108
 managing, 104
Virtual Machine Creation Wizard, 109
vms.log, 75
vms-commandline.log, 75
VMware ESX Server, 104
Vulnerability Management dashboard, 188
 configuring, 67
Vulnerability management server
 Configuration Server, 56
 Reporting database, 56

W

Windows CE, 123
Windows XP Embedded, 123

