HP Client Automation Enterprise

Patch Manager

for the Windows® and Linux operating systems

Software Version: 7.80

Installation and Configuration Guide

Manufacturing Part Number: None
Document Release Date: November 2009
Software Release Date: November 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

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.

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	7.50	Replaced references to using the HPCA Portal to using the HPCA Enterprise Manager for deploying the Patch Agent. Patching AIX, HP-UX or Solaris devices is not currently supported. Removed references to earlier support for patching these Operating Systems throughout the guide.
All	7.20 Aug 2008	Corrected invalid cross-references throughout the guide.
All	7.20	Most HP Configuration Management Version 5.1x product names have been rebranded with HP Client Automation names as of Version 7.20. Refer to the current Release Notes for more information.

Document Changes

Chapter	Version	Changes
1	7.20	Using this Guide with Core and Satellite Servers on page 18, new topic.
1	7.50	Terminology on page 18, added Patch Manager Gateway. Patch Manager Components on page 18, added HPCA Enterprise Manager entry. As of Version 7.50, the Enterprise Manager console is used to deploy the Patch Agent as part of the HPCA Agent, as well as view Patch Dashboards and Patch Reports.
2	7.50	Database Prerequisites for Microsoft SQL Server or Oracle on page 22, modified topic. Refer to the Database Support table in the accompanying release notes document for supported versions of Microsoft SQL Server or Oracle.
2	7.20	Database Prerequisites for Microsoft SQL Server or Oracle on page 22, modified the supported versions of Microsoft SQL Server or Oracle that can be used to host the Patch Manager Database. New support includes: • "SQL Server 2008 • "Oracle 11g, Release 1 with the latest Oracle patch set
2	7.20 Aug 2008	Creating the Database for Patch Manager on page 24, modified topic title, and added Roles and System Privileges to the defined user profile when creating the database using Oracle.
2	7.50	Implementation Task List on page 23, replaced “Install the HPCA Portal (Optional)” with “Install the HPCA Enterprise Manager (Optional)”.
2	7.20	"HPCA Patch Manager Server" is the rebranded Windows Service Name.

Document Changes

Chapter	Version	Changes
2	7.50	Configuring Patch Manager using the Patch Manager Administrator on page 32, new topic introduces the new Configuration task groups: Environment Settings, Acquisition Settings and Acquisition Jobs.
2	7.80	To access and use the Patch Manager Administrator on page 33 modified to indicate that the **Save** button now both saves and applies the changes.
2	7.50	Agent Options on page 38, new Configuration topic and panel used to set Agent options for patching Microsoft devices. Options include: Enable Download Manager, Disable Microsoft Updates, and Delete the SoftwareDistribution folder.
2	7.80	Agent Options on page 38, added field to set the Manage Installed Bulletins (-mib) option from this page.
2	7.80	Download Manager Option on page 39 has been modified where the delay time is now specified in seconds rather than minutes.
2	7.80	Agent Options for Patch Agents on page 41 more clearly explains the mib option and changes the default to none.
2	7.50	Preferences on page 43, modified to define Basic and Advanced-only fields.
2	7.80	Preferences on page 43, added Allow Internet Access field.
2	7.50	Vendor Settings on page 45, removed settings related to HP-UX and Solaris, which are no longer supported. All Vendor Settings pages default to showing Basic fields, and an Advanced tab exposes settings rarely changed. Vendor topics identify Basic and Advanced fields, accordingly.

Document Changes

Chapter	Version	Changes
2	7.20	Microsoft Data Feed Prioritization on page 46, the default Data Feed Prioritization has changed from MSSecure, Microsoft Update Catalog, Client Automation to Microsoft Update Catalog, Only. To use this default option, all devices in the enterprise must meet minimum operating system and product levels as set by Microsoft.
2	7.50	SuSE Feed Settings on page 52, added Feed Settings needed to acquire SuSE Version 10 security patches. SuSE Version 10 support covers both SuSE Linux Enterprise Server 10 (SLES10) and SuSE Linux Enterprise Desktop 10 (SLED10).
2	7.50	View Logs on page 57, new topic.
3	7.50 7.20	About HP-UX Patch Acquisition, topic deleted. About HP-UX Patch Acquisition, added note: HP-UX Patch Acquisition is not available for new HP Patch Manager installations as of Version 7.20; customers who upgraded from an earlier version of Patch Manager can continue to acquire and deploy HP-UX Patches to their devices under management by earlier versions of the HP Patch Manager Agent.
3	7.50	SuSE Patch Acquisition Requirements on page 71, modified topic. To access the SuSE 10 Patches and Updates, you need to obtain mirror credentials (username and password) from Novell.
3	7.80	SuSE Patch Acquisition Requirements on page 71, modified topic. To access the SuSE 10 and above Patches and Updates, you need to obtain mirror credentials (username and password) from Novell. SuSE 10 and SuSE 11 Registration Requirements on page 73, new topic advising customers of the Novell licensing and registration policy for devices running SuSE 10 and SuSE 11 Operating Systems.

Document Changes

Chapter	Version	Changes
3	7.80	Configure Acquisition Jobs on page 74, modified Bulletin field description to explain the required format for entering SuSE 9, 10, and 11 Bulletins. Note that any comma in a SuSE bulletin filename must be entered as a hyphen.
3	7.80	Microsoft Settings on page 77, modified to add the new supersedence option.
3	7.80	Setting the Manage Installed Bulletins (mib) Option on page 83 more clearly explains the mib option and changes the default to none.
3	7.50	Patch Acquisition Reports on page 84, updated report images.
4	7.50	To install the Patch Manager Agent from the HPCA Enterprise Manager on page 88, topic replaces the previous topic: "To install the Patch Manager Agent from the Portal."
4	7.50	To install the Patch Manager Agent on a Linux operating system on page 89, added support for Linux Agents on SuSE Linux Enterprise Server (SLES) and SuSE Linux Desktop Server (SLED) Version 10, 10 SP1 and 10 SP2 on x86 (32-bit) architectures as well x86-64 (AMD64 and Intel EM64T) architectures.

Document Changes

Chapter	Version	Changes
4	7.50	Patch Analysis and Reports on page 105, new topics, new reports, revised report contents and images: • Drilling Down to Detailed Information on page 108, new topic was added. • Executive Summaries on page 110, new for this release. Four reports (either a pie chart or bar chart) give an overview of the patch compliance status in your environment and allow you to drill down into compliance report tables giving details. • Patch Compliance Reports on page 114; reports, images, and content were modified. • Research Reports on page 126; some report images were updated.
4	7.80	Device Status on page 112, has new compliance status graphical reports showing percentage of patch compliance per device.
4	7.80	Research by Devices on page 127 has new columns for MSI installer version, WUA version, and WUA status.
4	7.80	Instance Naming Convention for SuSE 11 Bulletins on page 133, new topic explains how HP renames SuSE bulletin names to create shorter and unique instance names in the CSDB.
Appendix D	7.50	Patch.cfg Parameters on page 167, added parameters for SUSE Linux Enterprise Server Version 10 and SUSE Linux Desktop Server Version 10.
Appendix D	7.80	Patch.cfg Parameters on page 167, modified SuSE parameter to include support for SUSE Linux Enterprise Server and SUSE Linux Enterprise Desktop Version 11 support.

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

At the end of this chapter, you will:

- Know the capabilities of HP Client Automation Enterprise Patch Manager (Patch Manager). Topics include:
  - — HP Client Automation Patch Manager on page 16
  - — Using this Guide with Core and Satellite Servers on page 18
  - — Terminology on page 18
  - — Patch Manager Components on page 18
  - —

HP Client Automation Patch Manager

The HP Client Automation Patch Manager (Patch Manager) provides value for business continuity and security initiatives. The Patch Manager is offered as a complete stand-alone solution and can be used as a fully integrated component of the HP Client Automation Enterprise Suite (HPCAE Suite). The HPCAE Suite provides automated and ongoing configuration management for all software across the enterprise, ensuring that the entire software infrastructure is always in its desired state—up-to-date, reliable, and secure.

Key capabilities for patch management activities include:

- **Acquisition**:
  configurable tools to enable automatic collection of security updates (patches), update rollups, and service packs directly from Microsoft, as well as security bulletins (advisories) for Red Hat and SuSE, based on content derived from supported vendor supplied web-based repositories.

  This release drops supports for the acquisition of security bulletins (advisories) for HP-UX and Sun Solaris (Sparc). HPCA no longer supports managing HP-UX or Sun Solaris Agent devices.

- **Pilot Testing**:
  Patch Manager also allows IT administrators to select target pilot groups based on usage or critical need. HP Client Automation is the only solution with these unique pilot testing capabilities that help ensure the stability of business critical systems.

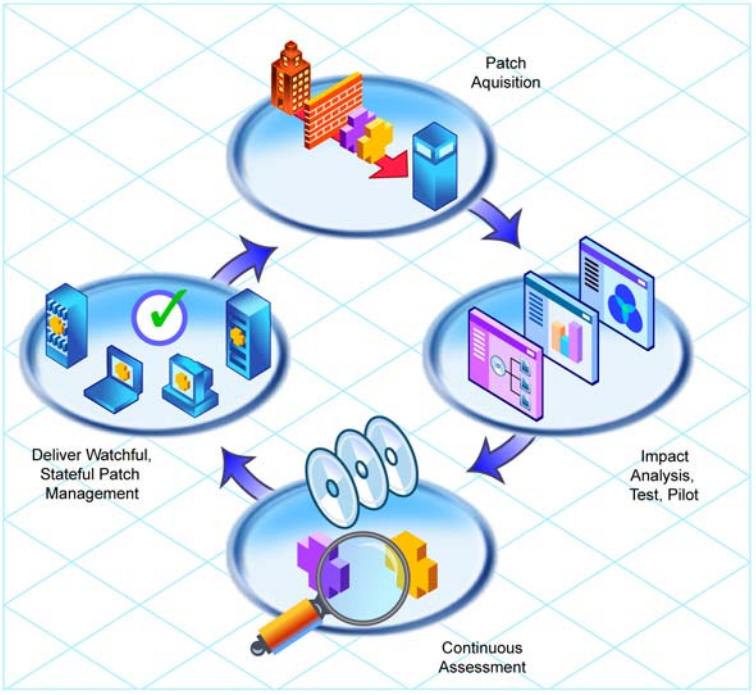
- **Compliance and Vulnerability Assessment**:
  automatic and continuous discovery of devices on the network, software products that are installed on each device, the security patches that are already applied by each software product, and identification of applicable software products. Through this complete discovery and assessment process, the IT administrator can understand the full scope of security vulnerability and system compliance at all times.

- **Deployment**:
  policy-based deployment capabilities that interface directly with a variety of existing policy sources such as Active Directory, LDAP, or SQL databases to enable automatic, rapid, and precise targeting of patches for deployment to servers, desktops, and laptops. HP Client Automation patented differencing, bandwidth optimization, multicast, and checkpoint-restart capabilities and multi-tiered infrastructure ensure

that security patches are deployed with minimal impact on network resources, and allow patches to be managed across an enterprise of any size.

- **Compliance and Assurance**:
  unique desired-state management that automatically and continuously ensures that security patches remain applied in their proper state as prescribed by policy. Devices and users are monitored and checked against policy and, if found to be out of compliance, are automatically adjusted to appropriate patch levels.

Figure 1 Patch Management life cycle



Using this Guide with Core and Satellite Servers

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

Terminology

The following terms are often used throughout this publication, and it may be helpful to become familiar with them before using this guide.

bulletin or security advisory

A bulletin is a security vulnerability reported by a vendor on one of its products. This term is used interchangeably with Red Hat and SuSE Security Advisories.

patch

A patch is a vendor-supplied binary file to be deployed and applied natively to fix the vulnerability. A bulletin can have multiple patches depending on the affected products, platforms, architectures, and languages.

Patch Manager Components

Patch Manager uses existing components of the HP Client Automation (HPCA) Infrastructure in addition to the Patch Manager Server. The following HPCA components are required:

- **Configuration Server**
  Applications and information about the subscribers and devices are stored in the Configuration Server Database (CSDB on the HP Client Automation Configuration Server (Configuration Server). The PATCHMGR Domain in the CSDB contains instances for patch management. The Configuration Server processes information received

from the Patch Manager Agent. The Configuration Server manages vulnerabilities based on policies established by the administrator. For more information, refer to the *HPCA Configuration Server Guide.*

- **Enterprise Manager**
  Use the HP Client Automation Enterprise Manager (Enterprise Manager) to deploy the Patch Manager Agent as part of the HPCA Agent, and to view the Patch Manager Dashboards or Reports. Refer to the *HPCA Enterprise Manager User Guide (Enterprise Manager Guide)* for more information.

- **Patch Gateway**
  The Patch Gateway is a component of the Patch Manager Server that supports lightweight Patch Distribution using Metadata on an HPCA Core Server. The Gateway downloads the patch binary data on request from the agent and caches it for other agents to use. Refer to the *HPCA Core and Satellite Enterprise User Guide* for more information.

- **Patch Manager Server**
  The Patch Manager Server acquires security patches from the Internet, loads them into the CSDB, and then synchronizes them with an SQL or Oracle Database for Patch Manager. The information on the patches and the vulnerabilities in your environment can be analyzed using Patch Manager reports. Patch Manager runs under its own service name: HPCA Patch Manager Server.

- **Patch Manager Agent**
  Install the Patch Manager agent on devices for which you want to manage vulnerabilities. The agent discovers products and patches eligible for management on devices.

- **Reporting Server**
  As part of the Client Automation extended infrastructure, the web-based HP Client Automation Reporting Server (Reporting Server) allows you to query the combined data in existing HP Client Automation SQL databases and create detailed reports. In addition, you have the option of mounting an existing LDAP directory, which allows you to filter your data using your LDAP directory levels. The Reporting Server interface provides a dynamic and intuitive way to use SQL data for reporting and overall environmental assessment. Refer to the *HP Client Automation Reporting Server Installation and Configuration Guide (HPCA Reporting Server Guide)* for more information.

- **Administrator CSDB Editor**
  The HP Client Automation Administrator CSDB Editor (CSDB Editor) gives an experienced administrator a user interface with which to view or edit service entitlement policies stored in the Configuration Server Database. For more information, refer to the *HP Client Automation Administrator User Guide (HPCA Administrator Guide).*

2 Creating the Patch Manager Environment

At the end of this chapter, you will:

- Be familiar with the tasks needed to set up the HP Client Automation Enterprise Patch Manager (Patch Manager) environment.
- Know how to modify the Configuration Server and Configuration Server Database.
- Be able to install the Patch Manager.
- Be able to access and use the Patch Manager Administrator Console for:
  - Configuration tasks
  - Acquisitions and Operations
  - Viewing Status and Logs
  - Online Help.

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

Patch Manager Implementation Tasks

Before setting up your environment for the Patch Manager, you must have already installed the latest version of the Configuration Server and either Microsoft SQL Server or Oracle.

Database Prerequisites for Microsoft SQL Server or Oracle

The Patch Manager database requires Microsoft SQL Server or Oracle.

- Install and use one of the supported versions of Microsoft SQL Server or Oracle as listed in the Database Server topic of the accompanying *Release Notes*.
- If using Oracle, you must use the Oracle Corporation's ODBC drivers specific to the precise Oracle version in your environment, not the Oracle ODBC drivers supplied by Microsoft.
- If using Oracle, HP also recommends that you verify that the Database Server, the Oracle Client, and the Oracle ODBC driver are *all* at the latest patch set level. Use the following procedures to find these Oracle versions in your environment.

To find the version of the Oracle Database:

- From the web-based Oracle Enterprise Manager: Access the **Home** tab, look in the **General** section next to **Version**.
- From Oracle Enterprise Manager Console: Select the database server in the tree, then **Instance** → **Configuration** → **General** tab. The Version is next to **DB Version**.
- From SQL*Plus: Login to the database server; if the version is not stated in the banner as you log in, then issue this command: **`SELECT * FROM V$VERSION`**

To find the version of the Oracle Client:

- From SQL*Plus: Log in to the database server, the version should be at top of window. For example:

```
SQL*Plus: Release 9.2.0.8.0 - Production on Tue Jan 8
12:10:232008
```

- From Windows Explorer: Navigate to `ORACLE_HOME\bin` (for example: `C:\Oracle\Ora92\bin`), right-click `oci.dll`, click **Properties → Version** tab, then use the **Item Name** list box to select **File Version**.

To find the version of the Oracle ODBC Driver:

- From ODBC Data Source Administrator: Open the ODBC Data Source Administrator (`odbcad32.exe`), select the **Drivers** tab and scroll to, for example: "Oracle in OraHome92". The version is in the Version column.
- From Windows Explorer: Navigate to `ORACLE_HOME\bin` (for example: `C:\Oracle\Ora92\bin`) and right-click on `SQORA32.DLL`. Click **Properties → Version** tab, then use the **Item Name** list box to select **File Version**.

Implementation Task List

To use the Patch Manager, you will need to complete the following tasks:

- Create the SQL or Oracle Patch Database and an ODBC DSN.
- Install the latest version of the Configuration Server. Refer to the *Client Automation Getting Started Guide.*.
- Install the Messaging Server on the Configuration Server. Refer to the *HPCA Messaging Server Installation and Configuration Guide*.
- Install the Administrator CSDB Editor. Refer to the *HPCA Administrator User Guide*.
- Run the Patch Manager installation. This installation includes:
  - Installing the Patch Manager Server
  - Installing the Configuration Server component updates required for Patch Manager
  - Installing the Configuration Server Database (CSDB) updates required for Patch Manager
  - Configuring Patch Manager options for use in your enterprise
  - Synchronizing the CSDB with the SQL or Oracle Database
- Add a Method Connection to your CSDB
- Install the Enterprise Manager. Optional. Refer to the *HPCA Enterprise Manager User Guide.*

- Install the Reporting Server. Refer to the *HPCA Reporting Server Installation and Configuration Guide.*.

Creating the Database for Patch Manager

Before installing Patch Manager, create a database using Microsoft SQL Server or Oracle. If you do not have security rights to create the database, contact your database administrator.

The required size will vary based on the number of patches and managed devices in your environment. The procedures below merely reflect recommendations.

To create a SQL Server database for Patch Manager

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

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

2 Use SQL Server Authentication.

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

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

The database owner name cannot be **sa** if you are using Windows Authentication.

4 On the computer that will host the Patch Manager Server, create an ODBC DSN with a name of your choice (for example, **PATCHMGR**) and point it to the new PATCH database on the SQL Server.

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

Install Microsoft Data Access Components (MDAC) on your Patch Manager Server. Download it from the Microsoft web site. The minimum version required is MDAC 2.8.

To create an Oracle database for Patch Manager

Ensure that your Oracle server ODBC driver versions precisely match your Core server; the connection to an Oracle database can fail if ODBC driver versions are mismatched.

For more information, contact your Oracle database administrator.

1 On the Oracle server, create a tablespace with the following recommended settings.

Tablespace Name	A name of your choice (for example, **PATCHDATA**)
Status	Online
Type	Permanent
Datafile	Fully qualified path and name of the data file, such as `patchdata.dbf`
Storage	Minimum Size 200 MB and Max size unlimited
Extent Management	Locally managed with automatic allocation
Segment Space Management	Automatic
Logging	No

2 Create a temporary tablespace with the following recommended settings.

Tablespace Name	A name of your choice (for example, **PATCHTEMP**)
Status	Online
Type	Temporary
Datafile	Fully qualified path and name of the datafile, such as `patchtemp.dbf`
Storage	Size 1000 MB

Tablespace Name	A name of your choice (for example, **PATCHTEMP**)
Extent Management	Locally managed with automatic allocation
Segment Space Management	Automatic
Logging	No

3 Create a user; associate the data and temporary tablespaces with the user with a default profile.

Username	A name of your choice (for example, **PATCH**)
Password	Create one based on your enterprise's security recommendations
Default tablespace	PATCHDATA
Temporary tablespace	PATCHTEMP
Profile	DEFAULT or a PROFILE NAME used for this schema
Roles	CONNECT and RESOURCE
System Privileges	CREATE ANY VIEW SELECT ANY TABLE UNLIMTED TABLESPACE UPDATE ANY TABLE

4 On the computer that will host the Configuration Server and Messaging Server, create an ODBC DSN with a name of your choice (such as, **PATCHMGR**) that is pointing to the new PATCH database on the Oracle server.

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

The database is now attached.

Installing the Administrator

The Configuration Server media contains an Administrator installation. Refer to *HPCA Administrator User Guide* for information on installing the Administrator components and using the CSDB Editor.

Installing the Patch Manager Server

System Requirements

- Identify a computer to act as your Patch Manager Server. It must be able to communicate with your Configuration Server, your ODBC Server, and the Internet. Patch Manager Server may be installed on a computer running one of the Windows Server versions identified on the accompanying *HP Client Automation Version 7.50 Release Notes*.

  To install the updates for the Configuration Server components and Configuration Server DB, you must run the Patch Manager installation program on the Configuration Server computer. These pieces cannot be installed over a network connection.

- The minimum version of Microsoft Data Access Components (MDAC) required is 2.8 on the Patch Manager Server.
- If you are using Oracle for your Patch Database, you must use the Oracle Corporation's ODBC drivers specific to the precise Oracle version in your environment, not the Oracle ODBC drivers supplied by Microsoft.

Installation

As of Version 5.10, Patch Manager must be installed into a path that *does not host* another HP Client Automation (HPCA) Infrastructure component or service; for example, it cannot be installed into a common Integration Server folder already hosting another HPCA component.

The default Patch Manager service name, and default port and install directory are given below:

- Service name: `httpd-patchmanager`
- Friendly service name: `Patch Manager Server`
- Default port: `3467`
- Default install directory:
  `C:\Program Files\Hewlett-Packard\CM\PatchManager`

The install allows for prompts to change the port and install path.

For migration details and options, refer to the *HPCA Patch Manager Migration Guide* located in the `\Migration` folder of the Patch Manager media.

To install the Patch Manager Server Components

1. Access the **Patch Manager** folder of the Client Automation Version 7.50 installation media.
2. Navigate to the `\extended_infrastructure\patch_manager_server\win32` directory and double-click **setup.exe**.

   The Welcome window opens.
3. Click **Next**. The HP Software License Terms window opens.
4. Click **Accept**. The New Installation / Migration window opens.
5. Select **New Installation** if this is a new installation of the Patch Manager. If you want to migrate from a prior Patch Manager Version, select **Migration**. Complete migration instructions can be found in the Patch Manager media's `\Migration` directory.

   If you are migrating, be sure to read the migration instructions before proceeding.

   The Select Components to Install window opens.

6 Select the components to install. If you are running the Patch Manager installation for the first time, you should check all the options.

— **Patch Manager Server**
Installs the Patch Manager Server, including the HPCA Integration Server executables `nvdkit` and `httpd.tkd`.

— **Configuration Server Component Updates**
Configuration Server Database Updates

To use the features of Patch Manager 7.50, you must select **Configuration Server Database Updates**. The PATCHMGR Domain, and only the PATCHMGR Domain, will be replaced, and all data in that domain removed.

The Configuration Server Components and Configuration Server DB Updates portions of the Patch Manager installation can only be run on the Configuration Server computer. These pieces cannot be installed over a network connection.

After applying the Configuration Server Database updates, also verify that the PATCHOBJ instance in your Configuration Server Database contains the correct connections. See Verify the Contents of the PATCHOBJ Instance in the Configuration Server Database on page 31.

After making your selections, click **Next**. The Warning window opens.

7 Click **Next** in the warning window. The Installation Folders window opens.

8 Type the location where the Configuration Server is installed, or click **Browse** to navigate to the location.

Type the location where you would like to install the Patch Manager Server, or click **Browse** to navigate to the location.

Where possible, accept the default for the Patch Manager server directory.

The Patch Manager Server cannot be installed into a directory that is hosting another HPCA component; it must be installed into its own directory.

9 Click **Next**.

10 Click **OK** to update the directory contents if you would like to continue.

The license file location window opens.

11 Type the location of your license file or click **Browse** to navigate to it.

12 Click **Next**. The HTTP Server IP Address window opens.

The HTTP Server IP address is used to open the Client Automation Patch Administrator page immediately following the installation.

13 Type the IP address of the Patch Manager Server, and click **Next**.

The HTTP Server Port window opens.

14 For the HTTP Server Port, accept the default or type an available port number for the Patch Manager Server, and click **Next**.

The port availability is checked.

If the selected port is not available, a Validation Failed dialog warns you; click **OK** and choose another port number.

The FINALIZE_PATCH service window opens.

15 Review the requirement to entitle all agents to the PATCHMGR.ZSERVICE.FINALIZE_PATCH service and click **Next**.

See Entitle the FINALIZE_PATCH Service on page 133 for additional details on entitling agents to the FINALIZE_PATCH service.

The summary window opens.

16 Verify the summary screen and click **Install**.

Read and answer any warning dialog boxes that appear. Which dialog boxes appear will depend on your configuration.

17 Click **Finish**.

The Configuration Server and its database have been updated, and the Patch Manager Server version 7.50 has been installed.

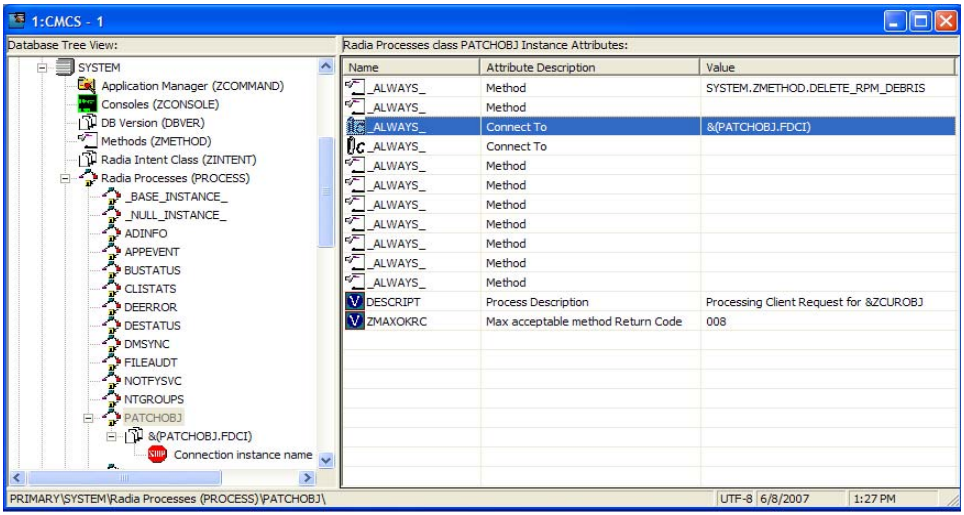
You should be directed to the **Client Automation Patch Administrator** page for final configuration and database synchronization. If you are not, open a web browser and go to: **http://<***patchserveripaddress***>:<***port***>/patch/manage/admin.tsp** to complete the configuration of Patch Manager and run a database synchronization.

Verify the Contents of the PATCHOBJ Instance in the Configuration Server Database

After updating the Configuration Server Database Components for Patch Manager, use the Administrator CSDB Editor to validate the contents of the PRIMARY.SYSTEM.PROCESS.PATCHOBJ instance in the Configuration Server database.

Display the PRIMARY.SYSTEM.PROCESS.PATCHOBJ instance and locate the Value for **&(PATCHOBJ).FDCI**. It must be defined as an _ALWAYS_ Connect To attribute, which looks like this:

The figure below shows the required connection type for **&(PATCHOBJ).FDCI.**



If &(PATCHOBJ).FDCI is found next to an _ALWAYS_ Method attribute, which looks like this:

copy and paste the value for **&(PATCHOBJ).FDCI** into an _ALWAYS_ Connect To attribute, and then delete the value from the _ALWAYS_ Method attribute.

Attribute values must be in uppercase.

An incorrect connection type can occur when the first three lines of the class definition for PRIMARY.SYSTEM.PROCESS have been customized from the HP-supplied default.

Configuring Patch Manager using the Patch Manager Administrator

The HP Client Automation Patch Manager Administrator (Patch Manager Administrator) includes a **Configuration** area which provides an interface to the Patch Manager Server settings file, `patch.cfg`.

The **Configuration** area settings are grouped into the following three areas:

- Expand **Environment Settings** to enter:
  - — Infrastructure Settings on page 34
    Use this panel to define and test the connecting to the Configuration Server and your Patch ODBC DSN, the Reporting Server and the external HP Patch Update Site.
  - — Proxy Settings on page 37
    Use this panel to define an HTTP or FTP Proxy Server.
  - — Agent Options on page 38
    Use this panel to configure Patch Agent options for your Microsoft managed devices. The options include: Enable Download Manager; Disable Automatic Updates; Delete the SoftwareDistribution Folder; and Manage Installed Bulletins (-mib).
- Expand **Acquisition Setting** to specify:
  - — Agent Updates on page 42
  - — Preferences on page 43
  - — Vendor Settings on page 45
- Click **Acquisition Jobs** to define jobs to acquire vendor bulletins. See Configure Acquisition Jobs on page 74.

Use the Patch Manager Administrator to enter or modify these settings.

To access and use the Patch Manager Administrator

1. From your web browser, go to **http://***patchserver_ip_address***:***port***/patch/manage/admin.tsp**.
2. Type or select the values for the Configuration area settings and parameters you want to enter or modify. Any setting that ends with an asterisk (*) is *required*. For detailed information on the available settings, see the information for the Configuration Settings that follow.
3. Click **Save** to save and apply the configuration changes to the Patch Manager Server. During this action, the Patch Manager Server will be initialized with the new configuration settings. During initialization, the Patch Manager establishes a connection to the DSN Name specified in the ODBC DSN settings. This connection must be established prior to an acquisition or synchronization so that the information is current.

To use the Patch Manager Administrator Online Help

Context sensitive online help is available throughout the Patch Manager Administrator.

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

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

Table 1 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.

Table 1 Online Help Navigation Tools

Button	Description
Contents	Display the table of contents.
Index	Display the alphabetical index of help topics.
Search	Search all online help topics for a keyword or phrase.

Infrastructure Settings

Use the **Environment Settings** group > **Infrastructure settings** page to configure parameters for the HP Client Automation components. The settings prompt for the HP Configuration Server, Data Source Name (DSN), HP Patch Manager Update Site, and the HP Client Automation Reporting Server alias. Where applicable, installation default values are displayed.

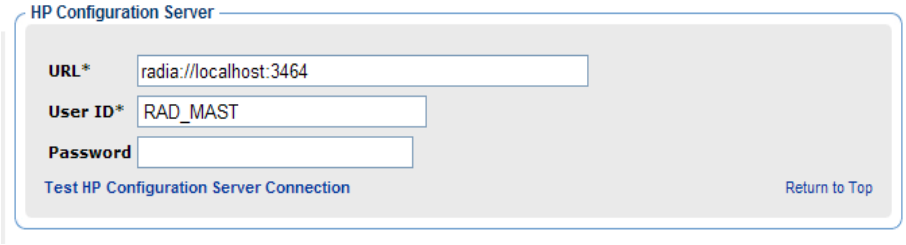
HP Configuration Server Settings

The following settings are configured in the HP Configuration Server section. Click the **Advanced** tab to expose Advanced-only fields.

Basic and Advanced Fields

- **URL**: Specify the location of your Configuration Server using the format: `radia://`*`ipaddress`* or *`hostname`*`:`*`port`*.
- **User ID**: Specify the Administrative User ID for accessing your Configuration Server.
- **Password**: If password authentication has been enabled on your Configuration Server, specify the password for the **User ID**.
- **Test HP Configuration Server Connection**: You can test your Configuration Server connection from the Patch Manager Administrator. To do this, click **Test HP Configuration Server Connection**. When prompted, click **Test Connection**. Wait for the results. If the values specified on the test page are

different than the original values, and your test is successful, click **Apply Changes** to copy the new values back to the Configuration page. The new settings can then be saved and applied to the Patch Manager Server.



ODBC DSN Settings

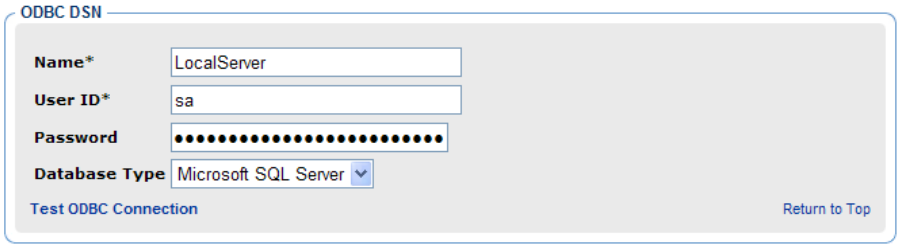
The following settings are configured in the ODBC DSN section:

- **Name***: Specify the Data Source Name (DSN) for the Patch Manager SQL or Oracle database.
- **User ID***: Specify the user for the dsn for the Patch Manager ODBC database.
- **Password**: Specify the password for the User ID of the Patch Manager ODBC database.
- **Database Type**: Specify the database type. This is the same as the db_type parameter in `patch.cfg`. The two possible values are `mssql` for Microsoft SQL Server and `oracle` for Oracle. Mssql is the default value for a new installation.

  If you are using Oracle, change this value to `oracle` before doing a patch acquisition or database synchronization.

- **Test ODBC Connection**: You can test your ODBC connection in the Patch Administrator. To do this, click **Test ODBC Connection**. When prompted, click **Test Connection**. Wait for the results. If the values specified on the test page are different than the original values, and your test is successful,

click **Apply Changes** to copy the new values back to the Configuration page. The new settings can then be saved and applied to the Patch Manager Server.



Advanced-only Fields

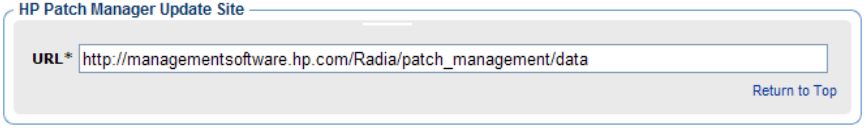
Click Advanced tab to see the entries for the HP Patch Manager Update Site and HP Client Automation Reporting Server Settings.

HP Patch Manager Update Site

The following setting is configured in the HP Patch Manager Update Site section:

- **URL***: Specifies the URL to connect to the HP Patch Manager Update web site provided by HP. The default is: **http://managementsoftware.hp.com/Radia/patch_management/data**

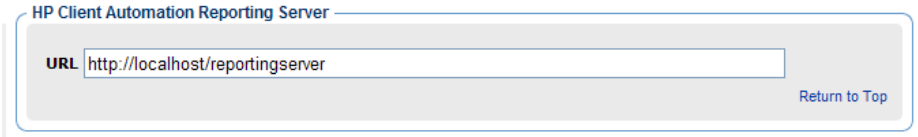
  There is no need to alter this installation default.



HP Client Automation Reporting Server Settings

This setting specifies the URL location (alias) of the HP Client Automation (HPCA) Reporting Server. Click the Reporting icon in the toolbar area of the Patch Manager Administrator page to gain access to the Reporting Server used to display Patch Reports.

- **URL**: Specify the location of the Reporting Server you are using for your Patch Manager.



Proxy Settings

Use the Proxy Settings page to configure your HTTP and FTP proxies for your enterprise.

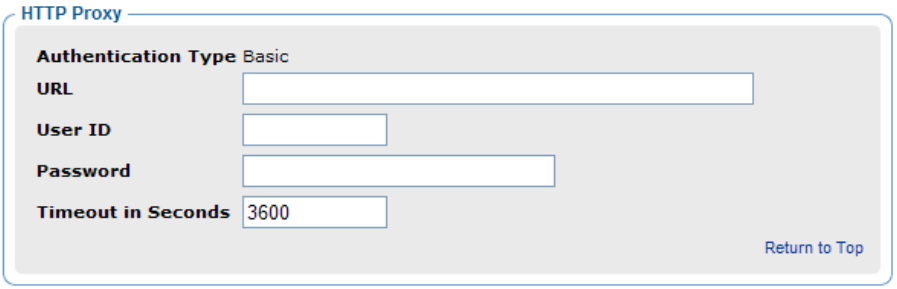
To accces the Proxy Settings page from the Patch Manager Administrator, use the **Configuration** area to expand **Environment Settings**, and then click **Proxy Settings**.

HTTP Proxy Settings

The following settings are configured in the HTTP Proxy Settings section:

- **Authentication Type**: Basic. This parameter is not configurable.
- **URL**: If you use a proxy server for http traffic, specify its URL in the format **`http://`***`ip`***`:`***`port`*.
- **User ID**: If you use a proxy server for http traffic, and the proxy requires authentication credentials, specify your user ID.
- **Password**: If you use a proxy server for http traffic, and the proxy required authentication credentials, specify your password.
- **Timeout in Seconds**: Set the total amount of time to wait for the file to be completely downloaded. If an acquisition session is unable to download the file in this time, then the acquisition will abort the current http location, and will continue the acquisition with the next http location.

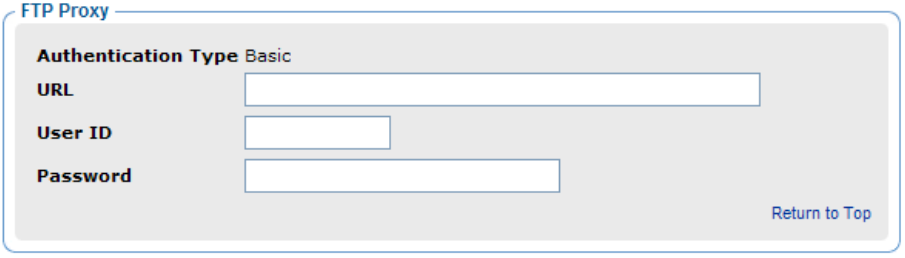
Increase the http_timeout if you need to allow additional time for a bulletin to download. Http_timeout is displayed in administrator interface in seconds, but stored in `patch.cfg` in milliseconds.



FTP Proxy Settings

The following settings are configured in the FTP Proxy Settings section.

- **Authentication Type**: Basic. This parameter is not configurable.
- **URL**: If you use a proxy server for ftp traffic, specify its URL in the format **`ftp://`***`ip`*`:`*`port`*.
- **User ID**: If you use an ftp proxy for ftp traffic, and the proxy requires authentication credentials, specify your user ID.
- **Password**: If you use an ftp proxy for ftp traffic, and the proxy requires authentication credentials, specify your password.



Agent Options

These Agent Options apply to patching Microsoft devices, only.

Use the Agent Options available from the Patch Manager Administrator's Configuration > Infrastructure Settings group to enable and configure these Patch Manager Agent options for patching Microsoft Devices.

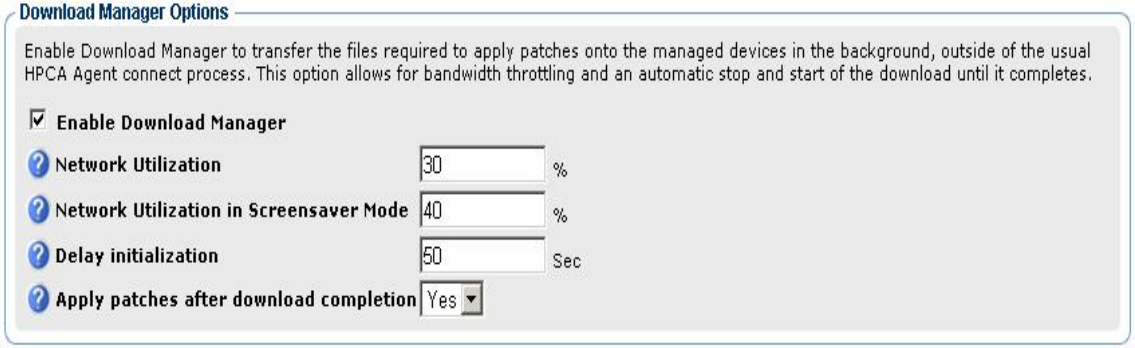
The next time the Patch Agents connect to the HPCA servers they will receive any configuration changes that you set on these panels.

- Download Manager Option on page 39
- Agent Options for Patch Agents on page 41

Download Manager Option

- **Enable Download Manager**: Check this box to have Download Manager control the download of the required patch files onto the Agent machines usng a background, asynchronous process. The Download Manager operates outside of the normal HPCA Agent Connect process.

  When checked, several Download Manager options are displayed.



Complete the Download Manager Options using the following information.

Set specific options for network utlization, network utilization in Screen Saver Mode, delay after initialization, and whether or not to apply the patches after download completion.

.

Table 2 Download Manager Options for Patch Agents

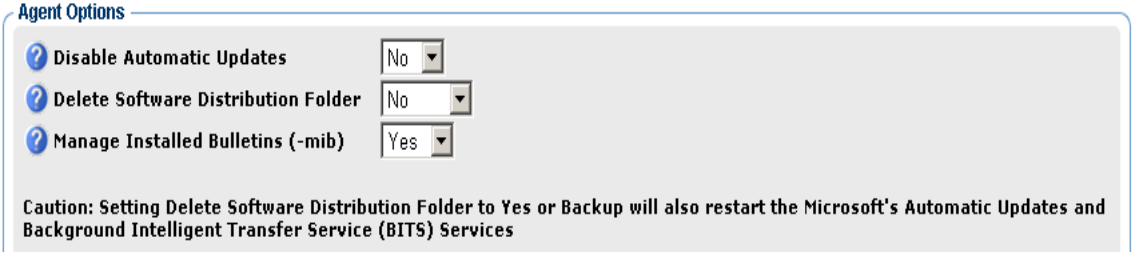
Option and Valid Values	Description
Network Utilization Values = 0 to 100 % 0 is default	Specifies the maximum percent of available network bandwidth to use to download the patch files when the device is active. A value of 0 means the download will use the available network bandwidth. Example: 25 specifies no more than 25% of the available bandwidth should be used for the patch download process.
Network Utilization in Screensaver Mode Values = 0 to 100 % 0 is default	Screen Saver network utilization option. Specifies the maximum percent of available network bandwidth to use to download the patch files when Screen Saver is on. This is typically a larger percent than when Screen Saver is off. A value of 0 means the download will use the available network bandwidth when Screen Saver is on. Example: 80 increases the bandwidth used to download the patch files 80% when screen saver is on.
Delay initialization Values = 0 to 999 seconds 0 is default	Upon initialization, specifies the number of seconds to delay before starting or resuming the download of patches. This allows other processes to startup first, and then resume the patch download. Example: Set to 15 to delay initialization 15 seconds. A value of 0 means there is no delay.
Apply patches after download completion Values = Yes or No (default)	After download completion, set to Yes to trigger a Patch Agent Connect to apply the patches. HP recommends setting the value to Yes. Leave the default of No to have the patches applied whenever the next Patch Agent Connect takes place.

Click Save to set these configuration options. The Patch Agents will receive the new configuration the next time they connect to the HPCA servers.

Agent Options for Patch Agents

The following Agent Options are available for patching Microsoft devices.

- **Disable Microsoft Automatic Updates**: Select Yes or No from the drop-down box. Use this option to address issues whereby the Patch Agent scan or deployment is getting interruped because Automatic Updates is set to ON.
  - **Yes**: The Patch Agent will disable Microsoft Automatic Updates before each scan or deployment. Once Patch scan/deployment is done, it reverts the Automatic Updates to its original state.
  - **No**: (The default) The Patch Agent will not disable Automatic Updates before each scan or deployment..



- **Delete Software Distribution Folder**: Select Yes, Backup, or No from the drop-down box. This option is available to address the following issues:
  - Drastic growth in the size of the SoftwareDistribution folder
  - SoftwareDistribution folder corruption
  - Increased load on the Configuration Server during Patch connects

  Setting Delete Software Distribution folder to Yes or Backup automatically restarts the services for Microsoft Automatic Updates and BITS. HP warns against setting this option if the service restarts will cause issues in your environment, especially for those customers who are using both HPCA Patch Management and Automatic Updates as co-located patch solutions.

  Set this option to Yes or Backup to improve Patch Manager performance due to folder size, corruption, or infrastructure load issues.

  - **Yes**: The Patch Agent deletes the contents of the SoftwareDistribution folder before every patch scan. Read the Caution (above) on service restarts.

— **Backup:** The Patch Agent first backs up and then deletes the contents of the SoftwareDistribution folder before every patch scan. Read the Caution (above) on service restarts.

— **No: (Default)** The Patch Agent will not do anything to the SoftwareDistribution folder.

- **Manage Installed Bulletins (-mib)**: Select None, No, or Yes from the drop-down box. This option controls how bulletins already installed on the target devices are handled.

  — **None: (Default)** Manage Patch Manager-installed bulletins only, and do not check the service library or binary resources for alternatively installed bulletins. This is the default behavior since there is no impact on the client agent in terms of vulnerability or re-patching, and it offers greater performance.

  — **No:** Manage Patch Manager-installed bulletins only; do not manage bulletins installed by an external source.

  — **Yes**: Manage all installed bulletins, whether installed by Patch Manager or an external source. This option is resource intensive.

Click **Save** to set the configuration options. The Patch Agents will receive the new configuration the next time they connect to the HPCA servers.

Agent Updates

Use Agent Updates to configure agent updates for Patch Management.

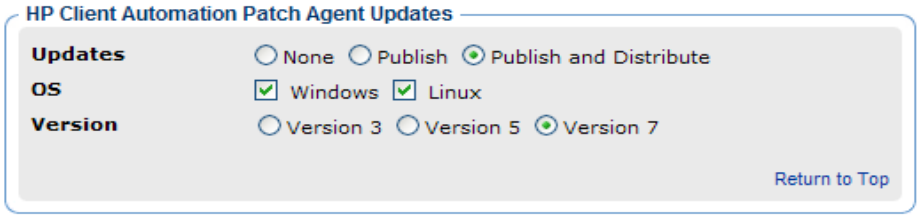
From the Patch Manager Administrator, access HP Patch Agent Updates settings from the **Configuration** area **Acquisition Settings** group. Click **Agent Updates**.

These settings are used to acquire and apply maintenance for HP Client Automation (HPCA) Patch Manager agent files. For more information on this, see Updating the Patch Manager Agent on page 9.. The following settings are configured in the HP Patch Agent Updates section.

- **Updates**: If you select Publish, the updates will be published to the PATCHMGR Domain, but will not be connected for distribution (deployment) to Patch Manager target devices. You will need to create these connections. If you select Publish and Distribute, the updates will be published to the PATCHMGR Domain and connected to the DISCOVER_PATCH instance. This option will distribute the updates to your Patch Manager target devices.

- **OS**: Specify the vendor operating system types for which you wish to acquire and manage Patch Manager agent updates.
- **Version**: Select the Patch Manager Version for which you would like to acquire agent updates. You can only publish one version to one Configuration Server. The default is the latest available Version.

  If you are installing Patch Manager for the first time, do not modify the Version parameter from the installation default.



Preferences

Under Preferences, configure vendors and acquisition settings. These settings will be reflected in the Vendor Settings and Acquisition Jobs.

- **Enable Patch Management For**: Specify the OS vendors you will be acquiring patches for. These vendors will be represented in Vendor Settings and Acquisition Settings. If you decide at a later date to acquire patches for additional vendors, they must be enabled here, first.
- **Save Acquisition Summary**: Specify how long in days to keep the Patch Auth Store (PASTORE) instances. This class contains one instance for each patch acquisition session. If this value is smaller than the Save History Detail value, then Save History Detail will be set to the value for Save Acquisition Summary. The value 0 means never delete any history of Patch Acquisition.

  HP recommends that you specify the **Save Acquisition Summary** and the **Save History Detail** values in the Patch Manager Administrator interface, and does not recommend specifying these parameters in command-line driven acquisitions.

- **Save History Detail**: Specify how long in days to keep the Publisher Error (PUBERROR) instances. This class contains one instance for each patch acquisition error.
- **Patch Data Repository Path**: The directory where patches are downloaded to before they are published to the Configuration Server. If you choose to perform an acquisition using a directory that is pre-populated with data from a previous acquisition, specify the pre-populated directory path in this parameter.
- **Retired Bulletins**: Shows the bulletins to retire separated by commas. This parameter works on the bulletin level, not at the product or release level.

  The retire function performs these functions.

  — Deletes specified bulletins if they exist in the Configuration Server DB during the current publishing session.

  — Does not publish the bulletins specified in the retire parameter to the Configuration Server DB during the current publishing session. The use of the Retire option supersedes the Bulletins option.
- **Excluded Products**: Precede any products you want excluded with an exclamation point (!) in the format of *vendor*::*product* in a comma separated list. If an include filter is not set, all products are assumed. If you provide any included filters, then the excluded filters will be a subset of the included products. Be sure to conform to the vendor's naming standards. For example, Microsoft refers to Internet Explorer using its full name, rather than a common abbreviation such as IE. For example, to include all Windows products except Windows 95, type `{Microsoft::Windows*,Microsoft::!Windows 95}`.

For new Patch Manager installations, the acquisition and management of Security patches for the following products are *excluded, by default*: Microsoft Office, Windows 95, Windows 98, Window Me,andMicrosoft Office products, and SuSE specific products *-yast2, *-yast2-*, and *-liby2 The automated

management of SuSE OS yast specific products are not supported by Patch Manager.

If you are migrating from a previous version of Patch Manager and did not remove your `patch.cfg` before migration, if you wish to exclude all Microsoft Office products or their standalone versions from Patch Manager acquisition and management, append the following text to your product exclusion list:

",!Access*,!Excel*,!FrontPage 200[023],!FrontPage 9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,!Project 200[023],!Project 98,!Publisher*,!Visio*,!Word*,!Works*"

Note the text shown above is all one line and the quotes displayed above are *not* to be included in the user interface Excluded Product text box.

- **Allow Internet Access:** Select Yes or No from the drop-down box. Use this option to specify whether the Patch Manager Server is to be allowed access to the internet.
  - **Yes:** (Default) Patch Manager will access the internet during acquisitions.
  - **No:** Patch Manager will not access the internet during acquisitions. In this case, only the bulletins (metadata and binaries) that already exist in the data folders are published.
- **Default Patch Acquisition Download Language**: Specify the languages for which you want to acquire and manage security patches. The default is en (English).

Vendor Settings

Vendor Settings displays vendor-specific URLs and other options required for patch acquisition and management activities on the agents in your enterprise.

From the Patch Manager Administrator, access Vendor Settings from the **Configuration** area, **Acquisition Settings** group.

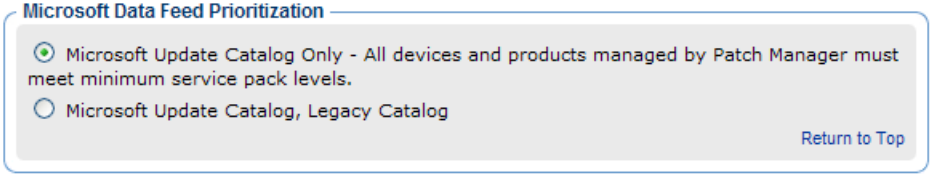
Before entering Vendor Settings, first use the Acquisition Settings, Preferences page to enable the appropriate vendor(s) and OS selections.

If you change vendor settings from one acquisition session to the next so that you exclude one or more products or operating systems that were previously selected, all patches specific to the excluded products or operating systems will be removed from the Configuration Server Database. This also means the excluded products or operating systems are no longer eligible for vulnerability assessment and management. This applies to all vendors.

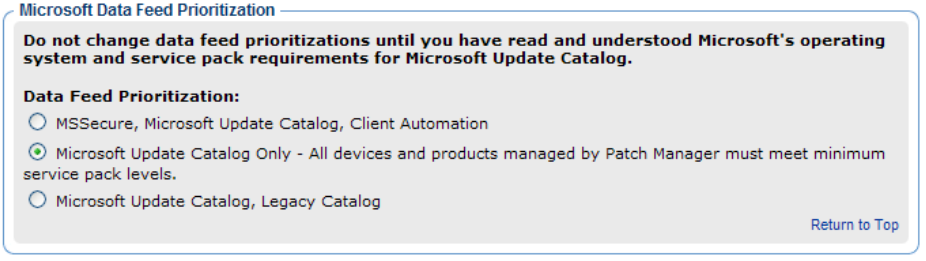
Microsoft Data Feed Prioritization

The following Microsoft Data Feed Prioritization settings are configured in the Vendor Settings section to support and prioritize the available Microsoft update repositories and methods for acquisition and download.

When the Patch Distribution Settings have the option to **Enable Download of Patch Metadata only** turned on, you have the option to choose one of the Microsoft Update Catalog data feeds.



When the Patch Distribution Settings have the option to **Enable Download of Patch Metadata only** turned off, the Microsoft Data Feed Prioritization panel includes three choices:



See About Microsoft Patch Acquisition and Management on page 65 and About Microsoft Automatic Updates on page 67 for important information related to Microsoft patch management activities.

- **MSSecure, Microsoft Update Catalog, Client Automation**: This option is displayed when the Patch Metadata Download option is turned off. Patches are acquired from both MSSecure and Microsoft Update Catalog. If a patch exists in both the MSSecure and Microsoft Update Catalog, then the technologies supporting MSSecure are used.

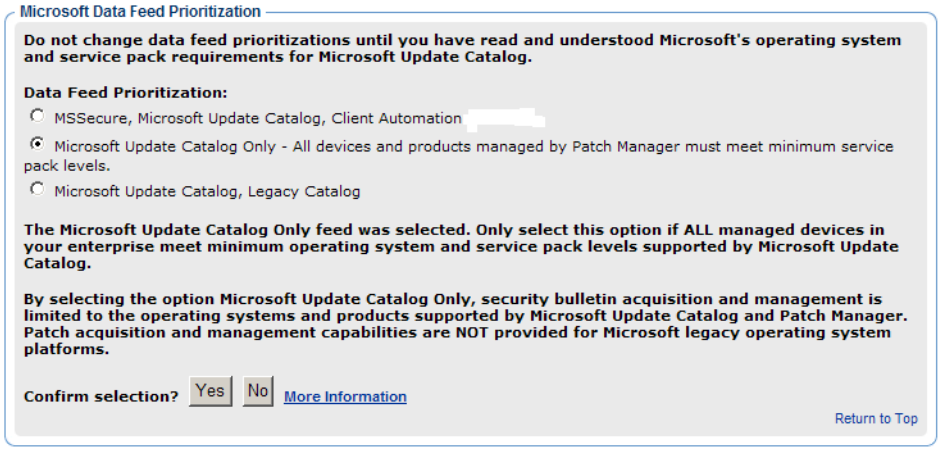
  Due to MSSecure technologies, this option cannot patch devices running Windows Vista (32-bit or 64-bit) or Windows on 64-bit architectures. To patch these devices, choose a Data Feed Prioritization that includes Microsoft Update Catalog.

  At the time of this writing, Microsoft's web site states that MSSecure.xml will no longer be updated after October 9, 2007, although they have continued to update their legacy catalog into 2008. See About Microsoft Patch Acquisition and Management on page 65.

- **Microsoft Update Catalog Only**: (Default option) All patches are acquired from the Microsoft Update Catalog. To use this option, all devices in the enterprise must meet minimum operating system and product levels as set by Microsoft. Devices not meeting these minimum requirements will not be patched.

If you change to this option, the following warning message will open, which you must accept to continue.



When you click **Yes**, you will again be prompted to make sure that this is the option you want. Click **Save** to confirm.

- **Microsoft Update Catalog, Legacy Catalog:** Patches are acquired from the Microsoft Update Catalog and an HP repository containing current MSSECURE and HP-corrected metadata, referred to as the Legacy Catalog. If a patch exists in both the Microsoft Update Catalog and the Legacy repository, then:
  - If the target device meets the minimum OS requirements supported by Microsoft Update Catalog, the device will be patched by leveraging Microsoft Update Catalog and Windows Update Agent technologies.

— If the target device does not meet the minimum OS requirements supported by Microsoft Update Catalog, the device will be patched using MSSecure technologies, using meta data hosted in the Legacy Catalog.

The HP Legacy Catalog will continue to be updated by HP as new patches are added to MSSecure. Patches hosted in the HP Legacy Catalog may require HP metadata correction. If you choose to enable the **Microsoft Update Catalog, Legacy Catalog** option Microsoft security bulletins deemed applicable to legacy Microsoft Operating systems (including Service Pack variants) and Microsoft products will have a "_L" appended to the Microsoft bulletin name for identification purposes within the Configuration Server PATCHMGR Domain as well as Patch Manager reports as viewed through the Reporting Server.

Office patches that are acquired and managed using Microsoft Update Catalog technologies will not detect if Office Applications are managed by HP Client Automation Application Self-service Manager or an Administrative Control Point. In either case, if a bulletin affecting an Office application is entitled to a device, Patch Manager will manage the Office patch and install it locally on the devices that are vulnerable.

Microsoft Feed Settings

The following settings are configured in the Vendor Feeds section:

Advanced-only Fields

- **MSSecure***: Specifies the URL for Microsoft's MSSecure cabinet file which contains the Microsoft supplied `MSSECURE.XML` file.

  Default: **http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB**

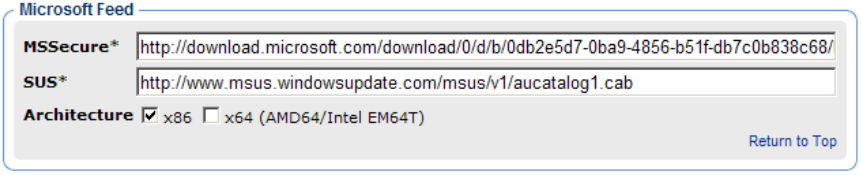
  At the time of this writing, Microsoft Knowledge articles suggest Microsoft plans to discontinue support and updates for `MSSecure.xml` after October 9, 2007 even though they have continued to update this catalog into 2008. See About Microsoft Patch Acquisition and Management on page 65.

- **SUS***: Specifies the URL for the Microsoft cabinet file that contains the Microsoft SUS data feed.

Default: **http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab**

Basic and Advanced Fields

- **Architecture**: Select the architectures for the acquisition of Microsoft patches. The supported architectures include:
  - **x86** for 32-bit Intel architectures
  - **x64** for AMD64 or Intel EM64T. If this target architecture is selected, your Microsoft Data Feed Prioritization must be set to either **Microsoft Update Catalog Only** or **Microsoft Update Catalog, Legacy Catalog**.



Red Hat Feed Settings

The following settings are configured in the Red Hat Feed section:

Advanced-only Fields

- **Red Hat**: Specifies the URL for the Red Hat Network data feed. The default is **http://xmlrpc.rhn.redhat.com/XMLRPC**.

Basic and Advanced Fields

- **Publish Package Dependencies**: Specify **yes** if you want to publish additional Red Hat packages that downloaded security advisories may depend on. The default is No.

  Prerequisite, or dependent, Red Hat packages required to install Red Hat Security Advisories can be acquired from two places. They can either be downloaded from the Red Hat Network during acquisition or they can be found locally if previously copied from the Red Hat Linux installation media. During an acquisition, Patch Manager will first look for the .rpm packages in the appropriate directory. For example:

  - For Red Hat Enterprise Linux 4ES on x86, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/4es`.

— For Red Hat Enterprise Linux 4ES on x86-64, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/4es-x86_64`.

— When naming the `data/patch/redhat/packages/` subdirectories, refer to the list of **OS Filter Architecture** values below. Use the applicable folder name based on the value following `REDHAT::` as the subdirectory name.

If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, HP recommends copying the dependency packages to the appropriate packages directory from your Linux installation media. The Red Hat RPM packages can be found on the Linux installation media under the `RedHat/RPMS` directory.

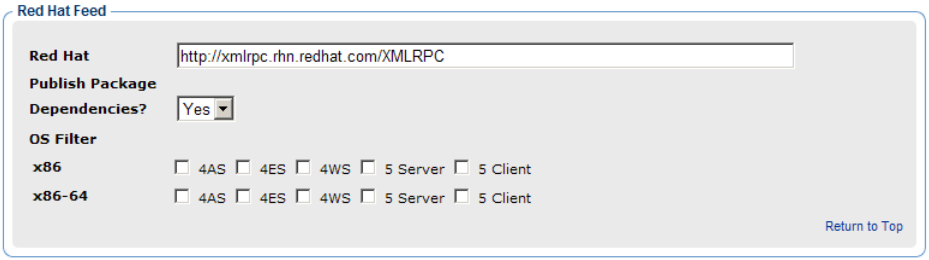
- **OS Filter**: Support is provided for x86 (32-bit Intel) and x86-64 (Opteron/EMT64) architectures for: all combinations of Red Hat Version 4 and Releases AS, ES and WS, and all combinations of Red Hat Version 5 Releases for Servers and Desktop clients. For a given architecture, select the operating system and release combination for the acquisition of Red Hat patches.

  — **x86** Architectures: Possible values for Red Hat x86 architectures in the `patch.cfg` file are:

  ```
  REDHAT::4as,      REDHAT::4es,     REDHAT::4ws,
  REDHAT::5server,   REDHAT::5client
  ```

  — **x86-64** Architectures: Possible values for Red Hat x86-64 architectures in the `patch.cfg` file are:

  ```
  REDHAT::4as-x86_64,     REDHAT::5server-x86_64,
  REDHAT::4es-x86_64,     REDHAT::5client-x86_64,
  REDHAT::4ws-x86_64
  ```



SuSE Feed Settings

To configure settings for patching SuSE Linux, choose the SuSE Feed Setting for the Version Levels and OS platforms that are in your environment. SuSE 9 feed settings are entered separately from SuSE 10 and 11 feed settings. SuSE 10 and 11 feed settings also include a Product Type selection for Enterprise Desktop and Enterprise Server.

Related Topics:

- SuSE Patch Acquisition Requirements on page 71

Switch from the Basic to Advanced settings if you also need to set or fix the URLs for the SuSE meta data feeds.

SuSE 9 Feed Settings

Click **Advanced** to view or modify the default URLs for SuSE 9 feed settings that are listed below.

Advanced-only Fields

- **SuSE 9**: Specifies the secure URLto acquire security advisory meta data for SuSE 9. The defaults are:

  https://you.novell.com/update/i386/update/SUSE-CORE/9/
  https://you.novell.com/update/i386/update/SUSE-SLES/9/

- **SuSE 9-x86_64**: Specifies the secure URL for acquiring updates for SuSE 9 on AMD64 or Intel EM64T architectures. The defaults are:

  https://you.novell.com/update/x86_64/update/SUSE-CORE/9/
  https://you.novell.com/update/x86_64/update/SUSE-SLES/9/

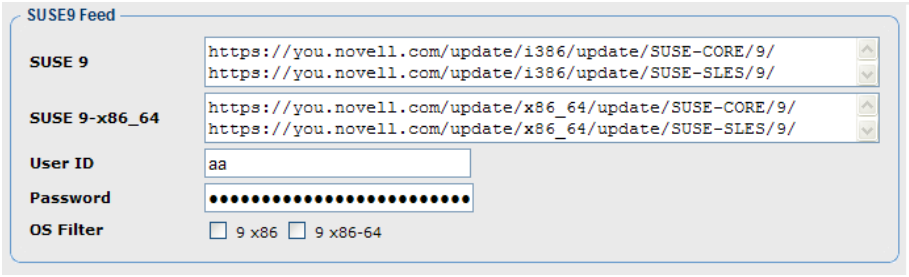
Basic and Advanced Fields

Use the Basic or Advanced page to enter the required settings for obtaining SuSE 9 Data Feeds.

- **UserID**: Specifies your SuSE user ID. Obtain a user id from the vendor.
- **Password**: Specify the password for the SuSE UserID.
- **OS Filter**: Select the operating system version and architecture combinations for the acquisition of SuSE Linux Enterprise Server patches. Support is provided for SuSE Versions 9 on x86 (32-bit) architecture as well as x86-64 (AMD64 and Intel EM64T) architectures.

  The valid OS Filter value for x86 architectures in patch.cfg is `suse::9`.

  The valid OS Filter values for x86-64 architectures in patch.cfg is `suse::9-x86_64`.



SuSE 10 and 11 Feed Settings

Use the field on the **Basic** view to enter the required feed settings to acquire security advisory patches for SuSE 10 and 11 devices.

Click **Advanced** to view or modify the default URLs for SuSE 10 and 11 feed settings that are listed below.

Advanced-only Fields

- **SUSE 10**: Specifies the secure URL to acquire security advisory meta data for SUSE 10 (SLES10 and SLED10) on x86 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-i586/

- **SUSE 10SP1:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 1 on x86 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-i586/

- **SUSE 10SP2**: Specifies the secure URL for acquiring updates for SUSE 10 (SLES10 and SLED10) Service Pack 2 on x86 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-i586/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-i586/

- **SUSE 10-x86_64**: Specifies the secure URL to acquire security advisory meta data for SUSE 10 (SLES10 and SLED10) on x86-64 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-Updates/sled-10-x86_64/

- **SUSE 10SP1-x86_64:** Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 1 on x86-64 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP1-Updates/sles-10-x86_64
  https://nu.novell.com/repo/\$RCE/SLED10-SP1-Updates/sled-10-x86_64/

- **SUSE 10SP2-x86_64**: Specifies the secure URL for acquiring updates for SUSE 10 (SLES 10 and SLED 10) Service Pack 2 on x86-64 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES10-SP2-Updates/sles-10-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED10-SP2-Updates/sled-10-x86_64/

- **SUSE 11**: Specifies the secure URL to acquire security advisory meta data for SUSE 11 (SLES11 and SLED11) on x86 architectures.

Defaults:
https://nu.novell.com/repo/\$RCE/SLES11-Updates/sle-11-i586/
https://nu.novell.com/repo/\$RCE/SLED11-Updates/sle-11-i586/

- **SUSE 11-x86_64**: Specifies the secure URL to acquire security advisory meta data for SUSE 11 (SLES11 and SLED11) on x86-64 architectures.

  Defaults:
  https://nu.novell.com/repo/\$RCE/SLES11-Updates/sle-11-x86_64/
  https://nu.novell.com/repo/\$RCE/SLED11-Updates/sle-11-x86_64/

Basic and Advanced Fields

Use the Basic or Advanced page to enter these required settings for obtaining SuSE 10 and 11 Data Feeds. SuSE Versions 10 and 11 support includes two product types: Enterprise Server and Enterprise Desktop.

All combinations of Product Type and OS Filters selected on this page will be available for SuSE acquisitions. Prior to running an acquisition, you can use the Exclusion option to omit any combinations that you do not want to acquire.

- **Product Type**: For SUSE 10 or 11, select the SUSE Linux product types installed on the devices in your environment.
  - **Enterprise Server:** Specifies the SUSE Linux Enterprise Server (SLES) product type. To obtain SLES 10 or SLES 11 security advisories, check the Product Type of Enterprise Server.
  - **Enterprise Desktop:** Specifies the SUSE Linux Enterprise Desktop (SLED) product type. To obtain SLED 10 or SLED 11 security advisories, check the Product Type of Enterprise Desktop.
- **UserID**: Specifies your SUSE 10 or SUSE 11 user ID. Obtain a user id from the vendor. For details, see SuSE Patch Acquisition Requirements on page 71.
- **Password**: Specify the password for the SUSE UserID.
- **OS Filter**: Select the operating system *version*, *service pack* and *architecture* combinations for the acquisition of SUSE Version 10 and 11 patches. Support is provided for:
  - SUSE Version 10 base and Service Packs 1 and 2 on x86 (32-bit) architectures, as well as SUSE Version 10 base and Service Packs 1 and 2 on x86-64 (AMD64 and Intel EM64T) architectures.

— SUSE Version 11 base on x86 (32-bit) and x86_64 (AMD64 and Intel EM64T) architectures.

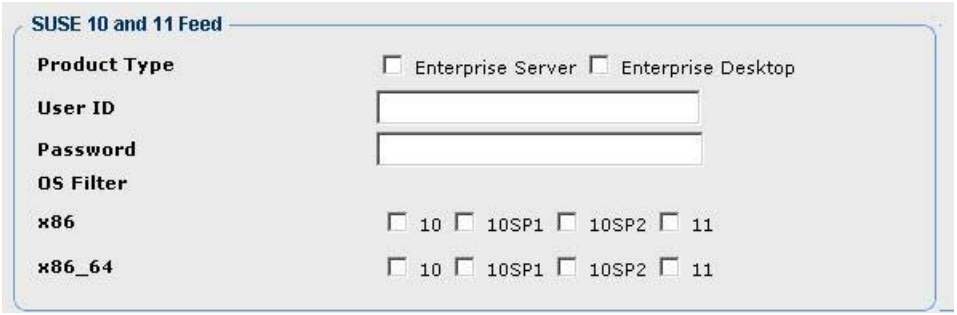
Valid SUSE 10 OS Filter values for x86 architectures in patch.cfg are: `suse::10, suse::10SP1,` and `suse::10SP2`.

Valid SUSE 10 OS Filter values for x86-64 architectures in patch.cfg are: `suse::10-x86_64`, `suse::10SP1-x86_64` and `suse::10SP2-x86_64`.

Valid SUSE 11 OS Filter values x86 architectures in patch.cfg are: `suse::11`.

Valid SUSE 11 OS Filter values for x86-64 architectures in patch.cfg are: `suse::11-x86_64`.

.



Patch Configuration Settings File

If you are unable to use the Patch Manager Administrator, you can make changes directly in the `patch.cfg` file, located in the `\etc` folder of where you installed the Patch Manager Server.

The default location is: *`System Drive`*`:\Program Files\Hewlett-Packard\CM\PatchManager\etc`.

See Appendix D, Patch.cfg Parameters for more information.

View Logs

The Patch Manager Server logs can be used to review and troubleshoot the patch management environment. These logs are available online from the Patch Manager Administrator.

From the Patch Manager Administrator console, go to the **Status and Logs** area and click **View Logs**.

Select a Log File from those listed to open and review it online, or to save it locally and review it with HP support.

- **`httpd-patchmanager-3467.log`** Log for the Patch Manager Server.
- **`httpd-3467.yy.mm.dd.log`** Web server access log for Patch Manager Server. This log shows who is accessing the server, either through the web services or through the console interface, and how many accesses were made.

These logs are located in the `\logs` folder of the Patch Manager Server installation directory.

Database Synchronization

The patch information that has been sent to the HPCA Configuration Server DB must be synchronized with the Patch SQL database for assessment and analysis. The HPCA Configuration Server DB and the Patch SQL database house identical information for the set of classes and instances that are synchronized.

- Each class in the PATCHMGR Domain becomes a table in the Patch SQL database. The corresponding table is named nvd_classname.
- Each attribute in each class becomes a column in its table. The corresponding column name is nvd_attributename. Expressions and connection variables are not replicated.
- Each instance in the class becomes a record in the corresponding table.

This synchronization occurs automatically after a patch acquisition and in normal HPCA operations.

However, there may be times when you need to run the synchronization manually. For example, synchronize the databases manually after an import of patch information from a different HPCA server. Also, synchronize the databases manually if you switch the SQL database configured for Patch Management after some acquisitions have taken place.

You can synchronize the databases manually using the Patch Manager Administrator or a command line.

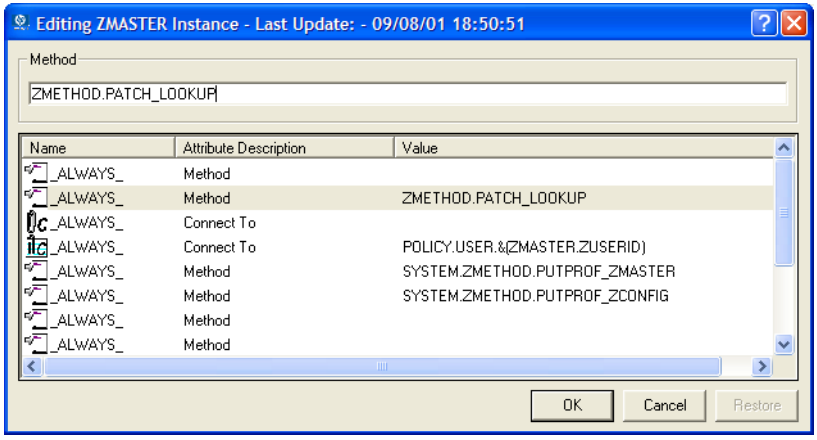
To synchronize the databases using the Patch Manager Administrator

1. From your web browser, go to **http://<*patchserveripaddress*>:<*port*>/patch/manage/admin.tsp**.
2. From Operations, click **Perform a Synchronization**.
3. Click **Submit**.

Adding a Method Connection

Use the Admin CSDB Editor to add an _ALWAYS_ Method connection to the PRIMARY.SYSTEM.PROCESS.ZMASTER instance as shown in the following figure.

Figure 2 Edit the ZMASTER instance



This method entry for ZMETHOD.PATCH_LOOKUP must precede the resolution of any services for a user.

Messaging Server

Install the Messaging Server; the latest version is recommended and version 5.10 must be installed at a minimum. For Patch Manager reports, you must enable the Messaging Server with the Patch Manager Data Delivery Agent. Review the *HPCA Messaging Server Installation and Configuration Guide* for more information.

Reporting Server

The latest version of the Reporting Server is recommended, a minimum version of 5.10 is required. Review the Reporting Server section of the accompanying HP Client Automation Release Notes prior to installation. The *HPCA Reporting Server Guide* also includes instructions on how to use the Reporting Server.

3 Patch Acquisition

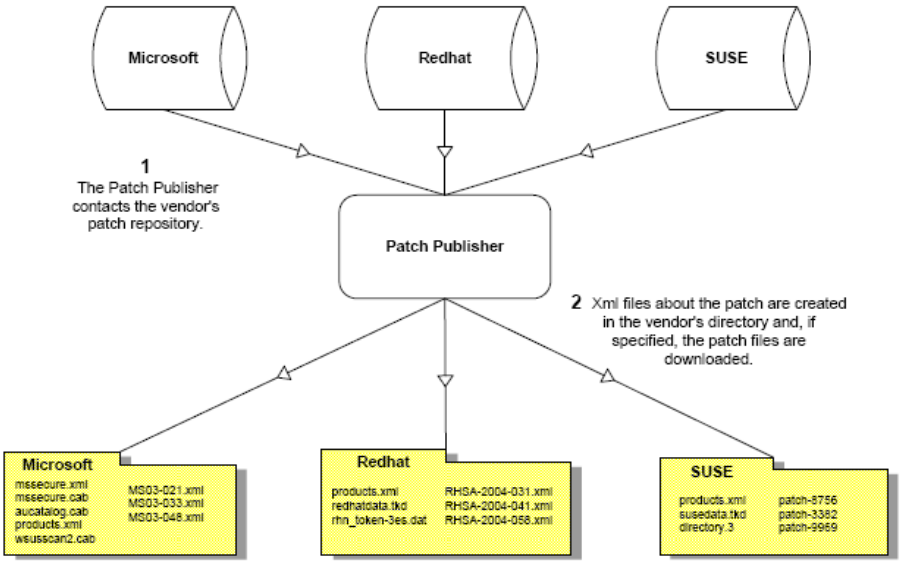
At the end of the chapter, you will:

- Be able to acquire patches.
- Know the parameters and Patch Manager Administrator operations available for patch acquisition and database synchronization.
- Know how to access and use the Patch Acquisition Reports:
  - Acquisition Summary
  - Acquisition by Bulletin
  - Acquisition by Patch

Patch Acquisition

Patch Manager provides a tool that connects to the selected vendor's web site, downloads the information regarding security patches including the files, and publishes this information to the Configuration Server DB. The acquisition process fetches security patches from the vendor *and* publishes this information to the Configuration Server DB.

Figure 3 Vendor's patch repository is contacted



Acquisition Overview

Patch Manager is used to acquire security patches and to synchronize the patch information in the CSDB on the Configuration Server with the Patch database on the SQL or Oracle Server. If you have already performed an acquisition, only instances that are different are updated.

During the acquisition, the following things occur:

- The vendor's web site is contacted to prepare for the acquisition.

- Either the information about the Bulletins, Security Advisories, and Service Packs and the actual patch files or only the information about the patches is downloaded. The information downloaded contains, but is not limited to, detailed data about each security patch, such as supersedence, reboot requirements, and probe information.
- An xml file is created for each bulletin acquired and is put in the vendor's folder in the Patch Manager's directory. These files are called patch descriptor files.
- The Configuration Server Database's PATCHMGR Domain is populated with this information.
- Services are created in the PATCHMGR Domain for each of the bulletins acquired.
- The PATCHMGR Domain is synchronized with the ODBC database you created.

About Patch Descriptor (XML) Files

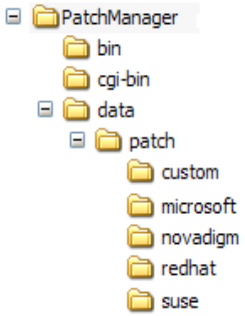
When security patches are acquired an xml, or patch descriptor file, with information about the patch is created and placed in the vendor's directory. The vendor directories are located by default in: *System Drive:*\Program Files\Hewlett-Packard\CM\PatchManager\Data\Patch.

For example, patch descriptor files for Microsoft bulletins would be in: *System Drive:*\Program Files\Hewlett-Packard\CM\PatchManager\Data\Patch\Microsoft

while those for Red Hat are located in:
*System Drive:**Program* Files\Hewlett-Packard\CM\PatchManager\Data\Patch\Redhat.

The bulletin number is the file name with an .xml extension. If the bulletin is identified by MS03-051, then the patch descriptor will be named MS03-051.xml. If you also acquired the actual files associated with the bulletin, a folder is created with the name of the bulletin that contains the patch files.

Figure 4 Acquired Patch Descriptor file directory structure

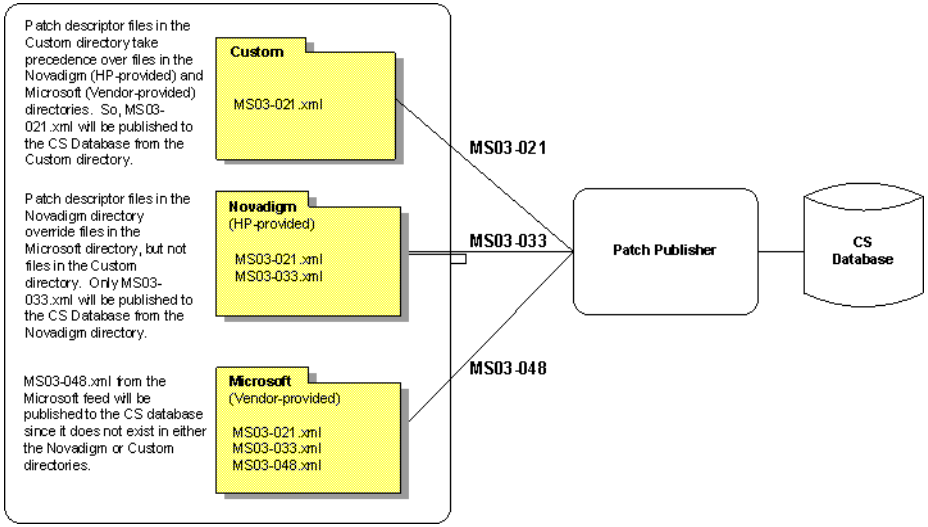


Some of the information acquired from the vendor may need to be altered before the patch can be managed. Therefore, there are two other subdirectories in the `\data\patch` subfolders: `novadigm` and `custom`. HP provides you with some additional patch descriptor files that are located in the `novadigm` subdirectory. Patch descriptor files located in the `novadigm` subdirectory override patch descriptor files in the relevant vendor's directory. You can also create or modify your own patch descriptors and place them in the `custom` subdirectory. These custom files will override files in the `novadigm, microsoft, redhat` and `suse` directories. Use a text editor to make the changes, name the file *exactly* as it is named in the vendor's directory, and place these xml files in the Custom subdirectory. The figure below illustrates an example of this hierarchy using Microsoft bulletins.

HP provides two *sample* descriptor files for Windows Operating System service packs, `MSSP-WIN2k_4.xml` and `MSSP-WINXP_1.xml`. To deploy other Microsoft Operating System service packs, you must create your own patch descriptor files and save them in the Custom subdirectory. You are responsible for deploying the service pack in a test environment before automating the deployment.

The figure below illustrates the patch descriptor override for Microsoft security bulletins. Note that the same hierarchy applies to all vendors: Microsoft, SuSE and RedHat.

Figure 5 Patch descriptor files



About Microsoft Patch Acquisition and Management

Embedded Support for the new Microsoft Update Catalog (wsusscn2.cab)

Microsoft has historically hosted its patches in a patch repository commonly referred to as MSSECURE. Microsoft recently introduced a new Microsoft Update Catalog, (`wsusscn2.cab`) as a centralized repository for all of their currently supported patches. As of this writing:

- Microsoft has stated patches for new Microsoft Products will only be available through the new Microsoft Update repository.
- Microsoft Website articles state that Microsoft intends to discontinue further updates to MSSECURE after October 9, 2007.

While Microsoft has continued to publish MSSECURE updates past this October 9, 2007 date, on the actual date of Microsoft's termination of support for MSSECURE, only patches hosted by Microsoft Update Catalog will be updated and maintained.

Presently, Patch Manager supports both sources of patches: MSSECURE and the new Microsoft Update Catalog, as well as an existing Legacy Catalog.

Patches acquired and deployed using Microsoft Update Catalog technologies require no HP metadata correction. For the products that can be managed, patches associated with these products can be tested and, then, deployed *immediately* after being published to the Configuration Server. As Microsoft expands their list of products supported in Microsoft Update Catalog, Patch Manager will be extended to enable patch management support for these products.

Microsoft Update Catalog Requirements: Minimum OS and Service Pack Levels

Refer to Microsoft's website for specific information concerning the minimum Operating System and Service Pack requirements for Microsoft Update Catalog and Windows Update technologies leveraged by Patch Manager. As of this writing, the supported OS Versions and languages can be viewed from the Microsoft Update Home page at this link: **http://update.microsoft.com/microsoftupdate/v6/default.aspx**

Click **Get help and support** and access the Frequently Asked Questions.

Customers can continue to patch older operating systems without enforcing the minimum service pack levels required by Microsoft Update Catalog. However, upgrading devices to minimum service pack levels at this time lessens the impact when Microsoft does terminate support for MSSECURE technologies.

Patch Manager Vendor Settings for Microsoft Data Feeds

To support the currently available Microsoft update repositories and methods, the Patch Manager Administrator offers the following Microsoft Data Feed Prioritization options on the Vendor Settings Page:

- **MSSecure, Microsoft Update Catalog, Client Automation**
- **Microsoft Update Catalog Only**
- **Microsoft Update Catalog, Legacy Catalog**

See Microsoft Data Feed Prioritization on page 46 for detailed information.

Microsoft Office and Microsoft Update Catalog

Office patches deployed via the Microsoft Update Catalog will not detect if Office Applications are currently being managed by an HP Client Automation management application (e.g., Application Manager or Application Self-service Manager), or an Administrative Control Point. In either case, if a bulletin affecting an Office application is entitled to a device, Patch Manager

will manage the Office patch and install it locally onto those devices that are vulnerable. For more information on patching devices with Microsoft Office, see Detecting and Managing Microsoft Office Security Bulletins on page 95.

Windows Installer 3.1 Requirement

When running Patch Manager, Windows Installer Version 3.1 *or above is* required on all target devices. To meet this MSI 3.1 requirement, HP recommends that customers either:

- Deploy the latest MSI 3.1 package manually by downloading it from the Microsoft website. This bulletin is defined for multiple languages. As of this writing, the US-English version is at **http://support.microsoft.com/kb/893803/en-us**,

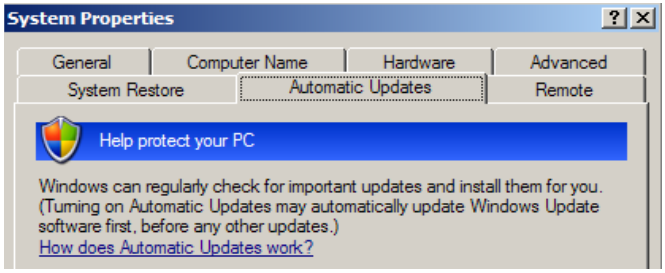
  or

- Use Patch Manager to acquire, distribute and manage the bulletin MS-KB893803. Specify this bulletin as part of your acquisition list and entitle it to your Windows agent machines.

About Microsoft Automatic Updates

Automatic Updates is a feature of Microsoft Windows that enables users to initiate a scan of their system for needed patches. Microsoft Automatic Updates also allows for the download and installation of the patches. This Microsoft feature is accessed from **My Computer** → **Properties** → **System Properties Automatic Updates** tab. as shown in the following figure.

Figure 6 System Properties -- Automatic Updates tab



Automatic Updates currently supports the following configuration options other than Automatic:

1 Download updates for me, but let me choose when to install them

2 Notify me but don't automatically download or install them

3 Turn off Automatic Updates

Both Microsoft Automatic Updates and Patch Manager use an underlying Windows component, Windows Update Agent (WUA), to scan a device and install updates.

To avoid a situation where WUA may be in use by another patch management product, you are strongly advised to **Turn off Automatic Updates**. HP makes this recommendation to prevent collisions in patch management products until such a time that Microsoft supplies a software update to Windows Update Agent.

The potential consequences of using Automatic Update options with Patch Manager are discussed below.

- If you **Turn off Automatic Updates,** as HP recommends, it is possible that you will not be informed of all updates available because Patch Manager does not support that product, but Automatic Updates does.
- If you set Automatic Updates to **Notify me but don't automatically download or install them**, it is imperative that users do not initiate the Automatic Updates download process while the Patch Manager Agent is scanning or installing updates. If the Automatic Updates process is initiated manually, it could result in *either* process failing to download and install updates on the managed device. This behavior is not specific to Patch Manager. It is also exhibited when other patch management products attempt to use WUA, and WUA is already in use.

Please consult the following Microsoft KB Articles for more information:

- Microsoft KB Article 910748; at the time of this writing, the url is **http://support.microsoft.com/kb/910748.**
- Microsoft KB Article 931127; at the time of this writing, the url is **http://support.microsoft.com/kb/931127.**

If you have virus scanners installed and enabled in your enterprise, please refer to Microsoft KB Article 922358. This documents a need to exclude the folder `%Windir%\SoftwareDistribution` from virus scans. While this Microsoft document references specific Microsoft patch management technologies, the same Windows Update Agent limitation can occur in an enterprise using Patch Manager, since it leverages Windows Update Agent technologies. Please review this Microsoft KB Article:

- Microsoft KB Article 922358; at the time of this writing, the url is: **http://support.microsoft.com/kb/922358**.

WUA uses the Microsoft Windows Service called **Automatic Updates Service;** this windows service must be set to either Automatic or Manual on target devices. The Automatic Updates Service can be in a stopped state since WUA will start it as needed.

Refer to the following Microsoft articles for more information about the configuration of Automatic Updates.

- *How to configure and use Automatic Updates in Windows XP*. At the time of this writing, the url is **http://support.microsoft.com/kb/306525.**
- *How to configure and use Automatic Updates in Windows 2000*. At the time of this writing, the url is **http://support.microsoft.com/kb/327850/**

About Red Hat Patch Acquisition

To acquire security patches for Red Hat:

- Establish a Red Hat Network account using the Red Hat web site. At the time of this writing, the location is **http://redhat.com**.
- You will need a Red Hat Network account with one system entitlement for each of the Red Hat Server OS Filter options (version + release + hardware architecture combination) for which you want to acquire and manage patches. These should correspond to the OS Filter options you selected in the Patch Manager Configuration.

  For example, to perform patch acquisitions for Red Hat Enterprise Server (ES) Version 4 on x86 systems only, you will need a Red Hat Network account with one Red Hat Network system entitlement. To perform patch acquisitions for Red Hat ES Version 4 on x86-64 systems, you will need an additional Red Hat Network system entitlement.

  To perform acquisitions for Red Hat Version 5 Servers, on both x86 and on x86-64 systems, you will need an additional two Red Hat Network system entitlements.

Prerequisite, or dependent, Red Hat packages required to install Red Hat Security Advisories can be acquired from two places. They can either be downloaded from the Red Hat Network during acquisition or they can be

found locally if copied from the Red Hat Linux installation media. During an acquisition, Patch Manager will first look for the `.rpm` packages in the appropriate directory. For example:

- For Red Hat Enterprise Linux 4ES on x86, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/4es`.
- For Red Hat Enterprise Linux 4ES on x86-64, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/4es-x86_64`.
- When naming the `data/patch/redhat/packages/` subdirectories, refer to the list of **OS Filter Architecture** values with on Red Hat Feed Settings on page 25. Use the applicable folder name based on the value following `REDHAT::` as the subdirectory name.

If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, HP recommends copying the dependency packages to the appropriate packages directory from your Linux installation media. The Red Hat RPM packages can be found on the installation media under the `RedHat/RPMS` directory.

- Use the rhn_register tool to create a Red Hat Network (RHN) `systemid` file. This file will be used to pass RHN credentials during acquisition. See the procedure below for details.

To create a Red Hat systemid file

1. Perform a root login to a Linux Server running the Red Hat OS for which you would like to automatically acquire security patches.
2. Execute the command rhn_register on the command line when logged into the system as root.
3. When prompted by the rhn_register tool to use an existing or new account, select existing and supply the Red Hat Network username and password you created on the Red Hat web site.
4. Enter a unique profile name for this computer such as the IP address or hostname, and exit the rhn_register tool without applying any patches to the system where you ran rhn_register. A file called `systemid` is created.
5. Copy the file `/etc/sysconfig/rhn/systemid` produced by the rhn_register tool to the `\PatchManager\etc` directory on your Patch Manager Server.

6 Rename the file from `systemid` to one of the following `redhat-*.sid` filename conventions. They vary according to the hardware architecture:

— For x86 systems, rename `systemid` to `redhat-`*`version+release`*`.sid`, where *`version+release`* represents one of the three combinations of Red Hat Version 4 followed directly by the Release (`as`, `es`, or `ws`), or, for Red Hat Version 5, *`version+release`* is either `5server` or `5client`.

For example, if the computer was running Red Hat Enterprise Server V 4, then rename the `systemid` file to `redhat-4es.sid`.

— For x86_64 systems, rename `systemid` to `redhat-`*`version+release`*`-x86_64.sid`. This is the same naming convention as above, except it adds the architecture type of **–x86_64** to the filename, prior to the `.sid` extension.

For example, if an x86_64 computer was running Red Hat Enterprise Server V 4, then rename the systemid file to `redhat-4es-x86_64.sid`.

Access to the Red Hat network might be disabled if the network determines that patches have been acquired too frequently. An error will show in the `patch-acquire.log` including the text `Abuse of Service detected for server linux`. To resolve this issue, delete the registered system from the Red Hat network web interface at **https://rhn.redhat.com**. Recreate the Red Hat credentials file (`systemid`) using the procedure above.

Now, you can run Red Hat Enterprise Server patch acquisition. Be sure that the proper Configuration Server and ODBC parameters are configured.

SuSE Patch Acquisition Requirements

SuSE feed settings require a secure (SSL) connection and a Vendor-supplied User ID and password, as discussed in this topics.

SuSE 10 and SuSE 11 devices have additional requirements; see SuSE 10 and SuSE 11 Registration Requirements on page 73.

SSL: The Novell website requires a secure (SSL) connection for patch acquisition. The need for a secure connection within Patch Manager is only required on the server that is used to perform secure patch downloads from the Novell website. At the time of this writing, the Novell website does not require or perform certificate validation.

SuSE Linux Vendor User ID and password: The requirements for obtaining a Vendor User ID and password vary by SuSE Version number.

- **SuSE 9:** For SuSE 9 security patch acquisition, you must establish a User ID and password through your SuSE Linux vendor to access SuSE Internet resources. Specify these credentials using the Patch Manager Administrator console. Go to the **Configuration > Acquisition Settings > Vendor Settings** page.
- **SuSE 10 and SuSE 11:** For SuSE 10 and SuSE 11 security patch acquisition of SLES10, SLED10, SLES11 or SLED11 patches, you must establish mirror credentials through your SuSE 10 or SuSE 11Linux vendor to access SuSE 10 or SuSE 11Channels.Specify these credentials using the Patch Manager Administrator console. Go to the **Configuration > Acquisition Settings > Vendor Settings** page.

To obtain SuSE 10 or SuSE 11 mirror credentials:

1. Establish the username and password for login to the Novell Customer Center (NCC) through your SuSE Linux vendor when the SuSE 10 or SuSE 11 product is bought.
2. Login to the NCC using using the login account information given by the vendor when the SuSE 10 or SuSE 11 product was bought.
3. Click on **Mirror Credentials** under the **Myproduct** link in the left panel.

   In the Credentials area of the Mirror Credentials page, you will see the Username and Password. In the Channels area, you will see the SuSE 10 or SuSE 11 Channel details.
4. Use the Username and Password obtained from the above steps when completing the User ID and password credentials for SuSE 10 or SuSE 11 Patch Acquisition. See the Vendor Settings topic for configuring SuSE 10 and 11 Feed Settings on page 53.

SuSE 10 and SuSE 11 Registration Requirements

Starting with SuSE 10 and onwards, Novell's explicit policy states that in order to receive security patches and updates, each SuSE agent Operating System must be registered with Novell and have their licenses managed and validated either directly through the Novell Customer Center (NCC) or Subscription Management Tool.

HPCA Patch Management does not validate that Novell's license or registration policy is met for SuSE 10 or above systems. It is the customer's responsibility to adhere to Novell's policy and have their SuSE10 and SuSE11 machines registered with validated licenses.

To register your SuSE 10 or SuSE 11 systems with the Novell Customer Center

Refer to the Novell website for details on registering your SuSE 10 and SuSE 11 systems with the Novell Customer Center.

As of this writing, the topic *Registering and Updating SUSE Linux Enterprise 10* is available at:

http://www.novell.com/support/dynamickc.do?cmd=show&forward=nonthreadedKC&docType=kc&externalId=3410833&sliceId=1

On Reboot Requirement for Linux Patches

Reboot is not required when applying application patches to Linux machines. However, a reboot is required when you apply any kernel-related Linux patches. As of now, HP PatchManager does not support the automatic rebooting of Linux machines when a kernel patch is installed. It is the user's responsibility to reboot manually whenever a kernel patch is installed.

Performing a Patch Acquisition

The Client Automation Patch Manager Administrator (Patch Manager Administrator) console provides a user friendly interface that allows you to create acquisition job profiles that can be saved and used repeatedly.

- Use the Configuration area Acquisition Jobs task to define the acquisition jobs.

- Use the Operations area Start Acquisition task to run the jobs.

Parameters specified in an acquisition job or on an acquisition command line override parameters set in the Patch Manager configuration file, `patch.cfg`. Be sure to use quotes around values containing spaces. See Configuring Patch Manager using the Patch Manager Administrator on page 32 for more information.

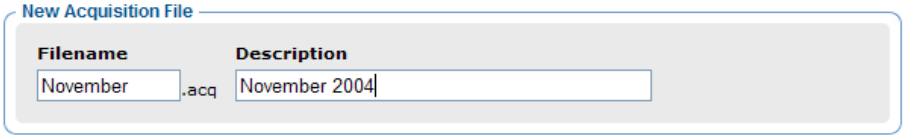
HP recommends acquiring from only one vendor at a time. In addition, some SuSE Security Advisories and Microsoft Office Security Bulletins may take an extended period of time to download. To account for this, consider adjusting the HTTP Timeout parameter as necessary.

The acquisition job settings that are required depend on your environment.

Configure Acquisition Jobs

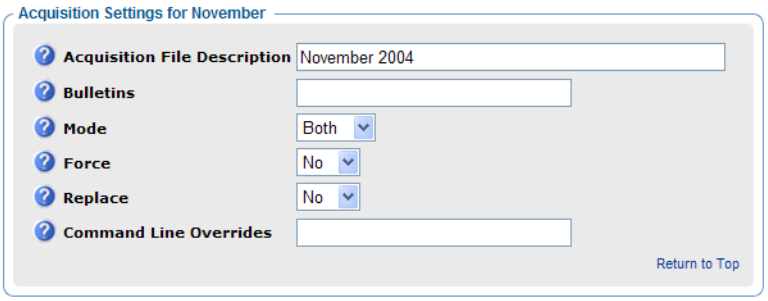
To create or edit an acquisition profile using the Patch Manager Administrator

1. From your web browser, go to **http://***patchserveripaddress***:***port* **/patch/manage/admin.tsp.**
2. From Configuration, click **Acquisition Jobs**.
3. Either select an existing file to edit, or click **New** to create a new file. Click the trashcan icon to delete an acquisition file. In this example, we click **New**.



4. If you are creating a new file, type a Filename and Description, then click **Next**.

5 You will be taken to Step 2, where you can complete Acquisition Settings for the new job.



- **Acquisition File Description**: Create a description for the acquisition file.
- **Bulletins**: Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. For Red Hat Security advisories, use a hyphen (-) in place of the colon (:) that appears in the Red Hat Security advisory number as issued by Red Hat.

  If you do not want to download any bulletins, type **NONE** in the Bulletins field.

  — Microsoft Security bulletins use the naming convention `MSYY-###`, where *YY* is the last two digits of the year that the bulletin was issued and *###* is a sequential number of the bulletin number being released for this the year specified. Microsoft service pack patch descriptor files supplied by HP are supplied with the following naming convention: `MSSP_operatingsystem_spnumber`. To acquire *sample* Microsoft Operating System service packs, specify MSSP*. This will download sample service packs acquired from the `novadigm` or `custom` folders. To acquire Microsoft Advisories, specify the KB articles using the naming convention `MS-KB*`, where * represents the number assigned to the Knowledge Base Article.

  — Red Hat Security advisories are issued using the naming convention `RHSA-CCYY:###`, where *CC* indicates the century and *YY* the last two digits of the year when the advisory was issued, and *###* the Red Hat patch number. However, because the colon is a reserved character in products, you must use a hyphen (-) in place of the colon (:) that

appears in the Red Hat-issued Security advisory number. Specify individual Red Hat Security advisories to Patch Manager using the modified naming convention of `RHSA-CCYY-###`.

— SuSE Security patches use version-specific naming conventions identified below.

Use a comma to separate multiple SuSE patch entries (regardless of version). Do not use a space to delimit multiple entries; it will not be accepted.

– For SuSE 9, use `SUSE-PATCH-####`, where the prefix `SUSE-` is followed by the SuSE 9 patch metadata filename. For example: `SUSE-PATCH-1234`

– For SuSE 10, use `SUSE-PATCH-platformrel-package-####`, where the prefix `SUSE-` is followed by the SuSE 10 patch metadata filename. For example: `SUSE-PATCH-SLESP1-MOZILLAFIREFOX-1234`

– For SuSE 11, use `UPDATEINFO-platformrel-package-####`, where the entry reflects the entire `UPDATEINFO*.xml` filename for the Suse 11 patch without the `.xml` extension. For example: `UPDATEINFO-SLESSP0-MOZILLAFIREFOX-1234..`

If the SuSE 11 filename contains a comma, you must replace it with a dash (-) when entering the bulletin name to be acquired. The comma is the reserved character to delimit multiple bulletins.

All SuSE 11 patch names are automatically reformatted into shorter, unique names when they are published to the PRIMARY.PATCHMGR domain of the CSDB.

- **Mode**: Specify BOTH to download the patches and the information about the patches. Specify MODEL to acquire only the metadata for patches. Only the Bulletins and Numbers for the patches are downloaded, but not the actual patch files. Use this mode so that you can use the reports to expose vulnerabilities on managed devices.
- **Force**: Use force in the following situations.
  — You previously ran an acquisition using the mode MODEL, and now you want to use BOTH.
  — You previously ran an acquisition filtering for one language (lang), and now, you need to acquire bulletins for another.

— You previously ran an acquisition specifying one product, and, now, you need to acquire for another.

For example, suppose that originally you had only Windows 2000 computers in your enterprise, so you used **`-product {Windows 2000*}`**. A month later, you roll out Windows XP. If you want to acquire the same bulletins, you will need to run the acquisition with **`-product {Windows XP*,Windows 2000*}`** and **`-force y`**.

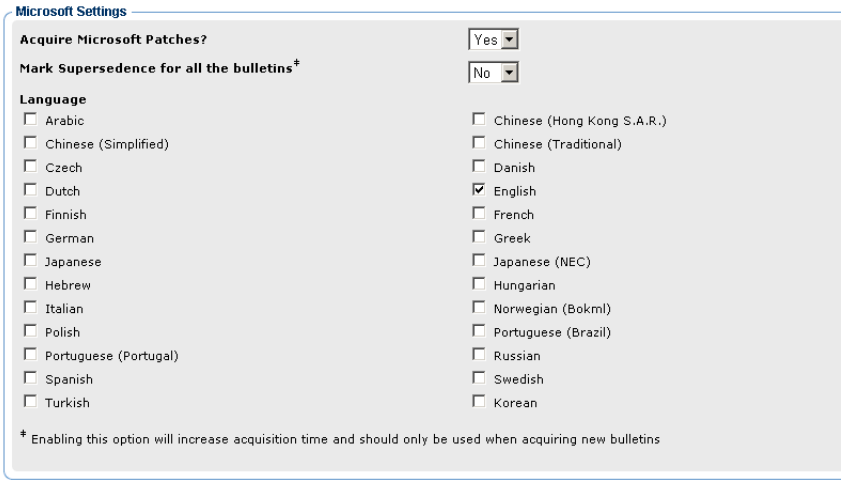
If replace is set to **`Y`**, the bulletins will be removed and reacquired, regardless of the value of force.

- **Replace**: Set replace to **`Y`** to delete old bulletins, specified in the bulletins parameter, and then re-acquire them. This will supersede the value for force. In other words, if you set replace to **`Y`**, then any bulletin specified for that acquisition will be deleted and reacquired, whether force is set to N or Y.
- **Command Line Overrides**: Use this parameter only when it is necessary to override your regular acquisition parameters. If used incorrectly, the acquisition will fail. Use the format of *`-parameter value`*. See Appendix D, Patch.cfg Parameters for a full list of parameters.

Microsoft Settings

- **Acquire Microsoft Patches?**: Select **Yes** if you want to acquire Microsoft Patches. For additional settings, go to the Vendor Settings page in the Patch Manager Administrator.

  If you select **Yes**, the **Mark Supersedence for all the bulletins** option appears as well as the **Language** option.



Select **Yes** for the **Mark Supersedence for all the bulletins** option, if you want to run acquisition for a particular bulletin and also want all of the existing bulletins in the Configuration Server Database to be updated. If you do not want to update the bulletins in the Configuration Server Database, select **No**. Selecting **Yes** for this option allows you to update the bulletins in the Configuration Server Database without running acquisition for all of the bulletins each time.

If you select **Yes** for the supersedence option and run an acquisition for any new bulletin using the Microsoft Update Catalog (MUC) or Optimized Patch Utility Service (OPUS) data feed, all existing MUC bulletins will be updated in the Configuration Server Database and the `bulletins.xml` file. At the same time, all existing OPUS bulletins will be updated in the `patch_data` file. As a result, the Configuration Server Database, the `bulletins.xml` file, and the `patch_data` file are all modified irrespective of the data feed selected for the new bulletin.

Bulletins can be marked for supersedence for the MUC and OPUS data feeds. They cannot be marked for supersedence for the MSSECURE data feed.

RedHat Settings

- **Acquire RedHat Patches?**: Select **Yes** if you want to acquire RedHat Patches. For additional settings, go to the Vendor Settings page in the Patch Manager Administrator.

SuSE Settings

- **Acquire SUSE Patches?**: Select **Yes** if you want to acquire SuSE Patches. For additional settings, go to the Vendor Settings page in the Patch Manager Administrator.

6 Click **Next** to go to Step 7 where you will select products to exclude from an acquisition session.

If you exclude one or more products or operating systems from one acquisition to the next, all patches specific to the products or operating systems that you excluded from acquisition will be removed from the Configuration Server Database. As a result, the removed products or operating systems are no longer eligible for vulnerability assessment and management. This applies to all vendors.

7 Expand the appropriate vendor's products and check the products you want to exclude from the acquisition. Uncheck the products you want to include.

8 Click **Finish** to save the acquisition file you created.

Now, you can use the Patch Manager Administrator to run an acquisition using your saved settings. From the **Operations** area, click **Start Acquisition** and select this job.

Start Acquisition

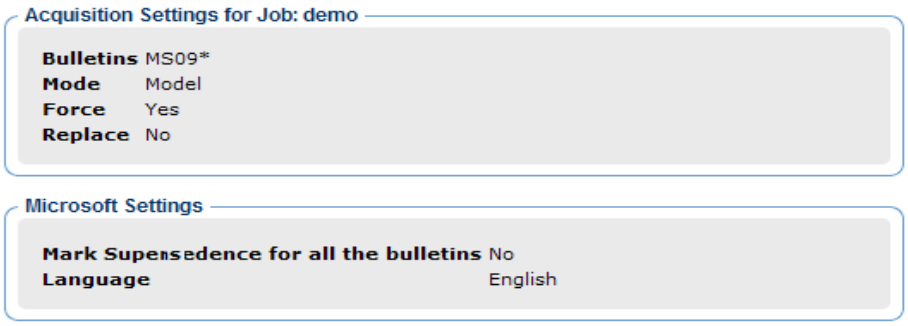
To run an acquisition job from the Patch Manager Administrator

1 From your web browser, go to **http://***patchserveripaddress***:***port* **/patch/manage/admin.tsp**.

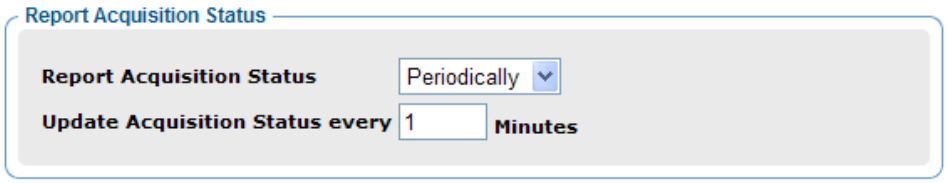
2 From Operations, click **Start Acquisition**.

3 Select a file by clicking on its name.

4 Confirm the settings for this acquisition.



Report Acquisition Status



- **Report Acquisition Status**: In addition to the acquisition log, you can specify how frequently you want to update the current acquisition status that is displayed when you View Acquisition Jobs, as discussed on
- **Update Status Information every**: If you specified **Periodically** in the Report Acquisition Status field, select how frequently you want to update the status file.

5 Read the notice on your agent update settings, and click **Submit** to begin your acquisition.

To check the status of the acquisitions:

- Use the HP Reporting Server to look at the Patch Acquisition Reports.
- Go to the Patch Manager Administrator's **Status and Logs** area to **View Acquisition Jobs**.

- Also use the **Status and Logs** area to access the **View Logs** page and select the `patch-acquire.log`. This patch acquisition log file is created in the Patch Manager's log directory and also includes the version and build number of `patch.tkd`.

View Acquisition History

From the **Status and Logs** area of the Patch Manager Administrator, click **View Acquisition History** to view the status and details of previous acquisitions.

Select an acquisition job from those listed to view the status and details.

Creating Custom Patch Descriptor Files

The patch descriptor files that are created using the **acquire** command use the information from the vendor data feeds. These files may be missing information or contain incorrect information regarding the patch. A **probe** defines what is needed to be in compliance with the security issue that the patch fixes. You can create a custom patch descriptor files using supported XML tags. The custom descriptor file must be placed in the custom directory and be named identically to the file it will be overriding in the `microsoft`, `redhat`, `suse`, or `novadigm` directories. Below is an example of creating a custom descriptor file for a Microsoft bulletin.

To create a custom descriptor file

1. Copy the Microsoft version of the XML file located in `C:\Program Files\Hewlett-Packard\CM\PatchManager\data\patch\microsoft` directory generated during an acquisition into the `C:\Program Files\Hewlett-Packard\CM\PatchManager\data\patch\custom` directory.
2. Use a text or xml editor to view the patch descriptor file. Validate the data with the releases itemized in the URL located at the top of the xml. Change `Source` to `Custom`.

```
<Bulletin PopularitySeverityID="0" URL="http://www.microsoft
.com/technet/security/bulletin" FAQURL="http://www
.microsoft.com/technet/security/bulletin"
MitigationSeverityID
="0" Supported="Yes" ImpactSeverityID="0" SchemaVersion="1.0"
```

```
PreReqSeverityID="0" DateRevised="20021119"
Source="NOVADIGM" Name="MS02-065" Title="Buffer Overrun in
Microsoft Data Access Components Could Lead to Code Execution
(Q329414)" DatePosted="20021119" >
```

When generating a custom xml, HP recommends including all Product releases. This allows a managed device running any available releases of the product to be discovered.

3 Make any changes required to adjust the data, and save the custom patch descriptor file. Change the `Source` tag to `Custom`. This value is reflected in the BULLETIN instance's SOURCE attribute.

Use the Patch Manager Administrator to publish the custom patch descriptor file. Be sure to set the Replace option to Yes if you wish to entirely replace the bulletin previously published to the Configuration Server.

4 You may view the `patch-acquire.log` to see where the publishing process obtained the xml from:

```
20040116 15:11:24 Info: Publishing MS02-065 1 of 1

20040116 15:11:24 Info: Using bulletin from custom C:/Program
Files/Hewlett-Packard/CM/PatchManager/data/patch/custom
/MS02-065.xml

20040116 15:11:24 Info: Loading XML file C:/Program Files/
Hewlett-Packard/CM/PatchManager/data/patch/custom
/MS02-065.xml

20040116 15:11:24 Info: Loading bulletin MS02-065 from RCS
```

Change Management using RADDBUTIL

To move security patches from a Quality Assurance environment to Production the Configuration Server Database utility called RadDBUtil; must be used.

For general information on using RadDBUtil, refer to:

- *HPCA Configuration Server Database Utility (RadDBUtil)* chapter in the *HPCA Configuration Server User Guide*.

For specific information on using RadDBUtil with Patch Manager, also refer to this Technical Document on the HP Software Support Site:

- *Managing the Patch Bulletin Data Export and Import Process* (Document ID: KM112025)

Setting the Manage Installed Bulletins (mib) Option

Patch Manager supports the Manage Installed Bulletins (-mib) option. By default, when Patch Manager runs a discovery on target devices, it starts managing all applicable bulletins it finds installed on the target device. This means upon successive connects, Patch Manager ensures previously installed bulletins are still installed.

The –mib option is available for customers who want Patch Manager to skip the processing of applicable bulletins already installed on target machines, and only process the bulletins not already installed on the machines. The –mib option can take the following values:

`-mib none`
Manage Patch Manager-installed bulletins only, and do not check the service library or binary resources for alternatively installed bulletins. This is the default behavior since there is no impact on the client agent in terms of vulnerability or re-patching, and it offers greater performance.

`-mib hppm (or n)`
Manage HP Patch Manager-installed bulletins, only; do not manage bulletins installed by an external source.

`-mib all` (or y)
Manage all installed bulletins, whether installed by Patch Manager or an external source. This option is resource intensive.

When the Patch Manager is configured with the **`-mib`** option set to **`hppm`** or **`none`**, there is a substantially-reduced processing load on both the Configuration Server and the Patch Manager agents.

To set the Manage Installed Bulletins (mib) Option

Use the Agent Options page from the Patch Manager Administrator Console to set the Manage Installed Bulletins (-mib) option.

The Agent Options page is accessed from the Configuration area, Environment Settings group.

Patch Acquisition Reports

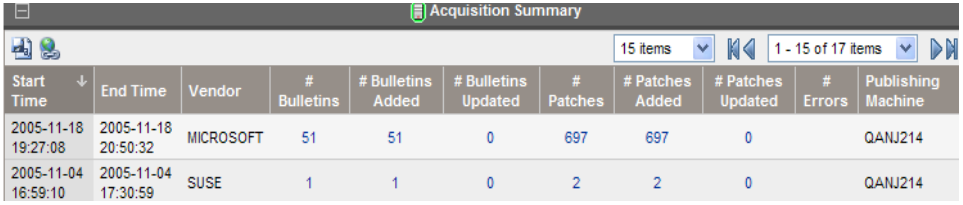
Acquisition based reports show the success and failures of the patch acquisition process from the vendor's web site.

To view the reports, access the Reporting Server; you can use the Reporting icon in the Patch Manager Administrator toolbar area. Under **Reporting Views**, click **Patch Management Reports** to expand the list of reports. Click **Acquisition Reports** to expand the list of available reports. For more information on using and filtering reports, refer to the *HPCA Reporting Server Guide*.

Acquisition Summary

The Acquisition Summary report shows the number of bulletins, patches, and errors for each acquisition session. In addition, it provides links to the acquisition reports for all bulletins and patches. The date and time of the publishing session is also listed.

Figure 6 View the Acquisition summary report



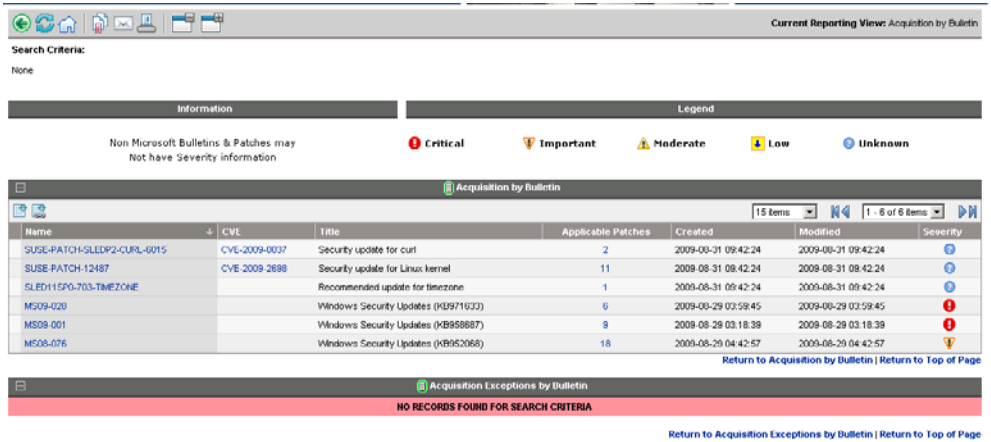
Start Time	End Time	Vendor	# Bulletins	# Bulletins Added	# Bulletins Updated	# Patches	# Patches Added	# Patches Updated	# Errors	Publishing Machine
2005-11-18 19:27:08	2005-11-18 20:50:32	MICROSOFT	51	51	0	697	697	0		QANJ214
2005-11-04 16:59:10	2005-11-04 17:30:59	SUSE	1	1	0	2	2	0		QANJ214

- Click **# Bulletins Added** or **# Bulletins Updated** to see the acquisition summary sorted by bulletin.
- Click **# Patches Added** or **# Patches Updated** to see the acquisition summary sorted by patch files.
- Click **# Errors** to see further explanations of why the acquisition failed. Numeric error codes displayed in the error reports are standard http status codes. For additional details on these codes, search for "HTTP Status Codes" on the World Wide Web.

Acquisition by Bulletin

Use the Acquisition by Bulletin report to see a summary of the bulletin's acquisition.

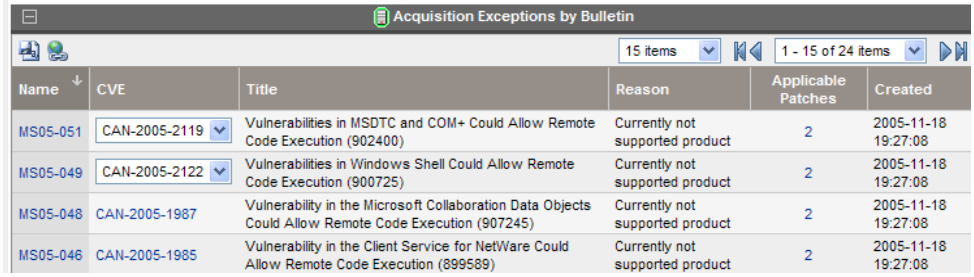
Figure 7 View the acquisition summary by bulletin



From this report click on the number for Applicable Patches to see the files associated with the bulletin. Remember that one bulletin may have multiple patches based on platform.

- If a bulletin has a patch that applies to a product that Patch Manager does not support, an asterisk (*) will be displayed preceding the bulletin name.
- The icon in the Severity column indicates the severity for Windows bulletins. They ratings range from Critical, to Important, to Moderate, to Low. If the bulletin is not for a Windows platform, the Unknown icon is displayed. Click on the icon in the Severity column to see all bulletins with the same severity. Pre-existing bulletins do not have severity ratings. To view severity ratings for existing bulletins and patches, you must re-acquire them using the Force and Replace options.
- At the bottom of this report, there is a second section that includes bulletins that apply to products that are not supported by Patch Manager. These bulletins will not appear in the Research reports.

Figure 8 View the acquisition exceptions by bulletin

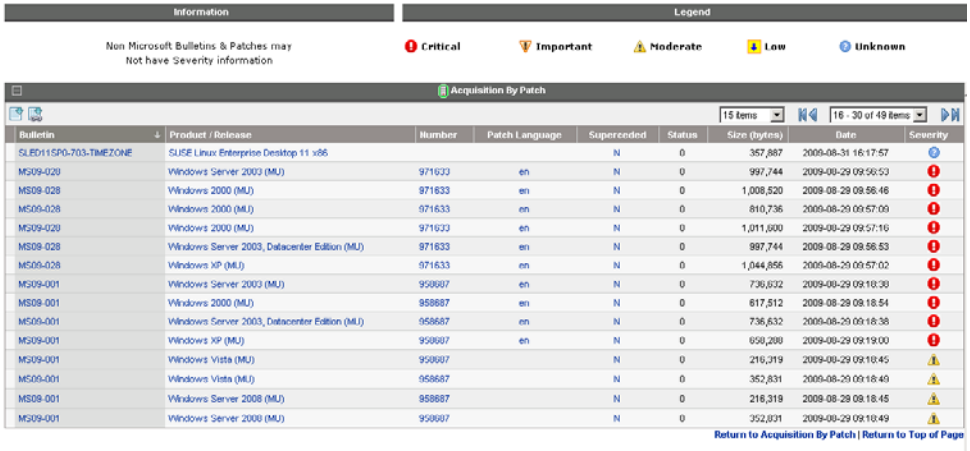


Name	CVE	Title	Reason	Applicable Patches	Created
MS05-051	CAN-2005-2119	Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (902400)	Currently not supported product	2	2005-11-18 19:27:08
MS05-049	CAN-2005-2122	Vulnerabilities in Windows Shell Could Allow Remote Code Execution (900725)	Currently not supported product	2	2005-11-18 19:27:08
MS05-048	CAN-2005-1987	Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution (907245)	Currently not supported product	2	2005-11-18 19:27:08
MS05-046	CAN-2005-1985	Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution (899589)	Currently not supported product	2	2005-11-18 19:27:08

Acquisition by Patch

Use the Acquisition by Patch report to see a summary of each patch's acquisition.

Figure 9 View the acquisition by patch



Bulletin	Product / Release	Number	Patch Language	Superceded	Status	Size (bytes)	Date	Severity
SLED11SP0-703-TIMEZONE	SUSE Linux Enterprise Desktop 11 x86			N	0	357,887	2009-08-31 16:17:57	
MS09-020	Windows Server 2003 (MU)	971633	en	N	0	997,744	2009-08-29 09:58:53	
MS09-028	Windows 2000 (MU)	971633	en	N	0	1,008,520	2009-08-29 09:58:46	
MS09-028	Windows 2000 (MU)	971633	en	N	0	810,736	2009-08-29 09:57:09	
MS09-020	Windows 2000 (MU)	971633	en	N	0	1,011,600	2009-08-29 09:57:16	
MS09-028	Windows Server 2003, Datacenter Edition (MU)	971633	en	N	0	997,744	2009-08-29 09:58:53	
MS09-028	Windows XP (MU)	971633	en	N	0	1,044,856	2009-08-29 09:57:02	
MS09-001	Windows Server 2003 (MU)	958687	en	N	0	736,632	2009-08-29 09:18:30	
MS09-001	Windows 2000 (MU)	958687	en	N	0	617,512	2009-08-29 09:18:54	
MS09-001	Windows Server 2003, Datacenter Edition (MU)	958687	en	N	0	736,632	2009-08-29 09:18:38	
MS09-001	Windows XP (MU)	958687	en	N	0	650,200	2009-08-29 09:19:00	
MS09-001	Windows Vista (MU)	958687		N	0	216,319	2009-08-29 09:18:45	
MS09-001	Windows Vista (MU)	958687		N	0	352,831	2009-08-29 09:18:49	
MS09-001	Windows Server 2008 (MU)	958687		N	0	216,319	2009-08-29 09:18:45	
MS09-001	Windows Server 2008 (MU)	958687		N	0	352,831	2009-08-29 09:18:49	

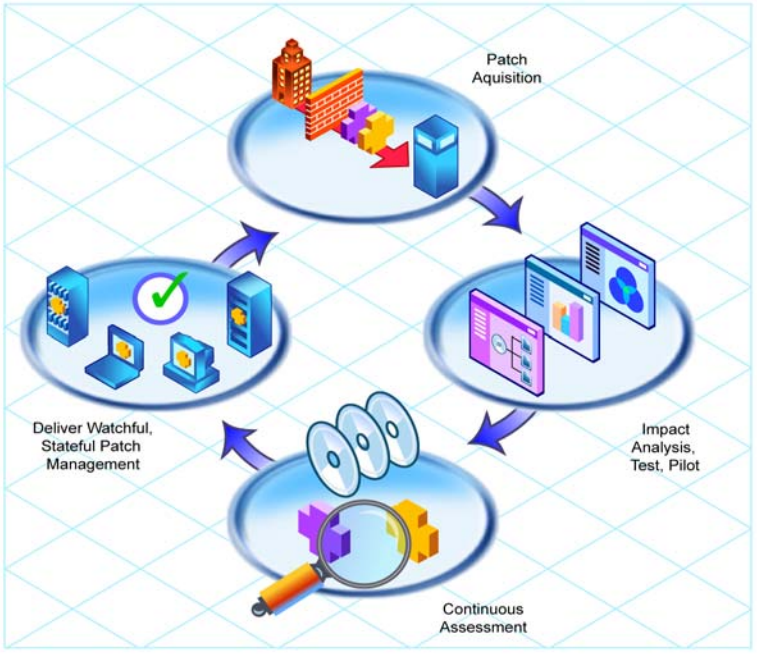
- Click on an item in the Product/Release column for a specific bulletin to drill down for full details on the patch.
- The icon in the Severity column indicates the severity for Windows patches. They ratings range from Critical, to Important, to Moderate, to Low. If the patch is not for a Windows platform, the Unknown icon is displayed. Click on the icon in the Severity column to see all patches with the same severity. Pre-existing patches do not have severity ratings. To view severity ratings for existing bulletins and patches, you must re-acquire them using the Force and Replace options.

4 Patch Assessment, Analysis and Reports

At the end of this chapter, you will:

- Know about Installing the Patch Manager Agent.
- Know how to manage patches on target devices.
- Be familiar with Patch Analysis and Reports. The reports generated for patch files using Reporting Server include: Executive Summaries, Compliance Reports, Acquisition Reports and Research Reports.

Figure 10 Product discovery and analysis



Installing the Patch Manager Agent

The Patch Manager agent must be installed on any target device that you want to manage vulnerabilities for. You can do this using the HPCA Enterprise Manager or using the installation from the Patch Manager media provided.

To accommodate Microsoft Update, your target devices must have the Windows Update Agent installed. This is part of the Patch Manager Agent Updates downloadable from the HP Patch Manager Update Site. The HP acquisition process automatically acquires the latest Windows Update Agent required for the Patch Manager Agent. The **DISCOVER_PATCH** Service will automatically apply the current Windows Update Agent to the managed device on the next agent connection.

For detailed installation instructions, refer to either the *HPCA Enterprise Manager User Guide* or the *HPCA Application Manager and Application Self-service Manager Guide*. For minimum system requirements, also refer to the *HPCA Application Manager and Application Self-service Manager Guide* for the appropriate operating system.

If you are using Patch Manager to manage Microsoft Windows devices you must have, at a minimum, Windows Installer version 3.1 pre-installed on the agent devices where Patch Manager is to run.

The recommended version of `nvdkit` for the Patch Manager devices is the build that is supplied with the HP Client Automation version 7.50 media.The absolute minimum `nvdkit` build required on a Patch Agent is **427**. If your target devices do not meet this requirement, visit the HP Support web site.

To install the Patch Manager Agent from the HPCA Enterprise Manager

The Patch Manager Agent is included automatically when you deploy the HPCA Agent from the Enterprise Manager Console to the device and device groups in your enterprise.

Deploying agents is performed from the **Management** tab of the Enterprise Manager Console using the **Agent Deployment Wizard**.

For details on using the Enterprise Manager and the Agent Deployment Wizard, refer to the *HPCA Enterprise Manager User Guide*.

To install from the HP Client Automation Media for Windows Agents

- Navigate to the appropriate subdirectory for your operating system on the Agents folder of the HP Client Automation media. Double-click **setup.exe**. When prompted, select the **Patch Manager** feature.

To use the install.ini file for Windows Agents

- In the [PROPERTIES} section of the `install.ini` file, add the line **`ADDLOCAL=NVDINSTALLPATCH`**.

After installing the agent, you will need to assign the appropriate services to the target devices.

To install the Patch Manager Agent on a Linux operating system

The minimum version of the Client Automation Agent that supports documented Patch Manager Agent version 7.50 functionality is Application Manager version 5.0; however, Application Manager version 7.50 is recommended. The absolute minimum build of `nvdkit` on the Linux agent is build 446.

The Patch Manager's maintenance file, `maint.tar`, contains the necessary agent files needed to enable the Patch Manager Agent. At the time of this writing, the Patch Manager Agent is supported on the following operating systems for Version 7.80.

- **Linux - RedHat**: Enterprise versions of Red Hat version 4.x on releases AS, ES, and WS, and version 5.x on server and client releases are supported for x86 (32-bit Intel) and x86-64 (Opteron/EMT64) architectures.
- **Linux - SuSE:** SuSE Linux Enterprise Server (SLES) versions 9, 10 and 11 are supported on x86 (32-bit) architecture as well as on x86-64 (AMD64 and Intel EM64T) architectures. SuSE Linux Enterprise Desktop (SLED) versions 10 and 11 are supported on x86 (32-bit) architecture as well as x86_64 (AMD64 and Intel EM64T architectures.

The Patch Manager Agent is not supported on HP-UX or Sun Solaris (SPARC) operating systems.

The Patch Manager agent maintenance file (`maint.tar`) is located with the Patch Manager media in the following operating system-specific directory.

— `Patch Agent Maintenance\linux\ram`

The supplied `maint.tar` files provided in the operating system-specific folders on the installation media are not interchangeable among device platforms.

To install the Patch Manager agent for RedHat and SuSE Linux from the HPCA Enterprise Manager

At a minimum, HP Client Automation Application Manager 5.00 is required to enable reboot management capabilities, and resume patch management processing after a reboot. To use this feature, the HPCA Scheduler Daemon (radsched) must be enabled as a system Service. Installation of the agent daemons as system services can be performed as a post installation task during the installation of the Application Manager agent. For additional information on UNIX agent post installation tasks, refer to the *HPCA Application Manager and Application Self-Service Manager Installation and Configuration Guide* (*HPCA Application Manager and Application Self-Service Manager Guide*).

For information concerning the installation of Client Automation agents from HPCA Enterprise Manager, refer to the *HPCA Enterprise Manager User Guide* and the *HPCA Application Manager and Application Self-service Manager Guide*.

To install from the HP Client Automation Media for RedHat and SuSE Linux

Navigate to the appropriate subdirectory for your operating system on the installation media. Start the installer using the UNIX **`./install`** command line and select the Patch Manager agent feature. Refer to the *HPCA Application Manager and Application Self-Service Manager Guide for UNIX* for more details.

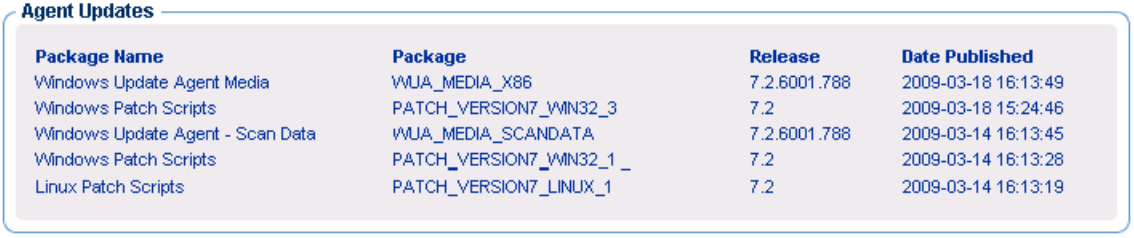
At a minimum, Application Manager 5.00 is required to enable reboot management capabilities, and resume patch management processing after a reboot. To use this feature, the HPCA Scheduler Daemon (radsched) must be enabled as a system Service. Installation of the agent daemons as system services can be performed as a post installation task during the installation of the Application Manager agent. For additional information on UNIX agent post installation tasks, see the *HPCA Application Manager and Application Self-Service Manager Guide for UNIX*.

Updating the Patch Manager Agent

When you run a patch acquisition, you can also download the latest Version and updates to the Patch Agent files. The Patch Agent files include the scripts to perform product discovery and management. These files are received from the Patch Update web site provided by HP. After download, the files are published to the PATCHMGR Domain and connected to the DISCOVER_PATCH Service instance.

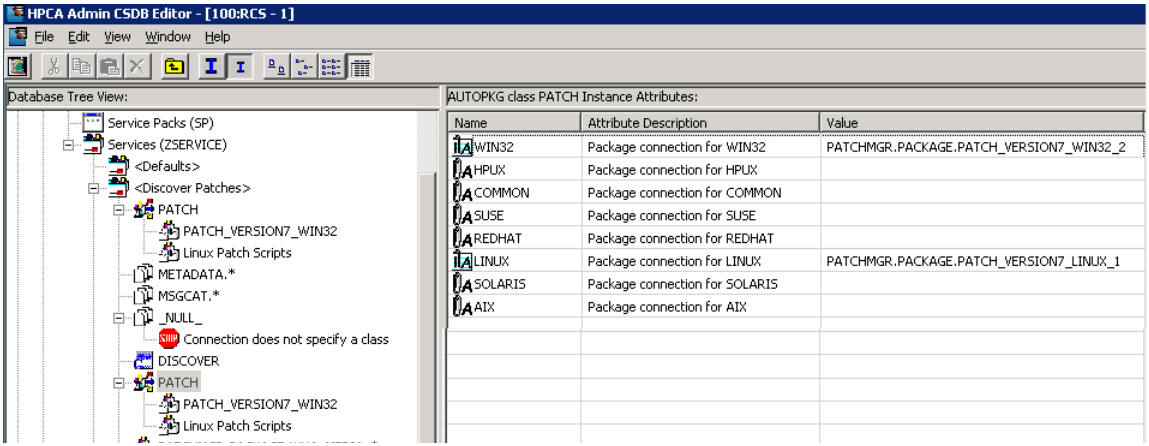
Use the View Agent Updates task in the Operations section on the Patch Administrator page to determine the status of updates. To do this, click **View Agent Updates.**

Figure 11 View agent updates



Agent files are distributed when the DISCOVER_PATCH Service is processed on the Patch Manager target device. This is accomplished through a connection in the DISCOVER_PATCH Service to the PATCH Instance in the AUTOPKG Class. In turn, the AUTOPKG.PATCH Instance connects to the agent maintenance packages created when you selected **Publish** or **Publish and Distribute**. If you have selected to publish only (not to distribute), you will need to create connections from the appropriate instance in the PACKAGE Class to the AUTOPKG.PATCH Instance. Use the Admin CSDB Editor to do this. An example is shown below.

Figure 12 Create connections to the published package



AIX, HP-UX and Solaris are not currently supported.

Agent Updates has the following values:

- **None**: The agent updates will not be published to the PATCHMGR Domain.
- **Publish, Distribute**: This is the default value. Publish the updates to the PATCHMGR Domain and connect them to the DISCOVER_PATCH Instance to distribute the updates to your Patch Manager-managed devices.
- **Publish**: The updates will be published to the PATCHMGR Domain, but will not be connected for distribution to Patch Manager-managed devices. You will need to create these connections.

There are two parameters that control which agent updates you download.

- **Operating System**: Specify which operating systems to acquire the agent updates for. The default is to download all operating systems.. Valid values are **Windows** and **Linux**.

- **Version**: Select the Patch Manager version for which you would like to acquire the agent updates. You can publish only one version to a Configuration Server; one Configuration Server cannot host multiple versions of the agent. If piloting, create a separate Configuration Server for the other version.

Never choose an agent version that is lower than the version of Patch Manager that is first installed or currently implemented in your enterprise.

To update to the current version, specify **Version 7**. This is the default for new Patch Manager 7.50 installations. This is also the default value if you migrated from an earlier release and removed the existing `patch.cfg` before performing the migration.

If you migrated from an earlier version and did not remove the existing `patch.cfg` before performing the migration, the version will default to the value contained in the old `patch.cfg` file. Migrating customers are advised to set the "**Publish and Distribute**" option and set the Agent Updates Version to **Version 7** using the Patch Manager Administrator. This will ensure the successful migration of Windows and Linux Patch Agents to Version 7.50. This is needed to continue management of Microsoft security patches when Microsoft discontinues updates to `MSSecure.xml`, in favor of the new Microsoft Update Catalog feed.

Note that when patches are acquired from Microsoft Update, the Source column in the report will show "Microsoft Update" instead of "Microsoft."

To accommodate Microsoft Update technologies, your target devices must have the Windows Update Agent installed. The Patch Manager acquisition process automatically acquires the latest Windows Update Agent required to perform vulnerability scans and patching when leveraging Microsoft Update Catalog technologies. The DISCOVER_PATCH Service will automatically apply the current Windows Update Agent to the managed device on the next agent connection.

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

Product Discovery and Analysis

Before you can manage vulnerabilities, the Patch Manager Agent must discover which products are on the device. Patch Manager objects are cached locally on the managed device to optimize bandwidth. Objects are downloaded only if they are different. In addition, the Patch Manager agent needs to detect which patches are installed for each discovered product. To do this, assign the Patch Manager services for DISCOVER_PATCH and FINALIZE_PATCH to the managed devices.

Running the Patch Manager agent connect requires that the **`dname`** parameter be set to **`PATCH`**. This will keep separate the resolution of services for the Patch Manager agent from the resolution of services for the Application Manager agent. If you are using Policy Server with Patch Manager, see Appendix C, Policy Server Integration.

To perform patch discovery

1. Connect your managed device (e.g. POLICY.USER.&(ZUSERID)) directly to the PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH service.

   This service is prioritized to run as the first service on Patch Manager agents. During a Patch Manager Agent connect, this service deploys methods to the patch manager agents, and performs product discovery and vulnerability assessment.

2. Connect your managed device (e.g. POLICY.USER.&(ZUSERID)) directly to the PRIMARY.PATCHMGR.ZSERVICE.FINALIZE_PATCH.

   During a Patch Manager Agent connect, applicable patches are downloaded and queued for management by a Patch Manager Service called FINALIZE_PATCH. This service is prioritized to run as the last service on Patch Manager agents. This service is required to report real time patch compliance information.

   Add the FINALIZE_PATCH service to the policy for all managed devices, in addition to any patch.

   Failure to use this service will result in extended patch management activities and failures to report real time patch compliance information.

3 Create a radskman command line to make a regular agent connect. At a minimum, the command line should resemble the following.

radskman ip=<*ConfigurationServerIPaddress***>,port=<***ConfigurationServerport***>,dname=patch,catexp=runmode:automatic**

For additional information on creating a radskman command line, refer to the *HPCA Application Manager and Application Self-service Manager Guide*.

Detecting and Managing Microsoft Office Security Bulletins

Patch Manager can manage the acquisition and deployment of Microsoft Office updates. However, because Microsoft Office applications use Windows Installer technology, patching and self-healing are inherently provided. Therefore, it is important to consider how you currently install and update Microsoft Office in your environment before you enable Patch Manager to deploy patches for Microsoft Office.

If you are currently distributing Microsoft Office using an external **ACP** (also known as an **Administrative Install Point**, **AIP**) or a Client Automation management application (Application Manager or Application Self-service Manager), it is recommended that you continue to use these solutions for updating Microsoft Office applications.

If you would like to begin using Patch Manager to update Microsoft Office applications, you must discontinue using an ACP or a Client Automation management application for distributing updates to your Microsoft Office

applications. You can continue to use an ACP or a Client Automation management application to deploy Microsoft Office applications; however, updates must be managed solely by Patch Manager.

After Patch Manager is used to distribute Microsoft Office application updates, ACP-managed and Client Automation-managed Microsoft Office applications will no longer be able to receive updates through those technologies. That is, ACP managed applications rely on a registered client-side synchronization mechanism by which updates are distributed from the ACP to the device, and Client Automation-managed applications use desired-state technology to distribute updates to Microsoft Office applications. Therefore, before enabling Patch Manager for the purpose of updating Microsoft Office applications, be sure that you no longer intend to use ACP or a Client Automation application to distribute Microsoft Office updates.

This topic outlines the choices, best practices, and implementation details related to managing Microsoft Office updates with Patch Manager. The topics include:

- Best Practices for Managing Microsoft Office Security Bulletins on page 96
- Best Practices with Microsoft Update Catalog Enabled on page 101
- Enabling Microsoft Office Updates in Patch Manager (Versions 3.0.2 and later) on page 102

Best Practices for Managing Microsoft Office Security Bulletins

The following information applies to both migrated and new installations. It identifies when and how to enable Patch Manager as your solution for patching Microsoft Office.

Windows Installer 3.1 Requirement

When running Patch Manager, Microsoft Windows Installer version 3.1 or later is required on all target devices. Windows Installer 3.1 is needed to detect updates for Microsoft Office applications.

Options for Updating Microsoft Office Products

The method initially used for deploying Microsoft Office products determines available options for patching the agent software. Microsoft Office products

use Windows Installer technology, which supports installation from compressed media typically found on a CD-ROM or an AIP. For details on Microsoft best practices, refer the Microsoft article, *Distributing Office 2003 Product Updates*.

If you deployed Microsoft Office to agents without using an HP Client Automation application, these Microsoft recommendations apply.

- If the Microsoft Office product was initially installed using compressed media from a CD-ROM or network file server, Microsoft recommends updating these agents by distributing the binary patch to the agent device, and allowing Windows Installer to perform local patching of the application.
- If the Microsoft Office product was installed from an AIP, Microsoft recommends that administrators obtain the appropriate administrative updates, and continue to update the centrally located AIP. This will keep agents reliably synchronized.

If you deployed Microsoft Office to agents using an HP Client Automation (HPCA) application, these HP recommendations apply.

- If the Microsoft Office product was deployed using Application Manager or Application Self-service Manager, determine if the application was published in accordance with the Basic or Advanced management guidelines. If the Basic approach was used, the media was in compressed (CD-ROM) format and there are no potential software conflicts in moving to the Patch Manager solution; HP recommends introducing Patch Manager into this model.
- If the Microsoft Office product was deployed using Application Manager or Application Self-service Manager using Advanced management guidelines, then the media was in AIP format; HP does not recommend introducing Patch Manager into this model. Administrators should continue to use the Admin Publisher to streamline the AIP update process, and distribute updates using Application Self-service Manager.

  Before ignoring this recommendation and enabling Patch Manager for Office products that were deployed using Advanced management guidelines (media in AIP format), read all of the ⚠ CAUTION and ■ WARNING statements throughout this topic to understand the potential software conflicts.

When to use Patch Manager to Deploy Microsoft Office Updates

Use Patch Manager to publish and deploy patches for Microsoft Office applications only when you no longer want to use another solution, such as Application Manager, Application Self-service Manager, or an external AIP. You must choose only one solution to publish and deploy patches.

Use Patch Manager to deploy Microsoft Office product updates only when you are certain that the Microsoft Office product was installed from:

- Compressed media (CD-ROM).
- An AIP, but you have decided to no longer use the AIP synchronization process for updating Microsoft Office products.
- Application Manager or Application Self-service Manager, but you have decided to no longer publish or deploy patches for Microsoft Office using Application Manager or Application Self-service Manager.

Administrators who manage agent devices running Microsoft Office products currently patched through the AIP synchronization process must be careful not to interchange these patching methods (AIP synchronization process and Patch Manager). Doing so may cause a break in the synchronization between the agent device and the AIP.

For details about the synchronization process, refer to the Microsoft article, *Updating Office XP Clients from a Patched Administrative Image*.

Client Automation Management Features that are Disabled when using Patch Manager

The management features of Application Manager and Application Self-service Manager that are derived from the method fields ZCREATE, ZVERIFY, and ZUPDATE will no longer be available for Microsoft Office applications once they are managed by Patch Manager; these include the ability to install on first use and the ability to manage MSI Features and Properties.

If you want to continue to use these features, do not introduce Patch Manager into this model. Instead, publish Microsoft Office patches using the Admin Publisher, and deploy and manage Microsoft Office patches using Application Manager or Application Self-service Manager.

Microsoft Office can still be uninstalled using Application Manager or Application Self-service Manager even after it has been enabled for patching using Patch Manager. This is because the ZDELETE method is never disabled.

Microsoft Update Catalog Supports Office XP, Office 2003, and Office 2007

When using the new Microsoft Update Catalog data feed, Patch Manager provides support for patching Microsoft Office XP, Microsoft Office 2003, and Microsoft Office 2007, as well as their stand-alone products. For example, the stand-alone products for Microsoft Office 2007 that can be patched using Patch Manager with the Microsoft Update Catalog are:

- Access 2007
- Excel 2007
- Groove 2007
- InfoPath 2007
- OneNote 2007
- Outlook 2007
- PowerPoint 2007
- Project 2007
- Publisher 2007
- SharePoint Designer 2007
- Visio 2007
- Word 2007

When using the new Microsoft Update Catalog data feed, the Patch Manager does not provide support for patching Microsoft Office 2000, or earlier, applications. This restriction is a result of the Patch Manager agent's reliance on the Microsoft Update Catalog to detect Microsoft vulnerabilities. Customers with Microsoft Office 2000 can continue to apply updates using Patch Manager with the MSSECURE data feed until Microsoft stops updating MSSECURE. As of this writing, Microsoft has announced it will no longer

update MSSECURE as of October 9, 2007, even though they have continued to update MSSECURE into 2008 and beyond. See About Microsoft Patch Acquisition and Management on page 65.

Customers who are currently patching Microsoft Office XP or Microsoft Office 2003 with Patch Manager and the MSSECURE data feed are encouraged to move to the new Microsoft Update Catalog feed; this will ensure continued patching capabilities after Microsoft retires the MSSECURE feed.

Microsoft Office Service Packs

HPCA Patch Manager supports deployment and acquisition of Microsoft Office service packs. In some cases, Microsoft will determine that a particular Microsoft Office patch is dependent on a specific service pack. In those cases, it will be necessary to distribute the Microsoft Office service pack prior to installing the patch.

The Microsoft Data Feed Prioritization selection determines whether Patch Manager has the ability to report and apply a pre-requisite service pack to a device.

- **For MSSecure, Microsoft Update Catalog, Client Automation**: Patch Manager Reports will assist in determining which bulletins have service pack dependencies, as that information is gathered during product discovery. For example, suppose you have Microsoft Project 2002 Gold installed locally to your agent computer. Patch Manager will identify that this computer is vulnerable to MS05-005. You will see this in the Patch Manager Compliance by Device report. In some cases, Microsoft requires that a service pack be installed before a bulletin can be applied. So, before MS05-005 can be deployed to your agent computer, Microsoft Project 2002 Service Pack 1 must be deployed. In some cases, application of the service pack will eliminate the vulnerability detected for the bulletin. For example, after this service pack is installed, the agent computer will still be out of compliance because MS05-005 has not been installed. In other words, for this agent computer to be in compliance, you will need to deploy Service Pack 1 and, then, MS05-005. Note that no bulletin or service pack will be deployed if the agent computer has not been entitled to it in policy.
- **For Microsoft Update Catalog Only**: Due to changes in this data feed, service pack dependencies cannot be obtained and reported by Patch Manager. It is imperative that Administrators research the pre-requisite service packs for applicable bulletins and entitle them to devices.

- **For Microsoft Update Catalog, Legacy**: For devices running Windows 2000 only, Patch Manager follows the behavior of the default data feed and will report and deploy dependent service packs to devices entitled to it in policy. For devices running platforms other than Windows 2000, Patch Manager follows the behavior of Microsoft Update Catalog and Administrators must research and entitle devices to pre-requisite service packs.

Best Practices with Microsoft Update Catalog Enabled

About Patch Manager and Microsoft Update Catalog

Enhancements introduced with Patch Manager version 3.0.2 enable it to use new technology, including the Microsoft Update Catalog data feed and the Windows Update Agent. For more information about Microsoft Update Catalog, refer to the Microsoft FAQs article at *http://update.microsoft.com/microsoftupdate/v6/about.aspx?ln=en-us*.

Patch Manager takes advantage of the Microsoft Update Catalog by using the Windows Update Agent to scan for vulnerabilities, install updates, and verify updates. The Windows Update Agent is responsible for installing updates for Windows operating systems as well as applications including Microsoft Office, thereby preventing Patch Manager from determining whether Microsoft Office applications are managed by Application Manager, Application Self-service Manager, or an Administrative Control Point.

Windows Installer version 3.1 is required to detect patches for Windows Installer-enabled applications like Microsoft Office, which use Microsoft Update Catalog.

When using Patch Manager Version 3.0.2 or above, updates for Microsoft Office applications will be detected and reported automatically, however the update will only be installed if the device is entitled.

- If you deploy patches for Microsoft Office using Patch Manager with Microsoft Update Catalog enabled, then you should no longer publish or deploy patches for Microsoft Office using Application Manager or Application Self-service Manager, or an external ACP. You must choose between the Patch Manager solution for patch management and your existing solution.
- If you choose Application Manager or Application Self-service Manager because you would like to leverage a feature derived from the ZCREATE, ZVERIFY, or ZUPDATE methods (such as their ability to manage MSI

Features and Properties or install on first use), then you are advised to publish Microsoft Office patches via the Publisher and then deploy and manage them using Application Manager or Application Self-service Manager. You should not introduce Patch Manager into this model.

- If you choose to continue to use an external ACP, then you should not introduce Patch Manager into this model. Doing so will likely break the synchronization between the agent and the ACP.
- If you choose to enable Patch Manager with the Microsoft Update Catalog data feed, perform the tasks in the topic below, Enabling Microsoft Office Updates in Patch Manager (Versions 3.0.2 or above).

Enabling Microsoft Office Updates in Patch Manager (Versions 3.0.2 and later)

Patch Manager is installed by default with Microsoft Office (`!Office*`) patches being excluded from acquisition. As of Version 5.0, both Microsoft Office and its set of standalone products are excluded from acquisition by default.

Use the steps below to enable Microsoft Office acquisition and deployment to agents in a Patch Manager environment that uses the Microsoft Update Catalog feed.

1. Ensure all devices have Windows Installer 3.1 installed.
2. When using Patch Manager with Microsoft Update Catalog data feed to deploy Microsoft Office patches, you do not need to modify any Patch Manager methods (as was required in versions prior to 3.0.2). This is because the code that honors the –IR and –IACP parameters is never executed due to changes in the Microsoft patch data feed.

As previously discussed, do not enable Patch Manager using Microsoft Update Catalog feed unless you will no longer be managing Microsoft Office updates with an existing solution: either Application Manager or Application Self-service Manager or an AIP. As soon as Patch Manager applies a patch using Microsoft Update Catalog, a Client Automation-managed application will fail verification, and the AIP-synchronized agents will no longer be connected to the AIP.

3 If you previously used Application Manager or Application Self-service Manager to manage Microsoft Office updates, blank out the existing values for the ZCREATE, ZVERIFY and ZUPDATE methods in the existing SOFTWARE.ZSERVICE class instance for Microsoft Office in your database. This ensures the `radiamsi` calls do not take place, and any desired-state processing by Application Manager or Application Self-service Manager does not undo the Patch Manager-deployed updates. For more information on editing these methods, refer to the Engineering Note, *Radia Client Methods and Pre-method Variables* (Document ID: KM99949) on the HP Software Support web site**.**

Do not blank out the ZDELETE method; ZDELETE gives you the ability to use Application Manager or Application Self-service Manager to uninstall Office.

4 On the patch acquisition machine, remove **`!Office*`** from the product exclusion filter.

5 If you are running Patch Manager V 5.0 or above from a fresh install, the default filter excludes acquisition of patches for Microsoft Office as well the individual Office products. On the patch acquisition machine, also remove any of the following Microsoft Office standalone products from the product exclusion filter, as desired:

```
,!Access*,!Excel*,!FrontPage 200[023],!FrontPage 9[78],
 !InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,
 !Project 200[023],!Project 98,!Publisher*,!Visio*,
 !Word*,!Works*
```

After removing the desired entries from the exclusion list, ensure the remaining entries are comma-separated.

6 Entitle the Microsoft Office bulletins to devices in policy.

About Patch Objects used for Device Compliance Reporting

The following agent objects are created to identify what products and patches are installed on the managed device.

- DESTATUS - Device Status Object: Contains a single heap identifying the overall device status, how many bulletins are in each compliance status, and the last scan time. Compliance status values include OK, Warning, Reboot Pending, Error, and Not Applicable.

- RESTATUS - Release Status Object: Contains one heap for every release that is present on the device.
- BUSTATUS - Bulletin Status Object; Contains one heap for each bulletin and gives the bulletin status.
- PASTATUS - Patch Status Object; Contains one heap for each patch and provides the patch status.
- DEERROR - Device Error Object: Contains any errors that occurred during discovery or management of the device.

These five objects correspond to five tables in the Patch ODBC Database: NVD_DESTATUS, NVD_RESTATUS, NVD_BUSTATUS, NVD_PASTATUS and NVD_DEERROR.

During the Client Automation Agent connect process, these objects are sent to the Configuration Server, where their contents are not stored in the Configuration Server Database, but copied to a directory that is monitored by the Messaging Server. The default location of this directory varies by platform, and is given below.

- `Drive:\Program Files\Hewlett-Packard\CM\ConfigurationServer\data\patch` (Windows).
- `/opt/HP/CM/ConfigurationServer/data/patch` (UNIX).

The Patch Delivery Agent in the Messaging Server posts this information to the Patch ODBC Database for storage and reporting. Only the most recent object for each device is kept.

Patch Agents prior to Version 5.0 reported this information using a single object, named ZOBJSTAT. The Patch Data Delivery Agent in the Messaging Server Version 5.10 and above will automatically post in-bound ZOBJSTAT objects to the current Patch Manager ODBC Database tables, as noted above.

Patch Manager Administrator Icons

When you are in the Patch Manager Administrator, there are icons available to take you to available functions, including access to the Reporting Server.

Figure 13 Click an icon

- Click the  icon to refresh the page.
- Click the  icon to return to Patch Manager Administrator home page.
- Click the  icon to print the currently viewed page.
- Click the  icon to go to Patch Manager Reporting using the Reporting Server.
- Click the  icon to see the latest Bulletin correction information.
- Click the  icon to see the latest agent update information.

Patch Analysis and Reports

The HPCA Reporting Server provides web-based reports for Patch Manager. For Reporting Server installation and configuration instructions, refer to the *HPCA Reporting Server Guide*. The Reporting Server installation media is with the Client Automation Infrastructure media.

To view the reports, access the Reporting Server using this icon in the toolbar:

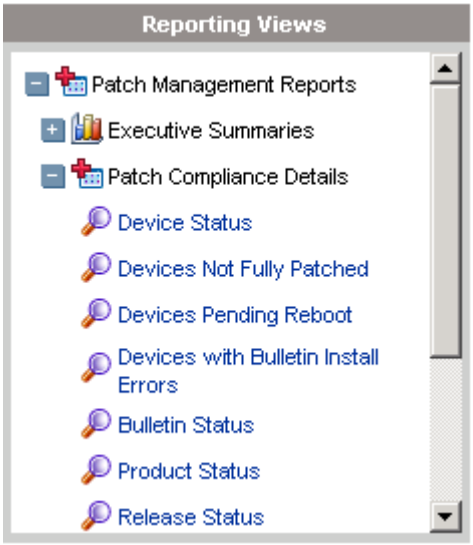
Then, under Reporting Views, click **Patch Management Reports** to expand the list of reports.

There are four types of Patch Manager reports:

- Executive Summaries on page 110: Executive Reports provide a snapshot of your environment from the patch-compliance perspective. Use these pie or bar chart reports to drill down into the detail reports about devices in or out of compliance, or about bulletins for which devices are in or out of compliance.
- Patch Compliance Reports on page 114: The Management Agent sends product and patch information to HPCA. This information is compared to the available patches to see if managed devices require certain patches to remove vulnerabilities. Compliance reports show only the information applicable to detected devices in your environment.
- Acquisition Reports on page 126: Acquisition-based reports show the success and failures of the patch acquisition process from a vendor's web site.
- Research Reports on page 126: Research-based reports display information about the patches acquired from the software vendor's web site. Research-based reports offer a Filter bar.

Expand each report type to see the list of available reports. For example, Figure 14 on page 106 shows the Patch Management report list expanded for Executive Summaries and Patch Compliance Details.

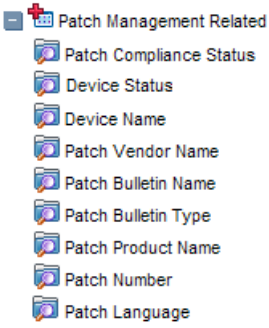
Figure 14 View the list of Patch Management Reports



Filtering Patch Reports with Reporting Server

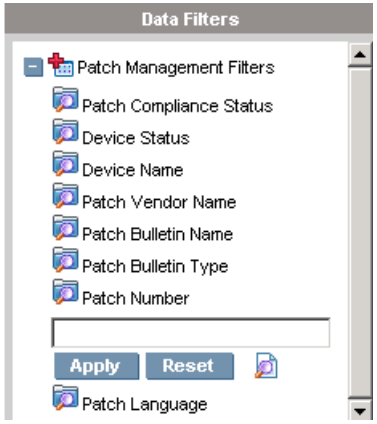
Reporting Server also provides filtering capabilities. To access the filters, expand Patch Management Related in the Search Controls section of the Reporting Server page.

Figure 15 View the Patch Management Related Data Filters



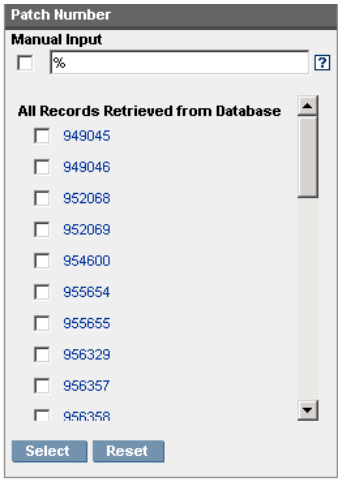
Some filters only allow a text entry. Others have a Show available options button or magnifying glass to open a filter lookup window.

Figure 16 Expand a filter



Click the magnifying glass  to open the filter lookup window.

Figure 17 Select the filter



Click any of the available criteria check boxes to select the criteria you would like to use in your filter.

Click **Select** to apply the filter and close the filter selection window.

For additional information on creating filters refer to the *Reporting Server Guide*.

Drilling Down to Detailed Information

Many reports enable you to drill down to very detailed information about a particular device or bulletin.

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.

Available Report Actions include Data Export Options

The following actions are available on the Reports page when a report is displayed, and include the ability to export report data to a comma-separated value (CSV) file or Web query (IQY) file:

Table 3 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.
	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.

Table 3 Report Actions

Icon	Description
	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.

HPCA reports are displayed in the Greenwich Mean Time (GMT) time zone.

Executive Summaries

There are four Executive Summaries for Patch Management that show a pie chart or bar chart of the patch compliance status in your environment.

The Executive Summary reports are color coded by patch status, which allow you to easily drill down into a particular report for a given patch status from the Executive Summary report.

Table 4 Patch Status on Executive Summary Reports

Color	Patch Status
Green	Compliant = Patched or Warning
Red	Not Compliant = Not Patched or Other or Reboot Pending
Green	Patched
Dark Green	Warning
Red	Not Patched
Yellow	Other
Gray	Reboot Pending
Dark Gray	Not Applicable

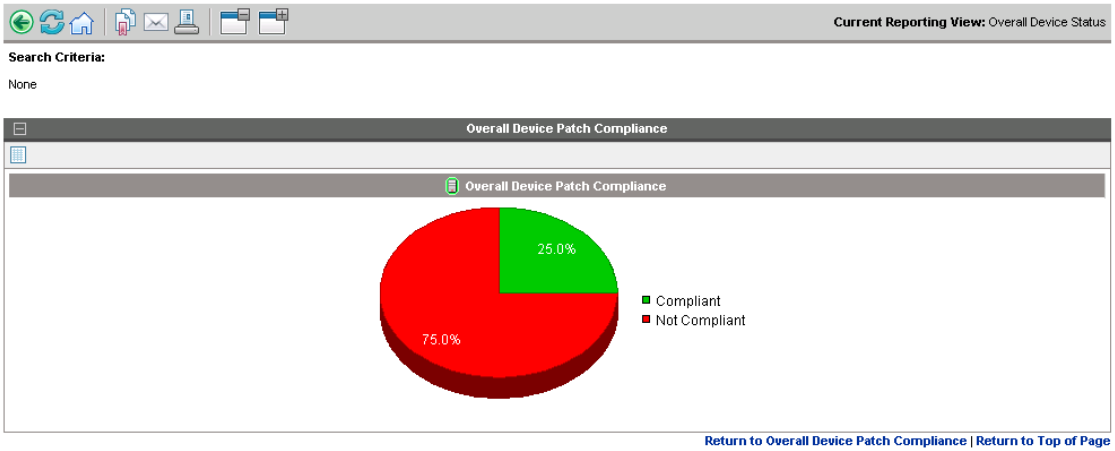
Sample Executive Summary Reports follow.

- Overall Device Status on page 111
- Device Status on page 112
- Bulletin Status on page 113
- Vendor Status on page 114

Overall Device Status

Shows a pie-chart of the overall percentage of managed-devices in your network that are patch-compliant and those that are not. A patch-compliant device has all applicable patches applied or has returned a warning status.

Applicable Filters: None.



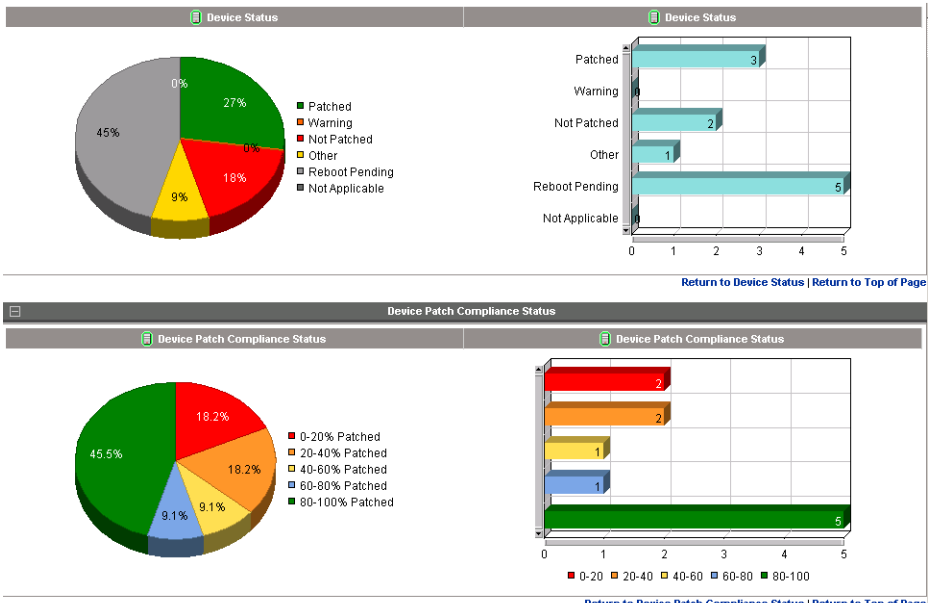
Device Status

Gives a pie-chart and bar graph breakdown of devices according to their patched-status. There are two graphical reports available:

- **Device Status**: This graphical report appears in the upper panel. The graphs provide percentages for devices in various states that include Patched, returned Warnings, Reboot Pending, Other Errors, or Not Patched.
  - Single-click on an individual status label or section to display the number of devices in that state.
  - Double-click on an individual status label or section to access a report that lists the devices in that state. Single-click on the name of a device in the device list to find the patch status for that particular device.
- **Device Patch Compliance Status**: This graphical report appears in the lower panel. The graphs provide patch percentages for devices indicating their patch compliance level. The patch compliance levels are shown in 20 percent bands. For example, if a device requires 10 bulletins, but only 5 patches have been applied, this device will be 50% patched and hence will be included in the 40-60% Patched band of the pie chart and bar graph.
  - Single-click on a band in the pie chart to display the list of devices that fall into this band.

— Single-click on the name of a device in the device list to see patch compliance information specific for that particular device.

Applicable Filters: Device name (finds the patch status and compliance status of a particular device).

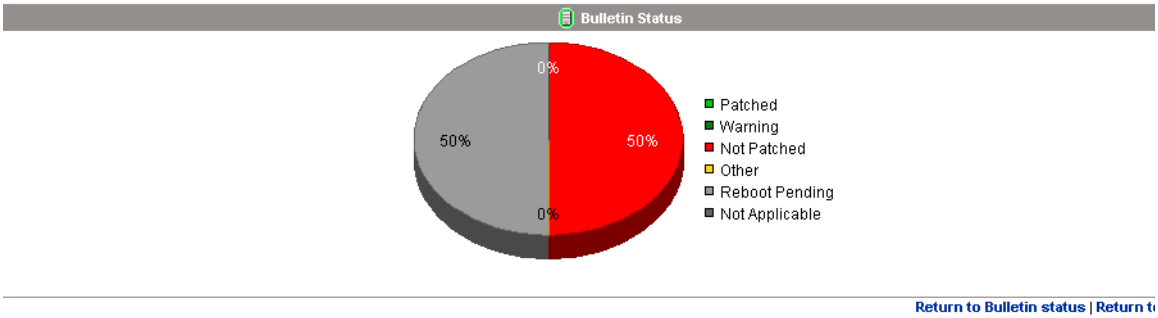


Bulletin Status

Give a pie-chart breakdown of all bulletins being-managed according to their patch-status.

- Single-click on an individual section or a status label to display the number of bulletins in that state.
- Double-click an individual section to list the bulletins with a particular status.

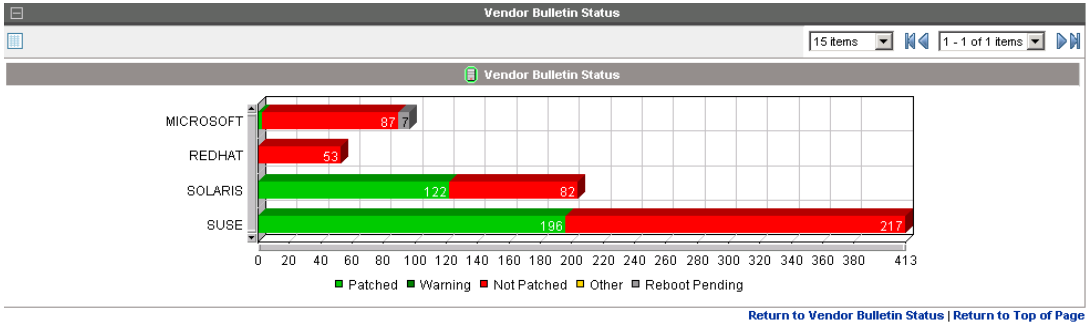
Applicable Filters: Device name (finds the patch status of different bulletins for this device).



Vendor Status

Gives a bar-chart of bulletins for each vendor according to their bulletin patched-status. The bar shows different colors for bulletins in different states.

Applicable Filters: None.



Patch Compliance Reports

When a device in your enterprise runs the Patch Manager Agent, product and patch information is sent to the Patch Manager. Then, this information is compared to the available patches to see if this device requires a patch to remove vulnerabilities. Patch Compliance reports show only the information applicable to detected devices in your environment.

The Patch Compliance Reports include:

The Patch Compliance Reports documented in this guide require the servers and agents in your Patch Manager environment to be at Version 7.50 or above.

In particular, the Product Status, Release Status, and Patch Status reports documented in this guide cannot be populated by pre-Version 7.50 Patch Agents.

Device Status

Use the Device Status report to see the patch compliance status of all devices under Client Automation patch management. The date of the last scan is listed next to the Device name.

Note: The Report title shows Device Status.

Applicable Filters: Device name and Patch Compliance Status (e.g. Patched, Not patched, Reboot Pending, etc.).

Each row contains information relating to a specific device and an icon.

— A check mark indicates all applicable vulnerabilities have been patched. This device is in compliance according to your current patch policy.

— A power button indicates that the vulnerability will be in compliance pending a device reboot.

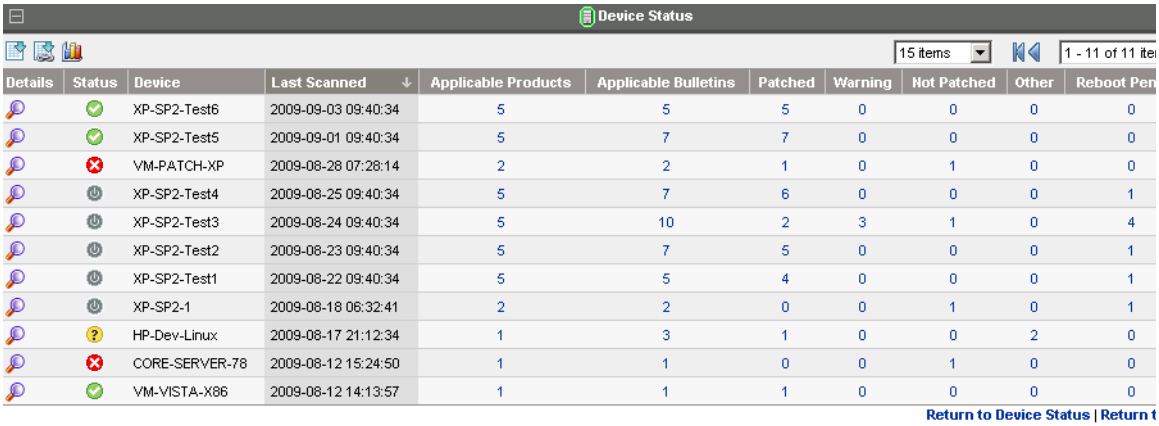
> A pending reboot status will take precedence over a not-patched status, because it is, typically, a short term device status. After the reboot, the device will again show the worst case status. For example, after reboot, if the device still has a vulnerability that has not been patched, the device will display with a red X to show this.

— A question mark indicates that at least one vulnerability could not be confirmed.

— A red X indicates that at least one vulnerability is not patched for this device.

— An exclamation point indicates a warning.

— A lower-case letter ‘i’ indicates *Not Applicable*.



Device Status

15 items | 1 - 11 of 11 ite

Details	Status	Device	Last Scanned	Applicable Products	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pen
		XP-SP2-Test6	2009-09-03 09:40:34	5	5	5	0	0	0	0
		XP-SP2-Test5	2009-09-01 09:40:34	5	7	7	0	0	0	0
		VM-PATCH-XP	2009-08-28 07:28:14	2	2	1	0	1	0	0
		XP-SP2-Test4	2009-08-25 09:40:34	5	7	6	0	0	0	1
		XP-SP2-Test3	2009-08-24 09:40:34	5	10	2	3	1	0	4
		XP-SP2-Test2	2009-08-23 09:40:34	5	7	5	0	0	0	1
		XP-SP2-Test1	2009-08-22 09:40:34	5	5	4	0	0	0	1
		XP-SP2-1	2009-08-18 06:32:41	2	2	0	0	1	0	1
		HP-Dev-Linux	2009-08-17 21:12:34	1	3	1	0	0	2	0
		CORE-SERVER-78	2009-08-12 15:24:50	1	1	0	0	1	0	0
		VM-VISTA-X86	2009-08-12 14:13:57	1	1	1	0	0	0	0

Return to Device Status | Return t

For each device, you can:

— Click the magnifying glass for additional detail.

— Click the number in the Applicable Products column to see the products discovered for that device.

— Click the number in the Applicable Bulletins column to see the applicable bulletins for that device.

— Click the number in the Patched column to see the list of bulletins that were installed as patches on this device.

— Click the number in the Warning column to see vulnerabilities that the Patch Manager cannot confirm as patched because there may be some discrepancy in the patch verification process.

  For example, a patch for Microsoft SQL server or Microsoft MSDE may show up as a warning. MSDE installs fewer files than SQL Server. A device with MSDE may qualify for the same patch as a device with SQL server, but does not require all the files in the patch. Since Patch Manager cannot report the vulnerability as being patched, this would be reported as a warning.

  Another example may be that a file version on the device is newer than the one delivered by the patch. Again, in this case, Patch Manager cannot report the vulnerability as being patched so it reports a warning.

— Click the number in the Not Patched column to see what patches are available but have not been applied to this device.

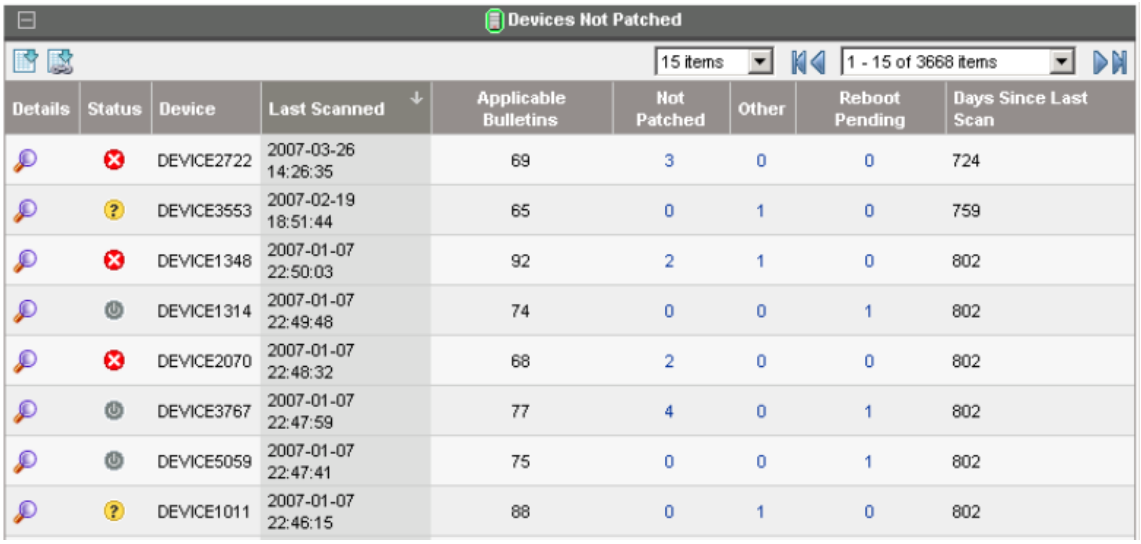
— Items in the Other column represent patches that Patch Manager was not able to verify or was not able to patch due to a device error.

— Items in the Reboot Pending column represent patches that will be complete after the device is rebooted. These devices will also have a power button icon next to the device name.

Devices Not Fully Patched

Use this Compliance report to focus on the devices that are not in compliance with your patch policy. The devices included on this report show one or more Applicable Bulletins with a status of Not Patched, Other (includes device errors) or Pending Reboot. This report is similar to the Device Status on page 115, except that it eliminates any devices considered in compliance because all of their applicable bulletins are either patched or just report warnings.

Applicable Filters: Device name and Patch Compliance Statuses of Not patched, Other, and Reboot Pending.



Devices Not Patched

15 items | 1 - 15 of 3668 items

Details	Status	Device	Last Scanned	Applicable Bulletins	Not Patched	Other	Reboot Pending	Days Since Last Scan
		DEVICE2722	2007-03-26 14:26:35	69	3	0	0	724
		DEVICE3553	2007-02-19 18:51:44	65	0	1	0	759
		DEVICE1348	2007-01-07 22:50:03	92	2	1	0	802
		DEVICE1314	2007-01-07 22:49:48	74	0	0	1	802
		DEVICE2070	2007-01-07 22:48:32	68	2	0	0	802
		DEVICE3767	2007-01-07 22:47:59	77	4	0	1	802
		DEVICE5059	2007-01-07 22:47:41	75	0	0	1	802
		DEVICE1011	2007-01-07 22:46:15	88	0	1	0	802

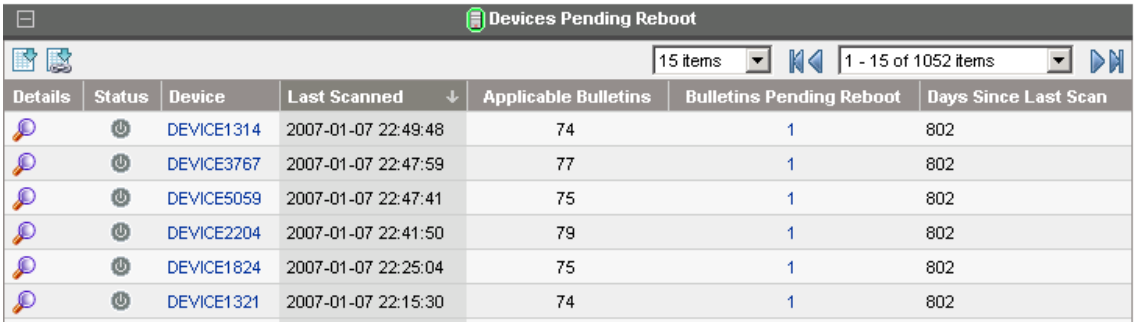
— For each device, you can perform the same operations as discussed with the Compliance report for Device Status on page 115.

— The last column indicates the number days since the device was last scanned.

Devices Pending Reboot

Use this Compliance report to focus on the devices that have at least one bulletin Pending Reboot.

Applicable Filters: Device name.



Devices Pending Reboot

15 items | 1 - 15 of 1052 items

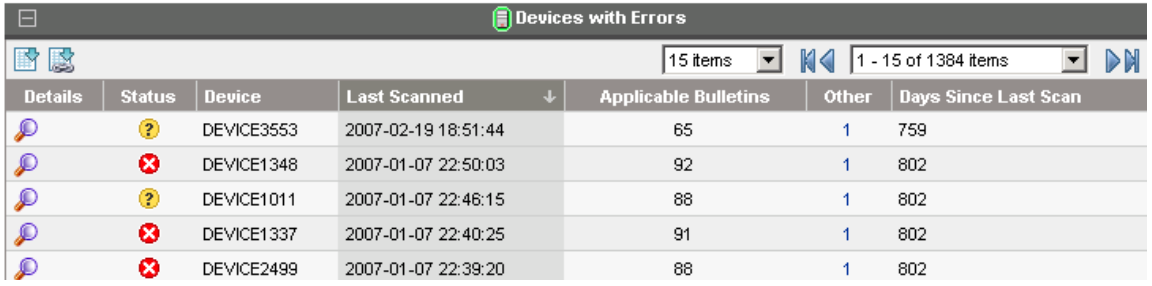
Details	Status	Device	Last Scanned	Applicable Bulletins	Bulletins Pending Reboot	Days Since Last Scan
		DEVICE1314	2007-01-07 22:49:48	74	1	802
		DEVICE3767	2007-01-07 22:47:59	77	1	802
		DEVICE5059	2007-01-07 22:47:41	75	1	802
		DEVICE2204	2007-01-07 22:41:50	79	1	802
		DEVICE1824	2007-01-07 22:25:04	75	1	802
		DEVICE1321	2007-01-07 22:15:30	74	1	802

— Click on links provided in a column to see the details for that column for the device.

Devices With Bulletin Install Errors

Use this Compliance report to view the list of devices that encountered any errors while installing bulletins.

Applicable Filters: Device name.

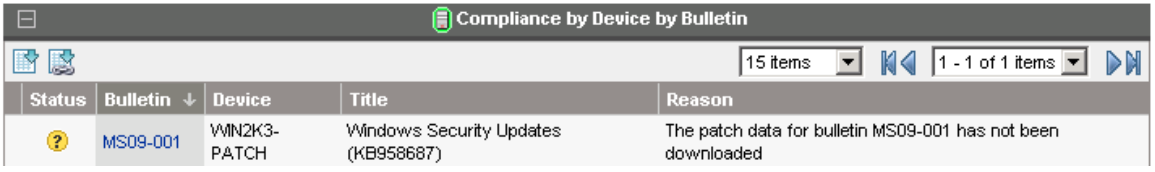


Devices with Errors

15 items | 1 - 15 of 1384 items

Details	Status	Device	Last Scanned	Applicable Bulletins	Other	Days Since Last Scan
		DEVICE3553	2007-02-19 18:51:44	65	1	759
		DEVICE1348	2007-01-07 22:50:03	92	1	802
		DEVICE1011	2007-01-07 22:46:15	88	1	802
		DEVICE1337	2007-01-07 22:40:25	91	1	802
		DEVICE2499	2007-01-07 22:39:20	88	1	802

— Click the number in the **Other** column to link to list of bulletin(s) for that device which encountered errors and the error description. An example is shown below:



Compliance by Device by Bulletin

15 items | 1 - 1 of 1 items

Status	Bulletin	Device	Title	Reason
	MS09-001	WIN2K3-PATCH	Windows Security Updates (KB958687)	The patch data for bulletin MS09-001 has not been downloaded

Bulletin Status

Use Bulletin Status to display the patch ‘Compliance by Bulletin’ report. For a given bulletin, the report lists the number of devices for which the bulletin is applicable and the number of devices with different patch statuses for the bulletin. The patch status include Patched, Warning, Not Patched, Other (Errors encountered) or Reboot Pending.Each row contains information relating to a specific bulletin and an icon.

Applicable Filters: Bulletin name, bulletin vendor or bulletin type (for example, Security Update or Service Pack).

Each row contains information relating to a specific bulletin and an icon.

— A check mark indicates that this bulletin has been patched on all applicable devices.

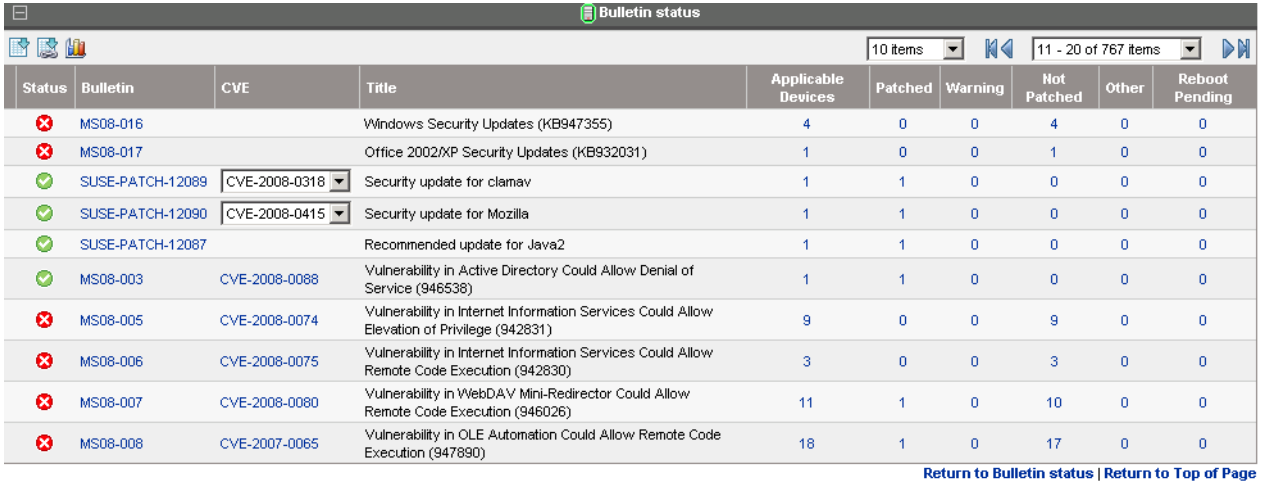
— A power button indicates that at least one device is pending a reboot to be in compliance.

A pending reboot status will take precedence over a not-patched status, because it is, typically, a short term device status. After the reboot, the device will again show the worst case status. For example, after reboot, if the device still has a vulnerability that has not been patched, the bulletin will display with a red X to show this.

— A question mark indicates that this vulnerability could not be confirmed on at least one device.

— A red X indicates at least one device is not patched for this bulletin.

— An exclamation mark indicates a warning.



Bulletin status

10 items | 11 - 20 of 767 items

Status	Bulletin	CVE	Title	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pending
	MS08-016		Windows Security Updates (KB947355)	4	0	0	4	0	0
	MS08-017		Office 2002/XP Security Updates (KB932031)	1	0	0	1	0	0
	SUSE-PATCH-12089	CVE-2008-0318	Security update for clamav	1	1	0	0	0	0
	SUSE-PATCH-12090	CVE-2008-0415	Security update for Mozilla	1	1	0	0	0	0
	SUSE-PATCH-12087		Recommended update for Java2	1	1	0	0	0	0
	MS08-003	CVE-2008-0088	Vulnerability in Active Directory Could Allow Denial of Service (946538)	1	1	0	0	0	0
	MS08-005	CVE-2008-0074	Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831)	9	0	0	9	0	0
	MS08-006	CVE-2008-0075	Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830)	3	0	0	3	0	0
	MS08-007	CVE-2008-0080	Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026)	11	1	0	10	0	0
	MS08-008	CVE-2007-0065	Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)	18	1	0	17	0	0

Return to Bulletin status | Return to Top of Page

For each bulletin, you can:

— Click the bulletin number in the Bulletin column to go to the vendor's web site for more information on the bulletin.

— Click the CVE number in the CVE column to go the Common Vulnerabilities and Exposures web site.

— Click the number in the Applicable Devices column to see the applicable devices for that bulletin.

— Click the number in the Patched column to see the patched devices.

— Click the number in the Warning column to see vulnerabilities that the Patch Manager cannot confirm as patched because there may be some discrepancy in the patch verification process.

  For example, a patch for Microsoft SQL server or Microsoft MSDE may show up as a warning. MSDE installs fewer files than SQL Server. A device with MSDE may qualify for the same patch as a device with SQL server, but does not require all the files in the patch. Since Patch Manager cannot report the vulnerability as being patched, this would be reported as a warning.

Another example may be that a file version on the device is newer than the one delivered by the patch. Again, in this case, Patch Manager cannot report the vulnerability as being patched so it reports a warning.

— Click the number in the Not Patched column to see what patches are available but have not been applied.

— Items in the Other column represent patches that Patch Manager was not able to verify or encountered an error.

— Items in the Reboot Pending column represent patches that will be complete after the device is rebooted.

Product Status

The Product Status view displays the Compliance by Products report, with one row for each product and patch distribution method. For example:

— Product names appended with (MSFT) were distributed with "Enable Download of Metadata" turned on.

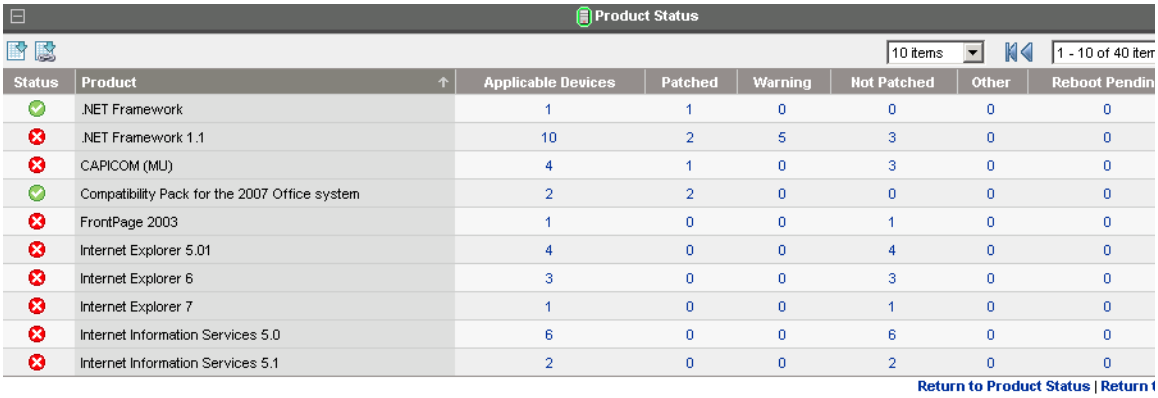
— Product names without qualification were distributed with "Enable Download of Metadata" turned off.

This report requires HPCA Agents at Version 7.50 or above. The report will not be populated and show zero records if pre-Version 7.50 Patch Agents are operating in an HPCA 7.50 Server environment.

Applicable Filters: Product Name, Device Name, Patch Compliance Status.

For each product, you can:

— View detected vulnerabilities



— Click a number in one of the count columns to see the details of the devices with the number of Applicable Bulletins for that product.

— From the resulting view, click on Applicable Bulletins to see the list of bulletins applicable for the selected device for the product release.

Release Status

The Release Status view displays the ‘Compliance by Release’ report listing products by release. There is one row for each release of each product and patch distribution method. For example:

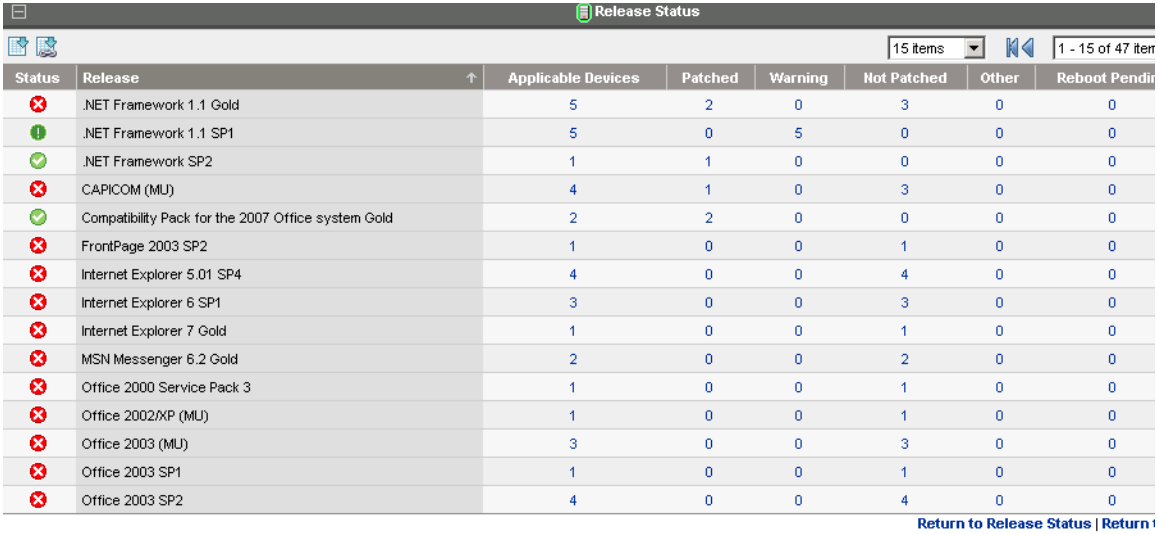
— Release names appended with (MSFT) have bulletins distributed with “Enable Download of Metadata” turned on.

— Release names without qualification have bulletins distributed with “Enable Download of Metadata” turned off.

Click to see Applicable Bulletins.

This report requires HPCA Agents at Version 7.50 or above. The report will not be populated and show zero records if pre-Version 7.50 Patch Agents are operating in an HPCA 7.50 Server environment.

Applicable Filters: Release Name, Device Name, or Patch Compliance Status.



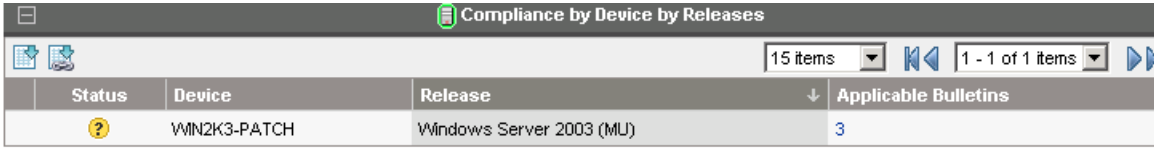
Release Status

15 items | 1 - 15 of 47 item

Status	Release	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pendi
✗	.NET Framework 1.1 Gold	5	2	0	3	0	0
!	.NET Framework 1.1 SP1	5	0	5	0	0	0
✓	.NET Framework SP2	1	1	0	0	0	0
✗	CAPICOM (MU)	4	1	0	3	0	0
✓	Compatibility Pack for the 2007 Office system Gold	2	2	0	0	0	0
✗	FrontPage 2003 SP2	1	0	0	1	0	0
✗	Internet Explorer 5.01 SP4	4	0	0	4	0	0
✗	Internet Explorer 6 SP1	3	0	0	3	0	0
✗	Internet Explorer 7 Gold	1	0	0	1	0	0
✗	MSN Messenger 6.2 Gold	2	0	0	2	0	0
✗	Office 2000 Service Pack 3	1	0	0	1	0	0
✗	Office 2002/XP (MU)	1	0	0	1	0	0
✗	Office 2003 (MU)	3	0	0	3	0	0
✗	Office 2003 SP1	1	0	0	1	0	0
✗	Office 2003 SP2	4	0	0	4	0	0

Return to Release Status | Return

— Click the number of Applicable Devices to see a list of devices with the number of applicable bulletins for each device for a this product release, as shown in the following figure.



Compliance by Device by Releases

15 items | 1 - 1 of 1 items

Status	Device	Release	Applicable Bulletins
?	WIN2K3-PATCH	Windows Server 2003 (MU)	3

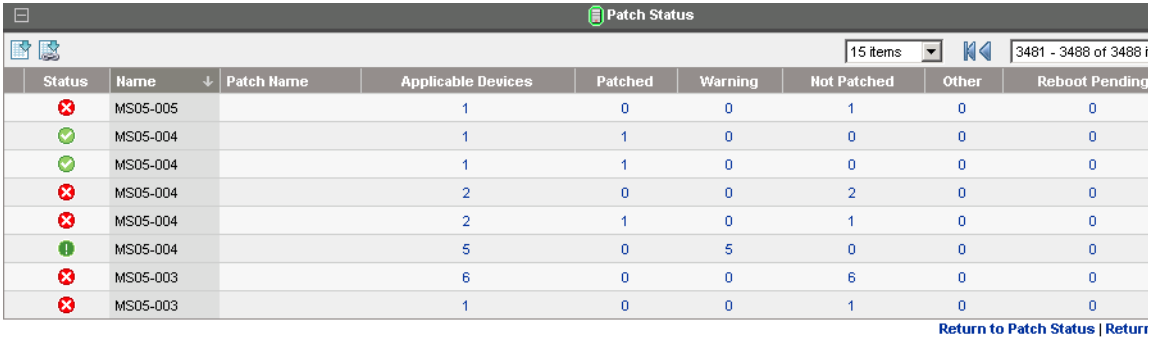
— Click the number of Applicable Bulletins to see the list of bulletins applicable for this device for this product release.

Patch Status

The Patch Status view displays a list of products by patch in the ‘Compliance by Patches’ report. There is one row for each patch.

This report requires HPCA Agents at Version 7.50 or above. The report will not be populated and show zero records if pre-Version 7.50 Patch Agents are operating in an HPCA 7.50 Server environment.

Applicable Filters: Patch Language, Patch Qnumber, Patch Number, Bulletin Name and Patch Compliance Status.



— Click the number of Applicable Devices or a count column to see the devices for that particular column.

Devices with Serious Errors

The Devices with Serious Errors view displays a report listing errors encountered on agent devices.

To use this report, ensure the FINALIZE_PATCH service has been entitled to the managed devices in your environment, as discussed in the sectionEntitle the FINALIZE_PATCH Service on page 133

Acquisition Reports

There are three Acquisition Reports:

- Acquisition Summary
- Acquisition Bulletin
- Acquisition by Patch

For information on the Acquisition reports, see Patch Acquisition Reports on page 84.

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.

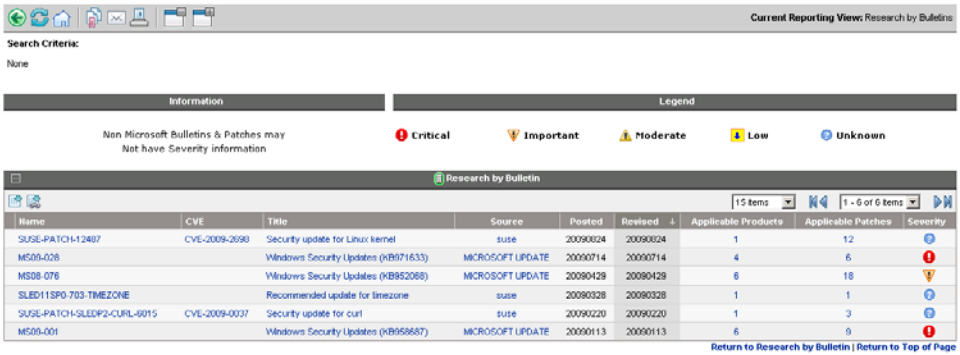
The Research Reports include:

- Research by Bulletin on page 126
- Research by Devices on page 127
- Research by Patches on page 128
- Research by Products on page 129
- Research by Releases on page 130
- Compliance and Research Exception Reports on page 130

Research by Bulletin

Use this report to drill down to all bulletins. Click on the bulletin's number in the Name column to go to the vendor's web site for more information. Click on the number in the CVE column to go to the Common Vulnerability Exposures web site. Click the number in the Title or Applicable Patches column to view the files needed for this bulletin, to see if they are available for deployment, and to see if the patch has been superseded by another patch. Click the number in the Applicable Products column to see which products are influenced by this bulletin. The icon in the Severity column indicates the severity for Windows bulletins. The severity ratings range from Critical, to Important, to Moderate, to Low. If the bulletin is not for a Windows platform, the Unknown icon is displayed. Click on the icon in the Severity column to see

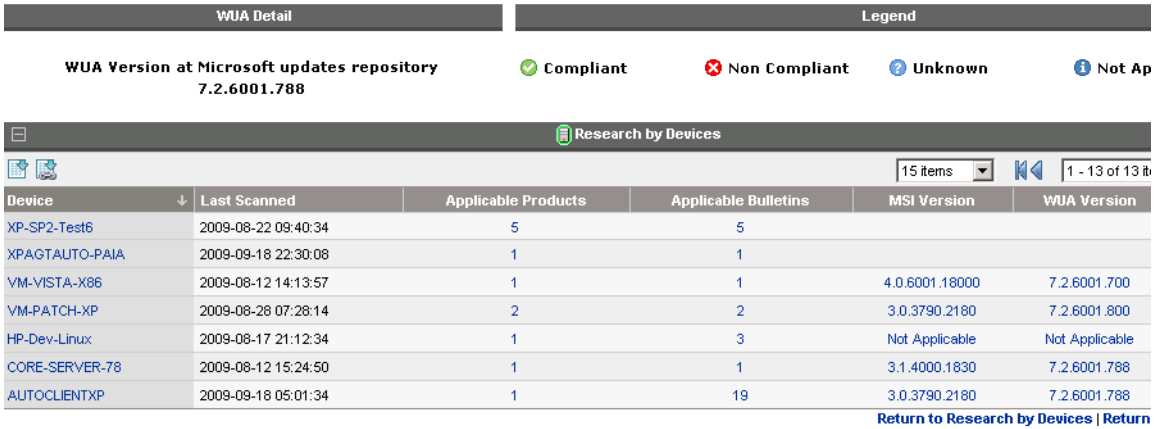
all bulletins with the same severity. Pre-existing bulletins do not have severity ratings. To view severity ratings for existing bulletins and patches, you must re-acquire them using the Force and Replace options.



Research by Devices

Use this report to drill down to all bulletins filtered by a particular device. Click the number in the Applicable Products column to see the discovered products on the device. Click the version number in the MSI Version column to see all devices having that version of the Microsoft Windows installer. Click the number in the WUA Version column to see all devices having that version of the Windows Update Agent. The Status column displays icons indicating Compliant or Non Compliant status depending if the version of the Windows Update Agent on the device is the same/newer or older than the latest version available on the server. If there is no Windows Update Agent version information available for the device, the Unknown icon is displayed. Click the status icon in the Status column to see all devices having that status for the Windows Update Agent. The filters in this table can be used in combination and the information can be sorted by clicking the column headings.

.

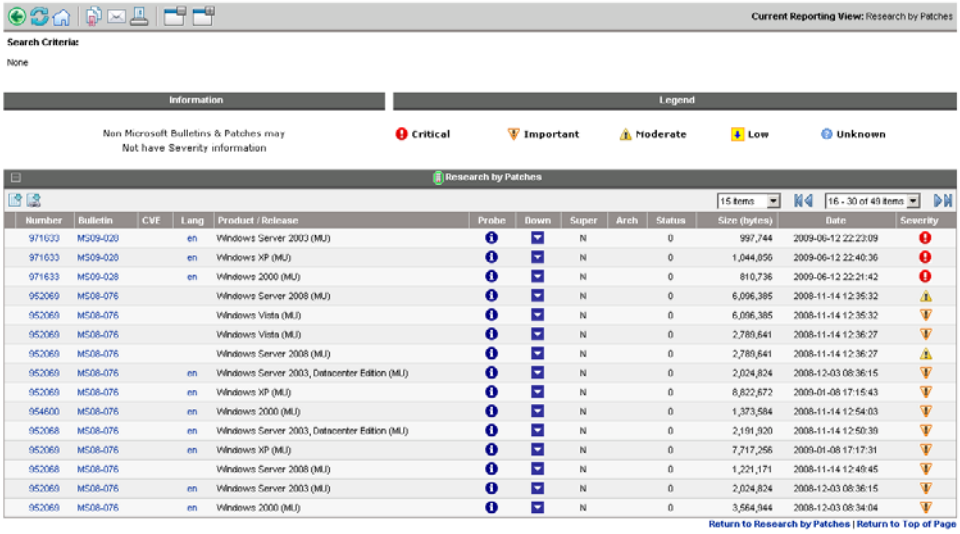


Device	Last Scanned	Applicable Products	Applicable Bulletins	MSI Version	WUA Version
XP-SP2-Test6	2009-08-22 09:40:34	5	5		
XPAGTAUTO-PAIA	2009-09-18 22:30:08	1	1		
VM-VISTA-X86	2009-08-12 14:13:57	1	1	4.0.6001.18000	7.2.6001.700
VM-PATCH-XP	2009-08-28 07:28:14	2	2	3.0.3790.2180	7.2.6001.800
HP-Dev-Linux	2009-08-17 21:12:34	1	3	Not Applicable	Not Applicable
CORE-SERVER-78	2009-08-12 15:24:50	1	1	3.1.4000.1830	7.2.6001.788
AUTOCLIENTXP	2009-09-18 05:01:34	1	19	3.0.3790.2180	7.2.6001.788

Research by Patches

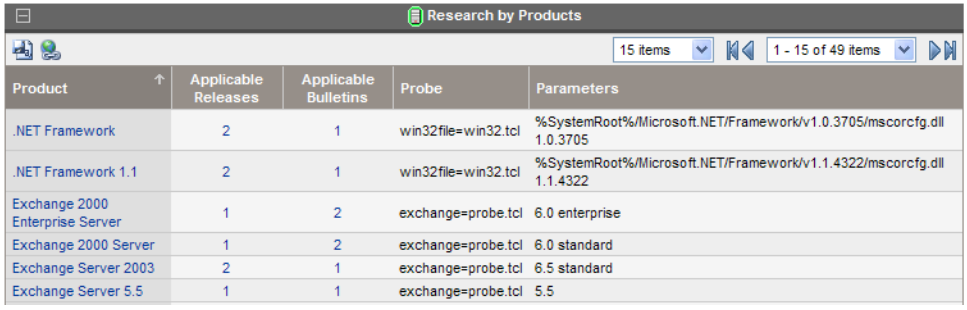
Use this report to view information on patch files including on acquisition status. Click the number in the CVE column to go to the Common Vulnerability Exposures web site. Click the icon in the Down column to download the patch file. The icon in the Severity column indicates the severity for Windows patches. The severity ratings range from Critical, to Important, to Moderate, to Low. If the patch is not for a Windows platform, the Unknown icon is displayed. Click on the icon in the Severity column to see all patches

with the same severity. Pre-existing patches do not have severity ratings. To view severity ratings for existing bulletins and patches, you must re-acquire them using the Force and Replace options.



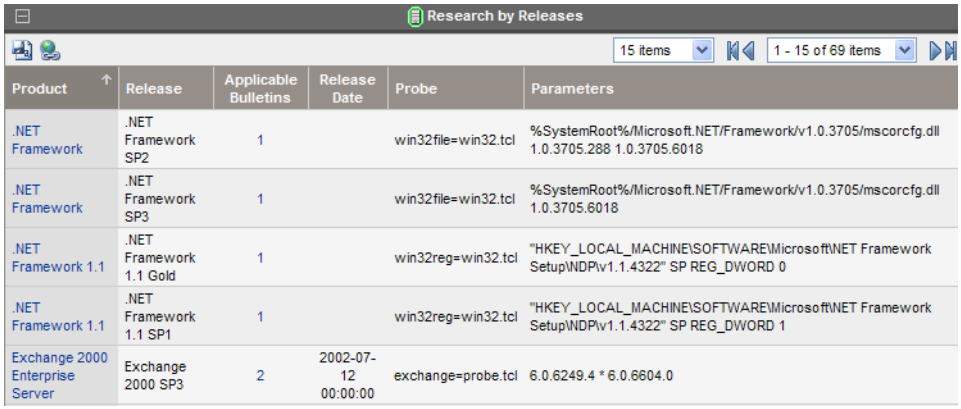
Research by Products

Use this report to drill down to all bulletins filtered by product.



Research by Releases

Use this report to filter by product release. Click the number in the Applicable Bulletins column to see all bulletins for the release.



Research by Releases

15 items | 1 - 15 of 69 items

Product	Release	Applicable Bulletins	Release Date	Probe	Parameters
.NET Framework	.NET Framework SP2	1		win32file=win32.tcl	%SystemRoot%/Microsoft.NET/Framework/v1.0.3705/mscorcfg.dll 1.0.3705.288 1.0.3705.6018
.NET Framework	.NET Framework SP3	1		win32file=win32.tcl	%SystemRoot%/Microsoft.NET/Framework/v1.0.3705/mscorcfg.dll 1.0.3705.6018
.NET Framework 1.1	.NET Framework 1.1 Gold	1		win32reg=win32.tcl	"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v1.1.4322" SP REG_DWORD 0
.NET Framework 1.1	.NET Framework 1.1 SP1	1		win32reg=win32.tcl	"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v1.1.4322" SP REG_DWORD 1
Exchange 2000 Enterprise Server	Exchange 2000 SP3	2	2002-07-12 00:00:00	exchange=probe.tcl	6.0.6249.4 * 6.0.6604.0

Compliance and Research Exception Reports

The Compliance and Research Exception Reports were introduced to provide information about devices that do not meet the criteria for the standard research and compliance device reports. All of the devices in these exception reports are in some sort of exception state. The three main reasons for this exception state are:

- connection errors during patch discovery.
- an acquisition performed with force and replace options that caused a disconnect with the device's status information.
- an inoperable Patch Manager Agent.

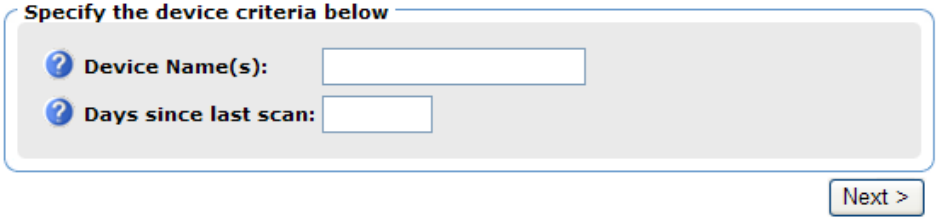
To resolve the exception, perform a new discovery on the device. The new discovery will either resolve the error, in the case of the acquisition disconnect and, possibly, the connectivity problem. In addition, it will produce logs that can be used to troubleshoot the inoperable Patch Manager Agent. The research exception report will likely show only a subset of the devices in the compliance exception report because the criteria for the research reports are less restrictive.

Deleting Devices

You can delete Patch Manager compliance data for specific devices using the Patch Administrator.

To remove compliance data from the Patch Manager ODBC database

1 Go to the **Operations** area of the Patch Manager Administrator and click **Delete Devices**.



2 Specify device-selection criteria for the devices to remove. You may:

- Specify a single device or multiple devices in a comma-separated list.
- Use wildcards.
- Specify the number of days since the last vulnerability scan was performed on the device. This may be used to remove compliance information for devices who are no longer reporting compliance data to the Patch Manager Infrastructure components.

3 The Patch Manager Administrator allows you to preview the devices that match the selection filters before removing them from the database.

4 Click **Delete** to remove the devices from the Patch Manager ODBC database.

Take care when removing devices from this database; this operation cannot be undone.

Managing Vulnerabilities

After you have found where vulnerabilities may exist in your enterprise, use Patch Manager to manage these vulnerabilities on managed devices. For every bulletin, there is a Services (ZSERVICE) instance in the PATCHMGR Domain that is similar to the Application (ZSERVICE) instance in the SOFTWARE domain. Refer to the *HPCA Application Manager and Application Self-Service Manager Guide* for complete descriptions of the attributes available in the ZSERVICE instance in the SOFTWARE domain. In addition, the PATCHMGR.ZSERVICE instance supports bandwidth throttling. Visit the HP Support web site for details.

Set policy entitlement at the ZSERVICE level. Connect the ZSERVICE instance that has the same name as a bulletin to the user instances in the POLICY domain or to the Null Instance.

SuSE 11 bulletins will have HP-assigned instance names that are derived from the original bulletin names. For details, see Instance Naming Convention for SuSE 11 Bulletins on page 133.

To manage a vulnerability

1. Open the Admin CSDB Editor and navigate to the PRIMARY.POLICY.USER class.
2. Right-click a user instance and select **Show Connections**.
3. Select **PATCHMGR Domain** from the **Show connectable classes for domain** drop-down box.
4. Click **OK**.
5. Drag-and-drop the bulletin you want to manage the vulnerability for to the appropriate user instance. When the cursor turns to a paper clip, release the mouse button.
6. Click **Copy**.
7. Click **Yes** to confirm the connection.

The patch is added to the user's policy. The next time the user logs in the vulnerability will be managed, including installation if necessary.

Instance Naming Convention for SuSE 11 Bulletins

As the instance field length in the CSDB is limited to 32 characters, all SuSE11 bulletins will be published using HP-reformatted instance names that are shorter and easier to distinguish than the actual SuSE 11 bulletin names.

During acquisition the SuSE11 bulletin name will be converted into a new name and the instance name under PRIMARY.PATCHMNGR.BULLETIN and PRIMARY.PATCHMGR.ZSERVICE will be created in the newly formed name.

The new instance name will be formed in the following way:

For example, HP Patch Manager will convert the SuSE 11 bulletin name entered for acquisition as:

`UPDATEINFO-SLESSP0-MOZILLAFIREFOX-1234`

to:

`SLES11SP0-1234-MOZILLAFIREFOX`

The reformatting drops the `UPDATEINFO-` prefix and reorders the remaining content to move the unique numbering scheme earlier in the format. For uniqueness among multiple SuSE versions, `SLESSP0` is expanded to include the version `(11)` between the product and service pack, as in `SLES11SP0`.

For the above example, the CSDB instance under `PRIMARY.PATCHMGR.BULLETIN` and `PRIMARY.PATCHMGR.ZSERVICE` will be created using the name `SLES11SP0-1234-MOZILLAFIREFOX`.

Note that any comma, dot, or underscore in the original SuSE bulletin name is always replaced by a hyphen (-) in the reformatted instance name created in CSDB.

Entitle the FINALIZE_PATCH Service

During a Patch Manager Agent connect, applicable patches are downloaded and queued for management by a Patch Manager Service called FINALIZE_PATCH. This service is prioritized to run as the last service on Patch Manager agents. This service is required to report real time patch compliance information.

Add the PRIMARY.PATCHMGR.ZSERVICE.FINALIZE_PATCH service to the policy for all managed devices, in addition to any patch.

Failure to use this service results in extended patch management activities and times, as well as failures in the reporting of real time patch compliance information.

Deploying Automatic and Interactive Patches

Some patches require user intervention for deployment as designed by the patch's vendor. Patch Manager defines a patch as **automatic** if it does not require user interaction for deployment. A patch is defined as **interactive** if it requires user interaction for deployment. Patch Manager can detect vulnerabilities for both automatic and interactive patches. Patch Manager supports deployment of both interactive and automatic patches. However, those which the vendor has created as interactive will either require user intervention to be installed or will fail to be installed.

Only bulletins that Hewlett-Packard has provided data correction for in an xml file or that a customer has customized may be marked as interactive. This information can be found in the Deployment attribute in the Bulletin and Patch nodes of a Hewlett-Packard provided xml file. Valid values are AUTOMATIC and INTERACTIVE. By default, the vendor does not supply this information. Therefore, customers are required to test the deployment of a patch to verify if it is interactive before entitling the bulletin in their environment.

When the bulletin is published to the Configuration Server Database, the RUNMODE attribute of the ZSERVICE class of the PATCHMGR Domain defines the type of patch. Use the catexp parameter of the radskman command line to limit your installation to bulletins marked as automatic only. The format would be catexp=runmode:automatic. If the catexp parameter does not exist, all bulletins will be processed. For a typical Patch Manager Agent connect, you may want to use the following radskman command line.

```
radskman ip=<RCSIP>,port=<RCSPORT>,dname=patch,catexp=
runmode:automatic
```

For more information on radskman, refer to the *Application Manager and Application Self-service Manager Guide*.

Customizing Reporting Options

In some cases, you may not want to mark a vulnerability as an error (shown as an X), or you may not want to mark a warning (shown as an exclamation point [!]) with a status of OK (check mark). Defaults are supplied in the OPTIONS class. You may want to view instances of the OPTIONS class as examples.

The information regarding the OPTIONS class applies only to patches downloaded using MSSECURE.XML not Microsoft Update. When patches are acquired from Microsoft Update, the Source column in the report will show “Microsoft Update” instead of “Microsoft.”

If you need to modify this behavior, create a custom `.xml` file using the following three new descriptor attributes.

- **DesiredState**
  This attribute maps to the DSTATE attribute in the OPTIONS, FILECHG, and REGCHG classes. Use this attribute to set what the return code should be based on the criteria stated in the USE variable.
- **Report Threshold**
  This xml attribute maps to the REPORT attribute in the OPTIONS, FILECHG, and REGCHG classes. The properties of the file or registry key will be sent to the Patch Manager based on this value. If the return code is greater than or equal to the value of the REPORT attribute, the file and registry information will be sent to the Patch Manager and will be available in Patch Manager reports. For example, set REPORT to **`1`** to send the properties if the return code is either 4 (Warning) or 8 (Error).

  Setting REPORT to **`0`** will send the information for all files that show an OK status. This may overburden the Patch Manager Server.

- **Use**
  This xml attribute maps to the USE attribute in the OPTIONS, FILECHG, and REGCHG classes. USE specifies what the criteria are that you are judging against. The possible criteria for the files (FILECHG) are GMTDATE, SIZE, VERSION, CHECKSUM, and CRC32. For registry the option is VALUE.

  Be aware that if you customize how a file or registry change is reported, then vulnerabilities may still exist, but will not be reflected in your reports. Prior to changing the reporting status of a detected vulnerability, be sure you have taken measures to eliminate the particular exposure or vulnerability in your environment. Keep track of any customizations that you create.

Values for these attributes in the FILECHG and REGCHG instances will override the value in a connection OPTIONS instance. If these variables are blank in the FILECHG and REGCHG instances, then the value from the connected OPTIONS class will be used. If the patch descriptor xml file does not contain these attributes, then the values from the connected OPTIONS instance will be used.

To customize reporting options

For the purpose of this exercise, assume that all changes are to the OPTIONS Class. Connect instances of the OPTIONS Class to the file or registry component that you want to customize reporting for.

1. In the USE attribute in the appropriate class (or in the patch descriptor file), specify what properties of the file or registry key you want to evaluate. For example, if you were only interested in the date of a file, set USE to GMTDATE.
2. Set DesiredState (DSTATE) by equating a state with a return code. Separate multiple conditions with commas. Use the appropriate state from the list below.
   - Use state E (exists) if your only criterion for status is the existence of the file or registry key.
   - Use state !E (does not exist) if your only criterion for status is whether the file or registry key does not exist.
   - Use state EQ (equal) if the file or registry key meets the exact criteria.
   - Use state !EQ (not equal) if the file or registry key does not meets at least one of the criteria.

— Use state LT (less than) if the file or registry key is less than at least one of the criteria.

— Use state GT (greater than) if the file or registry key is greater than at least one of the criteria.

Use the appropriate return code from the list below.

— Use 0 to represent a status of OK.

— Use 4 to represent a warning status.

— Use 8 to represent an error status.

Rules for Valid DSTATE Values

— At least one of the conditions should have a return code of 0 (OK), but you could have more than one condition return a non-zero value (4, 8).

— Testing for Equality (EQ) implies that the component should exist and need not be expressed in the DSTATE variable.

The samples below show an example of a customized option for a file option. The criteria specified in the Use tag are VERSION, GMTDATE, and SIZE. The DesiredState tag describes to:

— Return a status of OK if the file does not exist (!E=0).

— Return a Warning status if the VERSION, GMTDATE or SIZE of the file are greater than the patched file (GT=4).

— Return an Error status if the VERSION, GMTDATE or SIZE of the file is less than the patched file (LT=8).

```
<FileChg Name="snmpsfx.dll" CRC32="" Gmttime=""
Path="%windir%\system32" Size="" Checksum="14922"
Gmtdate="19990212" Version="4.0.1381.164"
DesiredState="!E=0,GT=4,LT=8" ReportThreshold="1"
Use="VERSION,GMTDATE,SIZE" />
```

The values in the XML file are entirely surrounded by quotes.

3 Set a REPORT threshold. The properties of the file or registry key will be sent to the Patch Manager based on this value. If the return code is greater than or equal to the value of the REPORT attribute, the file and

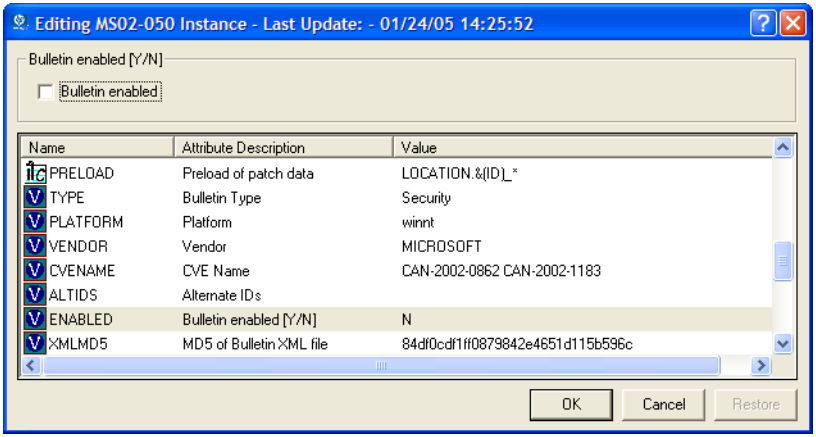
registry information will be sent to the Patch Manager and will be available in Patch Manager reports. For example, set REPORT to 1 to send the properties if the return code is either 4 (Warning) or 8 (Error).

The changes will take effect the next time you publish the patch descriptor file to the Configuration Server Database.

Disabling Vulnerability Detection and Deployment

You can disable the detection or deployment of a bulletin or patch. To do this, use the Admin CSDB Editor to set the ENABLED attribute to **N** in the Bulletin or Patch instance in the PATCHMGR Domain.

Figure 18 Disable detection of Bulletin MS00-001



If you want to disable all patches for a particular bulletin, set the ENABLED attribute to **N** in the bulletin's instance. If you want to disable only a specific patch file's detection and deployment, set the ENABLED attribute in the patch file's instance.

Controlling Patch Deployment (PATCHARG)

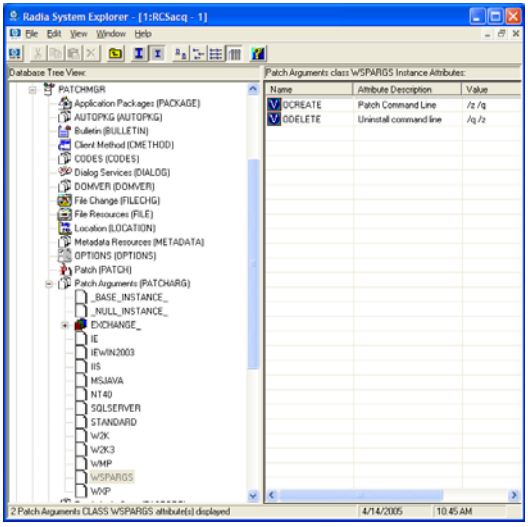
For each patch file, Patch Manager populates the parameters for installing and, where possible, for removing the patch. These parameters can be found in the Patch Command Line (OCREATE) and the Uninstall Command Line (ODELETE) attributes in the PATCHARGS class in the PATCHMGR Domain.

PATCHARG options apply only to patches downloaded using MSSECURE.XML not Microsoft Update. When patches are acquired from Microsoft Update, the Source column in the report will show "Microsoft Update" instead of "Microsoft."

You can change the command-line parameters for installing and uninstalling the patch file. To do this, use the PATCHARG class to create an instance and connect it to the appropriate patch file.

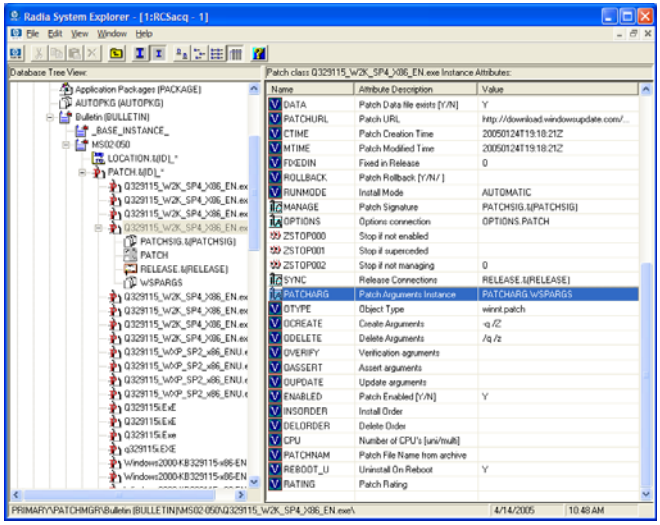
To create alternate command line parameters using PATCHARG

1. Use the Admin CSDB Editor to navigate to the PATCHARG Class in the PATCHMGR Domain.
2. Right-click **PATCHARG** and create a new instance. A new instance called WSPARGS has been created in the following figure.



3 Type the new parameters that you want to use. There are two attributes in the PATCHARG Class: OCREATE to install the patch, and ODELETE to remove the patch.

4 Type the path to the PATCHARG Instance in place of the PATCHARG Attribute for the patch file in the BULLETIN Class.



The parameters you created will be used for this patch file.

Preloading Client Automation Proxy Servers

If you are using a Client Automation Proxy Server you may want to preload the patch files. To do this, go to your preload user instance (the default for Proxy Server is **RPS**) in the POLICY Domain. If you do not already have a preload user instance, create one. You must add connections to the DISCOVER_PATCH service and the services for the bulletins to download. At the end of the bulletin you want to download put a suffix of **`(PRELOAD)`**. For example, to preload only the MS03-039 bulletin, add a connection to **PATCHMGR.ZSERVICE.MS03-039(PRELOAD)**. You can use wild cards in the bulletin name. If you want to preload all bulletins beginning with MS03, type **`PATCHMGR.ZSERVICE.MS03-*(PRELOAD)`** in the connection instance.

The next time you run a preload, the Proxy Server will load the compressed data files from the PATCHMGR Domain. For more information on preloading, refer to the *HP Client Automation Proxy Server Installation and Configuration Guide* (*Proxy Server Guide*).

Removing a Patch

By default, if you disconnect a user from a Microsoft vulnerability service (ZSERVICE) instance, the patch that was installed is not removed. This behavior is controlled in the ZDELETE attribute of the MANAGE instance in the Client Method (CMETHOD) class, and is disabled by default.

Both Red Hat Security Advisory and SuSE Security Advisory removal is disabled deliberately in Patch Manager. When a Linux vendor supplied patch is applied to a target system, the affected Linux software is updated to the current rpm package version and release that addresses the specific security vulnerability. Application of a Linux vendor supplied advisory (patch) does not maintain a backup of the original package, making automated rollback to a prior version impossible. An attempt to remove a Linux rpm package from a device would result in the removal of the patch as well as the rpm software package to which the patch applies. If a new vulnerability is found, Linux Security patch vendors release a new patch. This is the nature of Red Hat and SuSE Security Advisories as provided by these patch vendors.

For Microsoft patches, if you want the patch files removed when you remove a user from vulnerability management, edit the ZDELETE attribute.

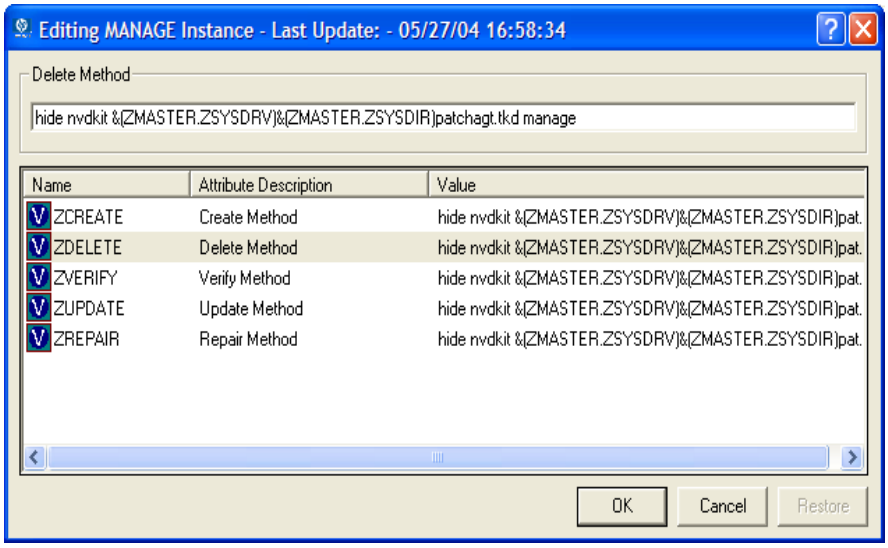
Modifying the PATCHMGR.CMETHOD.MANAGE.ZDELETE method will remove *all* patches for *all* users if the user is no longer assigned the vulnerability.

See Removing a Patch on page 141 for additional information.

To remove a patch when a user is no longer assigned the service

1. Use the Admin CSDB Editor to navigate to the MANAGE Instance of the Client Method (CMETHOD) Class in the PATCHMGR Domain.
2. Double-click the ZDELETE Attribute in the tree view, and in the text box, type:

```
hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)
patchagt.tkd manage
```



3 Click **OK** to change the instance. The Instance Edit Confirmation opens.

4 Click **Yes** to confirm the changes.

The Patch Manager Agent must make a connect in order for the managed device to receive the necessary configuration change to allow the removal of patches.

The next time you disconnect a user from a ZSERVICE Instance in the PATCHMGR Domain, the patch files will be removed.

Summary

- Install the Patch Manager Agent on devices that you want to manage.
- Patch Manager supplies you with research, patch acquisition, and vulnerability reports.
- Use the reports to identify vulnerabilities in your enterprise.
- Manage vulnerabilities by assigning the patch's service to your devices.

A Supported XML Tags for Patch

Descriptor Files

The patch descriptor files from HP contain information about Products, Releases, Patches, and Patch Manifests. These are shown in tables following Figure 19 on page 145.

If you are creating custom patch descriptor files, use the tags that are supported. The node hierarchy of a patch descriptor file is shown in the figure below.

Figure 19 View a sample patch descriptor file.


```
- <Bulletin PopularitySeverityID="0" Type="Security"
    URL="http://www.microsoft.com/technet/security/bulletin"
    FAQURL="http://www.microsoft.com/technet/security/bulletin" MitigationSeverityID="0"
    Vendor="MICROSOFT" Supported="Yes" ImpactSeverityID="0" SchemaVersion="1.0" PreReqSeverityID="0"
    DateRevised="20030120" Source="MICROSOFT" Name="MS03-001" Title="Unchecked Buffer in Locator
    Service Could Lead to Code Execution (810833)" DatePosted="20030120" Platform="winnt">
  - <Products>
    - <Product Name="Windows 2000 Advanced Server" FixedInRelease="Windows 2000 Service Pack 4">
      - <Releases>
        - <Release Name="Windows 2000 Service Pack 2">
          + <Patch VerifyCmdline=""
              PatchURL="http://download.windowsupdate.com/msdownload/update/v3-
              19990518/cabpool/Q810833_W2K_SP4_7BCAD659FA326D4979A3CE9034300EA83A30F5I
              Architecture="" Reboot="Y" InstallCmdline="-q /Z" Language="en"
              MSSUSName="com_microsoft.810833_W2K_SP4_5936" SupercededByBulletin=""
              SupercededByMSPatch="" OSVersion=""
              MSSecureName="Q810833_W2K_SP4_X86_EN.exe" ObjectType="winnt.patch"
              QNumber="810833" ProbeCmdline="" Superceded="N" OSType="" OSSuite=""
              Platform="winnt" UninstallCmdline="">
```


Bulletin Node

Node name:Bulletin

Parent node:None

Children:Products

Table 5 XML Tags in the BULLETIN class

XML Tag	HPCA Attribute	Description
PopularitySeverityID	POPULAR	Popularity ID Source: `MSSECURE.XML`
URL	URL	Bulletin URL Source: `MSSECURE.XML`
FAQURL	FAQURL	Frequently Asked Questions (FAQ) URL Source: `MSSECURE.XML`
Supported	SUPPORT	Supported [Y/N] Source: `MSSECURE.XML`
ImpactSeverityID	IMPACT	ImpactID Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
MitigateSeverityID	MITIGATE	Mitigate ID Source: `MSSECURE.XML`
PreReqSeverityID	PREREQ	Prereq ID Source: `MSSECURE.XML`
DateRevised	REVISED	Bulletin Revised On Date the bulletin was revised in YYYYMMDD format. Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds

Table 5 XML Tags in the BULLETIN class

XML Tag	HPCA Attribute	Description
Source	SOURCE	Source [MICROSOFT | NOVADIGM | CUSTOM | REDHAT | SUSE] Directory from which the patch descriptor file was published.
Vendor	VENDOR	MICROSOFT/REDHAT/SUSE
Type	TYPE	Type of Bulletin Security/ServicePack/Other
Platform	PLATFORM	winnt//redhat/suse
Name	NAME	External ID Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
Title	TITLE	Title Bulletin title. Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
DatePosted	POSTED	Bulletin Posted On Date the bulletin was posted in YYYYMMDD format. Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
Schema Version		The patch schema version currently 1.0
	MTIME	Time the instance was modified in the CSDB.

Table 5 XML Tags in the BULLETIN class

XML Tag	HPCA Attribute	Description
	CTIME	Time the instance was created in the CSDB.
	ID	Internal instance ID.
HPPosted	HPPOSTED	Date the bulletin was initially posted by HP.
HPRevised	HPREVISD	Date the bulletin was revised by HP.
Deployment	RUNMODE	Specifies whether the patch can be installed automatically (AUTOMATIC) or needs user interaction (INTERACTIVE).

Products Node

Node name:Products

Parent node:Bulletin

Children:Product

Attributes:None

Product Node

Node name:Product

Parent node:Products

Children:Releases

Table 6 XML Tags in the PRODUCT class

XML Tag	HPCA Attribute	Description
Name	NAME	Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
Name	NAME	Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds

Releases Node

Node name:Releases

Parent node:Product

Children:Release

Attributes:None

Release Node

Node name:Release

Parent node:Releases

Children:Patch

Table 7 XML Tags in the RELEASE class

XML Tag	HPCA Attribute	Description
Name	NAME	Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds

Patch Node

Node name:Patch

Parent node:Release

Children:Package

Table 8 XML Tags in the PATCH class

XML Tag	HPCA Attribute	Description
PatchURL	PATCHURL	A URL that points to an .EXE or .MSI file. Source: `MSSECURE.XML/SUS`, Red Hat Network, Novell (SuSE) data feeds
Reboot	REBOOT	Specified if the device should be rebooted, after the patch is installed. Source: `MSSECURE.XML/SUS`, Red Hat Network, Novell (SuSE) data feeds
Architecture	ARCH	x86|i64 Source: `MSSECURE.XML/SUS`, Red Hat Network, Novell (SuSE) data feeds
Language	LANG	en,fr,de Source: SUS
MSSUSName	SUSNAME	The SUS name for the patch from `MSSECURE.XML`. Source: `MSSECURE.XML`

Table 8 XML Tags in the PATCH class

XML Tag	HPCA Attribute	Description
SupercededByBulletin	SUPERBU	The bulletin name that supersedes this patch. Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
SupercededByMSPatch	SUPERMSS	The MSSECURE patch name that supersedes this patch. Source: `MSSECURE.XML`
Superceded	SUPERCED	Specifies if the patch has been superseded. Valid values are Y or N. Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
MSSecureName	MSSNAME	The MSSECURE name for this patch. Source: `MSSECURE.XML`
OSVersion	OSVER	Operating System Version
QNumber	QNUMBER	QNUMBER for the patch from `MSSECURE.XML`. Source: `MSSECURE.XML`
OSType	OSTYPE	The operating system type, such as server or workstation.
OSSuite	OSSUITE	The operating system suite, e.g., datacenter, blade.
Platform	PLATFORM	The platform type: winnt, redhat, suse

Table 8 XML Tags in the PATCH class

XML Tag	HPCA Attribute	Description
InstallCmdline	OCREATE	This is the arguments that are passed to the create procedure. Source: SUS, Red Hat Network, Novell (SuSE) data feeds
VerifyCmdline	OVERIFY	The Verify Arguments.
UninstallCmdline	ODELETE	The Uninstall Arguments.
ObjectType	OTYPE	Format: namespace=script filename Default: winnt.patch This specifies the type of the object and the name of the script file that would have the following procedures defined verify create delete assert The procedures should have the namespace as part of the name, e.g., winnt.patch::create. If the script filename is not specified then the filename is {namespace}.tcl. Source: Novadigm
ProbeCmdline	OVERIFY	The probe command line. Source: Novadigm
	ID	The unique ID created in the HPCA-CSDB for this patch.

Table 8 XML Tags in the PATCH class

XML Tag	HPCA Attribute	Description
	PATCHSIG	The name of the Patch Signature instance. Source: Novadigm
	LOCATION	The name of the LOCATION instance that contains the patch data.
	BULLETIN	The bulletin name set during publishing. Source: `MSSECURE.XML`, Red Hat Network, Novell (SuSE) data feeds
	DATA	Does the RCS have the patch data [Y/N] filled in during publishing. If the RCS has the data the value would be Y else it would be N.
	DSTATE	Desired state for a patch, this is usually classed in from an instance. Source: Novadigm
	REPORT	Report threshold, similar to DSTATE is classed in from an instance. Source: Novadigm
	USE	The variables used in checking the desired state. Source: Novadigm
Deployment	RUNMODE	Specifies whether the patch can be installed automatically (AUTOMATIC) or needs user interaction (INTERACTIVE).

Patch Signature Node

Node name: PatchSignature

Parent node:Patch

Children:FileChg, RegChg

Attributes:None

FileChg Node

Node name:FileChg

Parent node:PatchSignature

Chidren:None

Table 9 XML Tags in the FILECHG class

XML Tag	HPCA Attribute	Description
Name	NAME	File name. Source: `MSSECURE.XML`
Path	PATH	The directory name, this can contain environment variables, e.g., `%windir%`, and is used by the appropriate scripts for Windows and Linux. Source: `MSSECURE.XML`
CRC32	CRC32	The CRC of the data.
Gmttime	GMTTIME	The GMTDATE expressed as YYYYMMDD. Source: `MSSECURE.XML`
Gmtdate	GMTDATE	The GMTTIME expressed as HH:MM:SS. Source: `MSSECURE.XML`

Table 9 XML Tags in the FILECHG class

XML Tag	HPCA Attribute	Description
Size	SIZE	The size of the file. Source: `MSSECURE.XML`
Checksum	CHECKSUM	The checksum of the file. Source: `MSSECURE.XML`
Version	VERSION	The version of the file. Source: `MSSECURE.XML`
	DSTATE	The desired state of the FILECHG instance, this is usually classed in from another instance in the CSDB. Source: Novadigm
	REPORT	The report threshold. If on evaluation of this file change instance the RC is greater than the threshold then we will create a ZOBJSTAT for that instance. Source: Novadigm
	USE	The variables to use during comparison, e.g., Version,Checksum,Gmtdate. Source: Novadigm

RegChg Node

Node name:RegChg

Parent node:PatchSignature

Children:None

Table 10 XML Tags in the REGCHG class

XML Tag	HPCA Attribute	Description
Name	NAME	Value Name. Source: `MSSECURE.XML`
Path	PATH	The fully qualified Registry Key Name. Source: `MSSECURE.XML`
Value	VALUE	The Data value stored in the registry. Source: `MSSECURE.XML`
Type	TYPE	Registry data type should be one of the following: sz = Simple Registry String multi_sz = Registry Multi String expand_sz = Registry string with environment variables dword = Registry dword binary = Binary data Source: `MSSECURE.XML`
	DSTATE	Desired state of FILECHG instance, this is usually classed in from another instance in the RCS database. Source: Novadigm

Table 10 XML Tags in the REGCHG class

XML Tag	HPCA Attribute	Description
	REPORT	Report threshold. If on evaluation of this file change instance, the RC is greater than the threshold then we will create a ZOBJSTAT for that instance. Source: Novadigm
Type	TYPE	Registry data type should be one of the following: sz = Simple Registry String multi_sz = Registry Multi String expand_sz = Registry string with environment variables dword = Registry dword binary = Binary data Source: `MSSECURE.XML`
	DSTATE	Desired state of FILECHG instance, this is usually classed in from another instance in the RCS database. Source: Novadigm

HPFileset Node

Node name:HPFileset

Parent node:PatchSignature

Children:None

Table 11 XML Tags in the HPFSET class

XML Tag	HPCA Attribute	Description
Name	NAME	Fileset Name
Version	VERSION	Fileset Version

B Restarting the Managed Device

You may need to restart a managed device based on an application event. To do this, specify a reboot type and reboot modifiers in the ZSERVICE.REBOOT attribute. The modifiers allow you to:

- set the type of warning message
- handle a reboot with either a machine or user connect
- and cause an immediate restart after the application event.

Application Events

First, specify the application event that needs the reboot. Set the application event code to a reboot type and any reboot modifier that you need to use. The sections below describe each type of reboot and all reboot modifiers.

If the hreboot parameter is missing from the radskman command line, the parameter defaults to Y to handle service reboot requests. If you set hreboot to p, the managed device will *power down*, regardless of whether or not there is a service requiring a reboot.

If you need an application to immediately perform a hard reboot with no warning messages on application installation and repair, set the ZSERVICE.REBOOT variable to AI=HQI, AR=HQI.

If you wish to alter reboot panel behaviors based solely upon the requirements of a patch, as supplied by the vendor, use the AL event, to trigger the reboot event for locked files. The versioning event (VA) is not applicable in Patch Manager.

- Use AI to specify a reboot behavior for application installations. The default is no reboot.

- Use AD to specify a reboot behavior for application removals. The default is no reboot.
- Use AL to specify a reboot behavior when a locked file is encountered. The default behavior when a locked file is encountered is to perform a Hard reboot with just an OK button (HY).
- Use AU to specify a reboot behavior for application updates. The default is no reboot.
- Use AR to specify a reboot behavior for application repairs. The default is no reboot.
- Use AV to specify a reboot behavior for application version activations. The default is no reboot.

Reboot Types

After deciding which application events need a computer reboot, you will need to choose the type of reboot. Client Automation sends a message to the operating system that the computer needs to reboot. There are three types of reboot.

- **Hard Reboot (H)**

  All applications are shut down regardless of whether there are open, unsaved files or not. The subscriber will not be prompted to save open, modified files.

- **Soft Reboot (S)**

  Users are prompted to save their data if applications have open, unsaved files. If applications have unsaved data, the reboot will wait for the user to respond to the application's request for the user to save his data.

- **No Reboot (N) (default reboot type)**

  The computer will not restart after completing the specified application event. This is the default reboot type for all application events except a Locked File Event (AL). If you specify AL=N, then the managed device will not perform a hard reboot with OK and Cancel buttons when a locked file is encountered. If no restart type is specified for an application event, no restart will occur.

Reboot Modifier: Type of Warning Message

You can specify the type of warning message you want to send to the subscriber before the restart occurs. If you specify a type of reboot, but do not specify a type of warning message, the default warning message for that type will be displayed. There are three types of warning messages. Warning messages are displayed automatically for the Application Self-service Manager and for Application Manager used with the Client Automation System Tray. If you do not want to show a warning message, specify ask=N in a radskman command line.

The Application Manager for Linux does not display reboot panels.

- **Quiet (Q)**

  No reboot panel will be displayed.

- **OK Button (A)**

  A warning message will display with an OK button only. Click OK to initiate the reboot. The user will not be able to cancel the restart.

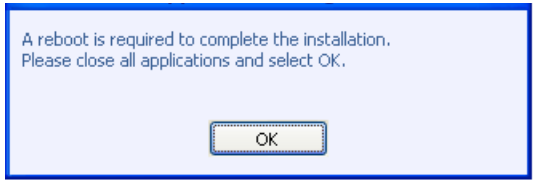
- **OK and Cancel Button (Y)**

  Click the OK button to initiate a reboot. If the subscriber clicks Cancel, the reboot will be aborted.

  You can specify a timeout value for the Warning Message box by adding the RTIMEOUT value to the radskman command line. Set RTIMEOUT to the number of seconds you want the managed device to wait before continuing with the reboot process.

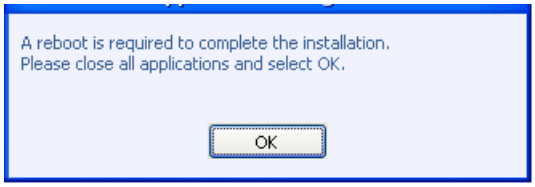
For example, the default Reboot panel displays both an OK and Cancel as shown in the figure below.

Figure 20 View the default reboot



If would like to suppress the Cancel button on the agent reboot panel, specify a ZSERVICE.REBOOT attribute of: AL=SA which would display the dialog box shown in the figure below. Use this if the vendor-supplied patch mandates a reboot to complete the Patch installation.

Figure 21 Change the reboot panel to show only the OK button



Reboot Modifier: Machine and User Options

The managed device can connect as a machine or as a user by specifying the context parameter on the radskman command line. Use the Machine/User reboot modifier to specify if the reboot should complete based on the type of connect.

Patch Manager Agent connects occur in the machine context.

- **Reboot on Machine connect (blank)**
  When a machine/user reboot modifier is not supplied, the default behavior will be to reboot only on a machine connect where context=m in radskman, or if the context parameter is not specified. This default behavior should satisfy the majority of reboot requirements.
- **Reboot on User connect only (U)**
  The reboot will be honored on a user connect only where context=u in radskman or if the context parameter is not specified. The reboot will NOT occur where context=m in radskman.
- **Reboot on both Machine and User connect (MU)**
  Reboot will only occur when both the machine and user components of the application are installed.

Reboot Modifier: Immediate Restart

You can modify each type of reboot by adding I for Immediate. Use Immediate when you want the computer to restart immediately after resolving the current service. Client Automation will resolve the rest of the subscriber's services after the computer restarts. If you specify I, but do not specify H or S as the type of reboot, a hard reboot will be performed.

Specifying Multiple Reboot Events

If you have two services that require a reboot event on the same Agent Connect, the most restrictive reboot type and reboot panel will be used. The least restrictive reboot type is No Reboot (N), followed by Soft Reboot (S), and the most restrictive is Hard Reboot (H). The least restrictive reboot warning message supplies both OK and Cancel buttons (Y), followed by an OK button only (A), and the most restrictive is completely quiet (Q).

Suppose a subscriber is assigned an application that needs a soft reboot with just an OK button on installation, AI=SA. The subscriber is also assigned a second application that needs a hard reboot that displays both an OK and Cancel button, AI=HY. After all of the subscriber's application events are completed, a Hard Reboot (H) with only an OK button displayed (A) will be performed

C Policy Server Integration

If you are using the HP Client Automation Policy Server (Policy Server) to create entitlements in your enterprise, you can filter out which domains the Policy Server will assign services from based on connect parameters.

If you are using Policy Server with Patch Manager, you should separate the resolution of regular software services from those for Patch Manager. Policy Server filters services based on the dname passed on the radskman command line.

The Policy Server configuration file, `pm.cfg`, contains filter settings in the format:

```
DNAME=<DOMAIN NAME>  { rule }
```

Where the DOMAIN NAME is the value passed in dname by RADISH. In the case of a Patch Manager Agent, this will be the dname parameter of radskman. Dname should be "patch". If the filter name passed in dname is not found in `pm.cfg`, then the filter `DNAME=*` will be used. The minimum version requirement for Policy Server is version 5.0.

The default configuration for these filters is shown in the figure below:

```
DNAME=*       { * !PATCHMGR !OS }

DNAME=PATCH   { PATCHMGR }

DNAME=OS      { OS }
```

In this configuration the default rule (*) will ignore PATCHMGR and OS domains and allow everything else. The "!" denotes the named domain is to be ignored. The PATCH and OS rules allow only policies for PATCH and OS domains respectively. If, for instance, we wanted to allow any policies for OS manager resolution we would change the last filter to: `DNAME=OS { * }`.

D Patch.cfg Parameters

This appendix describes all of the possible parameters in the Patch Manager Server configuration file, `patch.cfg`. Wherever possible these parameters should be edited using the Patch Manager Administrator. This list is provided as supporting information.

Patch Manager Server Configuration Parameters

HP recommends that you configure the Patch Manager parameters in the Patch Manager Administrator. If you cannot use the Patch Manager Administrator, you can make changes directly in the `patch.cfg` file. The default location is *`Drive`*`:\Program Files\Hewlett-Packard\CM\PatchManager\etc`. The parameters are listed in this appendix.

If you are migrating from a previous version of Patch Manager, your old values in `patch.cfg` will be retained. Be aware that you will not get the new available parameters in your old `patch.cfg`, nor will you get the new default values for old parameters.

- **admin_date_fmt**: Specify the date and time format for the Patch Manager Administrator. The default is {%Y-%m-%d %H:%M:%S} where %Y is the year with century, %m is the month number, %d is the day of the month, %H is the hour in 24-hour format, %M is the minute, and %S is the seconds.
- **data_dir**: Specify the directory on the local computer (Patch Manager Server) where you want the patches downloaded to before they are sent to your Configuration Server. Use this parameter to set where to store your patch descriptor files and patch data files in an alternate directory. If you choose to perform an acquisition using a directory that is pre-populated

with data from a previous acquisition, specify a different directory in this parameter. The default is *Drive*:\Program Files\Hewlett-Packard\CM\PatchManager\data\patch.

- **db_type**: Specify the database type. The two possible values are **mssql** for Microsoft SQL Server (the default) and **oracle** for Oracle. If you are using Oracle, change this value to **oracle** before doing a patch acquisition or a database synchronization. This parameter is required to synchronize with an Oracle database.
- **dsn**: Specify the **Data Source Name** (**DSN**) the Patch SQL database. This parameter is required.
- **dsn_user**: Specify the SQL user for the DSN for the Patch SQL database.
- **dsn_pass**: Specify the password for the SQL user for the DSN for the Patch SQL database.
- **ftp_proxy_pass**: If you use a proxy server for FTP traffic, specify your password.
- **ftp_proxy_url**: If you use a proxy server for FTP traffic, specify its URL in the format f**tp://ip:port**. At the time of this writing, Patch Manager supports basic authentication only.
- **ftp_proxy_user**: If you use a proxy server for FTP traffic, specify your user ID.
- **history**: Specify how many days to keep the Patch Auth Store (PASTORE) instances. This class contains one instance for each patch acquisition session. HP recommends specifying this in the `patch.cfg` file, not on the command line. If history has a smaller value than purge_errors, then purge_errors will be set to the value for history. The default of 0 means never delete any history of Patch Acquisition.
- **http_proxy_pass**: If you use a proxy server for HTTP traffic, specify your password.
- **http_proxy_url**: If you use a proxy server for HTTP traffic, specify its URL in the format **http://ip:port**. At the time of this writing, Patch Manager supports basic authentication only.
- **http_proxy_user**: If you use a proxy server for HTTP traffic, specify your user ID.
- **http_timeout**: Set the total amount of time to wait for the file to be completely downloaded. If the acquisition session is unable to download the file in this time, then the acquisition will abort the current HTTP

location, and will continue the acquisition with the next HTTP location. Increase the http_timeout if you need to allow additional time for a bulletin to download.

This parameter is expressed in seconds in the `setup.tsp` page. Specify http_timeout in either the `patch.cfg` file or on the command line in milliseconds. This is reflected in `patch.cfg` as 3600000. If you specify http_timeout on the command line, it will be for this acquisition session only.

- **lang**: Patch Manager supports non-double byte languages. Specify the abbreviation of the languages for which you want to acquire patches. Precede any products you want excluded with an exclamation point (**!**). The default is en (English). If you wanted to include French and English, specify, **`- lang fr, en`**.
- **microsoft_sus_url**: Specify the URL for the Microsoft SUS feed. The default is **http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab**.
- **microsoft_url**: Specify the URL for the Microsoft `MSSECURE.XML` file. The default is **http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB**.
- **nvdm_url**: Specify the URL to connect to the Patch Update web site provided by HP. This is the same as the nvdm_url parameter in `patch.cfg`. The default is **http://managementsoftware.hp.com/Radia/patch_management/data**.
- **purge_errors**: Specify how many days to keep the Publisher Error (PUBERROR) instances. This class contains one instance for each patch acquisition error. HP recommends specifying this in the `patch.cfg` file, not on the command line. If history has a smaller value than purge_errors, purge_errors will be set to the value for history. The default is 7.
- **rcs_pass**: If authentication has been enabled on your Configuration Server, specify the password for the rcs_user.
- **rcs_url**: Specify the location of your Configuration Server in URL format. This parameter is required. Use the format **`radia://`***`ipaddress`***`:`***`port`**, where:
  - **`radia`** indicates the session type to be opened to the Configuration Server

- *ipaddress* is the hostname or IP address of the computer hosting the Configuration Server
- *port* is the port number of the Configuration Server.

- **rcs_user**: If authentication has been enabled on your Configuration Server, specify the rcs_user.
- **reporting_url**: Specifies the URL of your Reporting Server. The default is **http://localhost/reportingserver**.
- **retire**: Specify the bulletins to retire separated by commas. Use the -retire parameter to:
  - Delete specified bulletins if they exist in the Configuration Server database during the current publishing session.
  - Not publish the bulletins specified in the retire parameter to the Configuration Server database during the current publishing session. The use of the retire option supersedes the bulletins option.

  This parameter works on the bulletin level, not at the product or release level.

  To only retire a specific bulletin, but not acquire any new ones, use **-bulletin NONE** in addition to the retire parameter.

  Note the following:
  - The only time the **retire** option should be used on the command line is to delete specific bulletins from the Configuration Server Database. However, it does not keep a cumulative list of retired bulletins if you specify the option on the command line.
  - It is recommended that you set a retired bulletin list in the `patch.cfg` so a cumulative list is maintained. As needed, add to the list in `patch.cfg` instead of recreating the list of retired bulletins on the command line each time you want to retire a new one.
  - If you have enabled patch-removal capabilities, and retire bulletins that are currently under management in your enterprise, the retired security patches may be removed from your Patch Manager Agent devices.

  Example: **-retire MS00-001,MS00-029**
- **rh_depends**: Specify **yes** if you want to publish additional Red Hat packages that downloaded security advisories may depend on. You can override this setting for a specific acquisition in Acquisition Settings.

Prerequisite, or dependent, Red Hat packages required to install Red Hat Security Advisories can be acquired from two places. They can either be downloaded from the Red Hat Network during acquisition or they can be found locally if copied from the Red Hat Linux installation media. During an acquisition, Patch Manager will first look for the `.rpm` packages in the appropriate directory. For example:

- For Red Hat Enterprise Linux 4ES on x86 devices, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/4es`.
- For Red Hat Enterprise Linux 4ES on x86-64 devices, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/4es-x86_64`.
- When naming the `data/patch/redhat/packages/` subdirectories, refer to the list of **OS Filter Architecture** values listed in Red Hat Feed Settings on page 25. Use the applicable value following `REDHAT::` as the subdirectory name.

If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, HP recommends copying the dependency packages to the appropriate packages directory from your Linux installation media. The Red Hat RPM packages can be found on the installation media under the `RedHat/RPMS` directory.

The default is No.

- **rhn_url**: Specify the URL for the Red Hat Security Network. The default is **http://xmlrpc.rhn.redhat.com/XMLRPC**.
- **suse_pass**: :Specify the password for the Novell web site that is hosting SuSE 9 patches.
- **suse_urls**: :Specify the URLs for the Novell web site that is hosting SuSE patches. The defaults are:

  9:

  {**https://you.novell.com/update/i386/update/SUSE-CORE/9/**}

  {**https://you.novell.com/update/i386/update/SUSE-SLES/9/**}

  9-x86_64:

  {**https://you.novell.com/update/x86_64/update/SUSE-CORE/9/**}

  {**https://you.novell.com/update/x86_64/update/SUSE-SLES/9/**}

- **suse_user**: Specify the user for the Novell web site that is hosting SuSE 9 security patches.
- **suse10_pass**: Specify the password for the Novell web site that is hosting SuSE 10 and 11 patches.
- **suse10_urls**: Specify the URLs for the Novell web site that is hosting SuSE 10 and 11 patches. The defaults are:

  10:

  {https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-i586}

  {https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-i586}

  10SP1:

  {**https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-i586**}

  {**https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-i586**}

  10SP2:

  {https://nu.novell.com/repo/$RCE/SLES10-SP2-Updates/sles-10-i586}

  {https://nu.novell.com/repo/$RCE/SLED10-SP2-Updates/sled-10-i586}

  10-x86_64:

  {https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-x86_64}

  {https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-x86_64}

  10SP1-x86_64:

  {https://nu.novell.com/repo/$RCE/SLES10-SP1-Updates/sles-10-x86_64}

  {https://nu.novell.com/repo/$RCE/SLED10-SP1-Updates/sled-10-x86_64}

  10SP2-x86_64:

  {https://nu.novell.com/repo/$RCE/SLES10-SP2-Updates/sles-10-x86_64}

  {https://nu.novell.com/repo/$RCE/SLED10-SP2-Updates/sled-10-x86_64}

11:

https://nu.novell.com/repo/$RCE/SLES11-Updates/sle-11-i586/
https://nu.novell.com/repo/$RCE/SLED11-Updates/sle-11-i586/

11-x86_64:

https://nu.novell.com/repo/$RCE/SLES11-Updates/sle-11-x86_64/
https://nu.novell.com/repo/$RCE/SLED11-Updates/sle-11-x86_64/

- **suse10_user**: Specify the user for the Novell web site that is hosting SuSE 10 and 11 security patches.
- **sync**: Specify the targets that need to be synchronized. The default is rcs.

Patch Acquisition Parameters

To acquire patches from a command line

1 From a command prompt on your Patch Manager Server, navigate to the Patch Manager directory. The default location is

System Drive:`\Program Files\Hewlett-Packard\CM\PatchManager`

You can also use the acquisition file you created from a command line. To do this, use the config parameter.

2 Using the parameters listed in the bulleted list below, create a command line similar to the following:

```
nvdkit ./modules/patch.tkd acquire -bulletins MS04-*
```

where you want to acquire the patch files for only bulletins from the Microsoft web site matching a filter of MS04-*.

Parameters specified on the command line overwrite those specified in `patch.cfg`. Use `patch.cfg` for default parameters.

- **arch**: Specify the computer architecture for which you want to acquire patches separated by a comma. Valid values for the arch parameters are given in the Vendor Feed Settings in Chapter 2, Creating the Patch Manager Environment.

- **bulletins**: Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. This is the same as the bulletins parameter in `patch.cfg`. For Red Hat Security advisories, use a hyphen (-) in place of the colon (:) that appears in the Red Hat Security advisory number as issued by Red Hat.

  — Microsoft Security bulletins use the naming convention `MS`*`YY`*`-###`, where *`YY`* is the last two digits of the year that the bulletin was issued and `###` is a sequential number of the bulletin number being released for this the year specified. Microsoft service packs are listed in the format `MSSP_`*`operatingsystem_spnumber`*. To acquire *sample* Microsoft Operating System service packs, specify MSSP*. This will download sample service packs using information in the `novadigm` or `custom` folders. For example, specify -bulletins MS00-001,MS00-029.

  — Red Hat Security advisories are issued using the naming convention `RHSA-`*`CCYY`*`:###`, where *`CC`* indicates the century and *`YY`* the last to digits of the year when the advisory was issued, and `###` the Red Hat patch number. However, because the colon is a reserved character in Client Automation products, you must use a hyphen (`-`) in place of the colon (:) that appears in a Red Hat-issued Security advisory. Specify individual Red Hat Security advisories to Patch Manager using the modified naming convention of `RHSA-`*`CCYY`*`-###`.

  — SuSE Security patches use the naming convention `SUSE-PATCH-####`, where `###` represents a numbering scheme provided by SuSE.

  If you do not want to download any bulletins, use –bulletins NONE. You may want to do this when you want to only acquire agent updates.

- **config**: Use this parameter to append an alternate configuration file for acquisition to override settings in `patch.cfg`. The default is `patch.cfg`.

- **data_dir**: Specify the directory on the local computer (Patch Manager Server) where you want the patches downloaded to before they are sent to your Configuration Server. Use this parameter to set where to store your patch descriptor files and patch data files in an alternate directory. The default is: *`Drive`*`:\Program Files\Hewlett-Packard\CM\PatchManager\data\patch`.

- **force**: Use force in the following situations.

  — You previously ran an acquisition using the mode MODEL, and now you want to use BOTH.

— You previously ran an acquisition filtering for one language (lang), and now, you need to acquire bulletins for another.

— You previously ran an acquisition specifying one product, and, now, you need to acquire for another.

For example, suppose that originally you only had Windows 2000 computers in your enterprise, so you used -product {Windows 2000*}. A month later, you roll out Windows XP. If you want to acquire the same bulletins, you will need to run the acquisition with -product {Windows XP*,Windows 2000*} and -force y.

The default is N. If replace is set to Y, the bulletins will be removed and reacquired, regardless of the value of force.

- **mode**: Specify BOTH to download patches and the information about the patches. Specify MODEL to acquire only the metadata for patches. Only the Bulletins and Numbers for the patches are downloaded, but not the actual patch files. Use this mode so that you can use the reports to expose vulnerabilities on Agent devices. BOTH is the default.

- **product**: Specify which products you want to include in the acquisition in the format of *vendor*::*product* in a comma separated list. Precede any products you want excluded with an exclamation point (!). If an include filter is not set, all products are assumed. If you provide any included filters, then the excluded filters will be a subset of the included products. Be sure to conform to the vendor's naming standards. For example, Microsoft refers to Internet Explorer using its full name, rather than a common abbreviation such as IE. For example,to include all Windows products except Windows 95, type `{Microsoft::Windows*, Microsoft::!Windows 95}`.

  By default, the following Microsoft products are excluded from patch acquisition and management:

  ```
  !Windows 95,!Windows 98*,!Windows
  Me,!Access*,!Excel*,!FrontPage 200[023],!FrontPage
  9[78],!InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,!P
  roject 200[023],!Project
  98,!Publisher*,!Visio*,!Word*,!Works*
  ```

  The following products are in the exclusion list because they are not supported by Patch Manager: Microsoft Windows 95, Windows 98, Windows Me and SuSE specific products *-yast2, *-yast2-*, and *-liby2.

If specifying a product for exclusion on the command line, surround the complete product string filters in quotes.

- **Replace**: Set replace to Y to delete old bulletins, specified in the bulletins parameter, and then re-acquire them. This will supersede the value for force. In other words, if you set replace to Y, then any bulletin specified for that acquisition will be deleted and reacquired, whether force is set to N or Y. The default is N.
- **superseded_patches**: Set superseded_patches to Y if you want to publish the data even if a patch is marked as superseded. The default is N.
- **vendors**: Specify the vendors to acquire patches from. Example: -vendors Microsoft, RedHat, SuSE, HPUX, SOLARIS. The default is Microsoft.
- **vendor_os_filter**: Specify a filter for the vendor's operating systems in the format *vendor*::*operatingsystem*. Red Hat and SUSE filters for x86_64 architectures use the format: *vendor*::*operatingsystem*-x86-64.

  SUSE 10 filters indicate a relevant service pack (SP1 or SP2) directly after the operating system, as in: *vendor*::*operatingsystem*SP1-x86-64.

  — RedHat examples:
  REDHAT::2.1es,REDHAT::3ws,REDHAT::4as;
  REDHAT::2.1es-x86_64,REDHAT::3ws-x86_64,

  — SuSE examples: SUSE::8, SUSE::9, SUSE::10SP1-x86-64; SUSE::11; SUSE::11-x86_64

  — Do not use vendor_os_filter to specify Microsoft operating systems as they are treated as products. Use the product filter for Microsoft operating systems instead.

Database Synchronization Parameters

To synchronize the databases from a command line

- Run the following command line from the Patch Manager directory:

```
nvdkit ./modules/patch.tkd sync -db_type mssql
-dsn patch -dsn_user rpmadmin -dsn_pass rpmdb
-host localhost:3464 -class "*"
```

dsn is a required parameter; db_type is also a required parameter when the database type is Oracle.

For example, if you only wanted to update the PRODUCT class for a SQL Server database, you would type:

```
nvdkit ./modules/patch.tkd sync -dsn PATCH ø
-host localhost:3464 -class "PRODUCT"
```

If you wanted to update the PRODUCT class for an Oracle database, you would type:

```
nvdkit ./modules/patch.tkd sync -db_type oracle ø
-dsn PATCH -host localhost:3464   -class "PRODUCT"
```

where the dsn is called PATCH and the Configuration Server is the local machine.

The parameters are described below:

- **db_type**: Specify the database type. Valid values are mssql for Microsoft SQL Server and oracle for Oracle. The default is mssql. Specify this parameter (-db_type oracle) to synchronize with an Oracle database.
- **dsn**: Specify the Data Source Name (DSN) the Patch ODBC database. This parameter is required.
- **dsn_user**: Specify the user for the dsn for the Patch ODBC database.
- **dsn_pass**: Specify the password for the user of the Patch ODBC database.
- **host**: Specify the location of your Configuration Server in URL format. This parameter is required. Use the format radia://*ipaddress*:*port*
  - radia indicates the session type to be opened to the Configuration Server.
  - *ipaddress* is the hostname or IP address of the computer hosting the Configuration Server.
  - *port* is the port number of the Configuration Server.
- **class**: Specify the classes you wish to synchronize between the Configuration Server and the Patch SQL Database. For example, if you want to synchronize only the DEVICE class, specify class="DEVICE". This parameter also accepts a wildcard. The default is "*" (synchronize all classes).

- **commit**: Specify 1 if you want to commit changes found in the Configuration Server database to the SQL database. Specify 0 if you do not want change automatically committed. You can view the changes. By default, all changes are committed.
- **rcs_pass**: If authentication has been enabled on your Configuration Server, specify the password for the rcs_user.
- **rcs_user**: If authentication has been enabled on your Configuration Server, specify the rcs_user.

Patch Agent Update Parameters

These settings are for the maintenance of the Patch Manager Agent files. For more information on this, see Updating the Patch Manager Agent on page 9. The following settings are configured in the Patch Agent section:

- **agent_updates**: Use Publish and Distribute to publish the updates to the PATCHMGR Domain and connect them to the DISCOVER_PATCH instance. This option will distribute the updates to your Patch Manager managed devices. Use Publish only to publish the update, but not connect for distribution (deployment) to Patch Manager managed devices.
- **agent_os**: Specify for which operating systems to acquire the agent updates. Valid values are win32, linux and suse.
- **agent_version**: Select which Patch Manager versions you would like to acquire the agent updates for. You can only publish one version to one Configuration Server.

See the sample `patch.cfg` file below. Note the use of brackets for parameters and *forward* slashes in directory paths. If you are specifying any of these from a command line for acquisition, be sure to use quotes around values containing spaces.

```
patch::init {
AGENT_UPDATES PUBLISH,DISTRIBUTE
ARCH REDHAT::*,SUSE::*,HPUX::*,SOLARIS::*,MICROSOFT::x86
BUILD 899
CFG_VER 7.5
DATA_DIR { C:/Program Files/Hewlett-Packard/CM/PatchManager/data}
DL_DATEFMT {%Y-%m-%d %T}
DSN PATCH
DSN_USER sa
```

```
ETC C:/Program Files/Hewlett-Packard/CM/PatchManager/etc/patch
FORCE no
FTP_PASS {{AES256}vQP8q3G7N5j4iMhgA2QUuw==}
HOME C:/Program Files/Hewlett-Packard/CM/PatchManager/modules/patch.tkd
HTTP_RETRIES 2
LABEL PATCH
LANGUAGE {}
LOG C:/Program Files/Hewlett-Packard/CM/PatchManager/logs
MODE both
MODULE patch
RCS_URL radia://localhost:3464
RCS_USER RAD_MAST
REPLACE no
RETIRE {}
ROOT C:/Program Files/Hewlett-Packard/CM/PatchManager/
SECTION all
TITLE {HPCA Patch Manager}
URL /patch
USING_DEFAULT_PATCH_CFG Y
VENDOR_OS_FILTER {}
VERSION {7.50.000}
}
```

Index

D

E

F

G

H

I

L

M

N

Q

R

S

T

U

V

W

X

Z