

HP Client Automation Enterprise

Patch Manager

for the HP-UX, Linux, Solaris and Windows® operating systems

Software Version: 7.20

Installation and Configuration Guide

Manufacturing Part Number: None

Document Release Date: August 2008

Software Release Date: July 008



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2004-2008 Hewlett-Packard Development Company, L.P.

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

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

OpenLDAP
Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.
Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License
Copyright © 1998-2001 The OpenSSLProject.

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

DHTML Calendar
Copyright Mihai Bazon, 2002, 2003

Documentation Updates

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

- Software Version number, which indicates the software version.
 - The number before the period identifies the major release number.
 - The first number after the period identifies the minor release number.
 - The second number after the period represents the minor-minor release number.
- 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, visit the following URL:

<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.

Table 1 indicates changes made to this document for Version 7.20.

Table 1 Document Changes in this Version

Chapter	Version	Changes
All	7.20 Aug 2008	Corrected any 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 for Version 7.10. Refer to the current Release Notes for more information.
1	7.20	Page 14, Using this Guide with Core and Satellite Servers , new topic.
2	7.20	Page 18, Database Pre-requisites for Microsoft SQL Server or Oracle , modified the supported versions of Microsoft SQL Server or Oracle that can be used to host the Patch Manager

Chapter	Version	Changes
		Database. New support includes: <ul style="list-style-type: none"> • SQL Server 2008 • Oracle 11g, Release 1 with the latest Oracle patch set
2	7.20 Aug 2008	Page 20, Creating the Database for Patch Manager , modified topic title, and added Roles and System Privileges to the defined user profile when creating the database using Oracle.
2	7.20	Page 23, “HPCA Patch Manager Server” is the rebranded Windows Service Name.
2	7.20	Page 35, Microsoft Data Feed Prioritization , the default Data Feed Prioritization has changed from MSSecure, Microsoft Update Catalog, Client Automation to Microsoft Update Catalog, Only . To use this default option, <i>all</i> devices in the enterprise must meet minimum operating system and product levels as set by Microsoft.
3	7.20	Page 51, 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.

Support

You can 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 software 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 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 an active support contract. To find more information about support access levels, go to the following URL:

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

To register for an HP Passport ID, go to the following URL:

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

Contents

1	Introduction	11
	HP Client Automation Patch Manager	12
	Using this Guide with Core and Satellite Servers	14
	Terminology	14
	Patch Manager Components	14
	Summary	16
2	Creating the Patch Manager Environment	17
	Patch Manager Implementation Tasks	18
	Database Pre-requisites for Microsoft SQL Server or Oracle	18
	Implementation Task List	19
	Creating the Database for Patch Manager	20
	Installing the Administrator Workstation	22
	Installing the Patch Manager Server	23
	System Requirements	23
	Installation	23
	Verify the Contents of the PATCHOBJ Instance in the Configuration Server	
	Database	26
	Configuring the Patch Manager Server	27
	Infrastructure Settings	28
	Network and Proxy Settings	30
	HP Patch Agent Updates Settings	32
	Preferences	33
	Vendor Settings	35
	Patch Configuration Settings File	43
	Database Synchronization	44
	Adding a Method Connection	44
	Messaging Server	45
	Reporting Server	45
	Summary	46

3 Patch Acquisition	47
Patch Acquisition.....	48
Acquisition Overview	48
About Patch Descriptor (XML) Files	49
About HP-UX Patch Acquisition.....	51
About Microsoft Patch Acquisition and Management.....	52
About Microsoft Automatic Updates	53
About Red Hat Patch Acquisition.....	55
About Solaris Patch Acquisition	58
About SuSE Patch Acquisition Prerequisites	58
Performing a Patch Acquisition.....	59
Creating Custom Patch Descriptor Files	64
Change Management using RADDDBUTIL	65
Setting the Manage Installed Bulletins (mib) Option	65
Patch Acquisition Reports	67
Summary.....	70
 4 Patch Assessment and Analysis	 71
Installing the Patch Manager Agent.....	72
Sun Solaris Patch Agent pre-requisites	75
Sun Solaris 8 agent OS pre-requisites	75
Sun Solaris 9 agent OS pre-requisites	75
Sun Solaris 10 agent OS pre-requisites	76
Sun Solaris Single User Patch Installations	78
Updating the Patch Manager Agent.....	79
Product Discovery and Analysis	82
Detecting and Managing Microsoft Office Security Bulletins.....	83
Best Practices for Managing Microsoft Office Security Bulletins	84
Best Practices with Microsoft Update Catalog Enabled	88
Enabling Microsoft Office Updates in Patch Manager (Versions 3.0.2 or above) ..	89
About Patch Objects used for Device Compliance Reporting.....	91
Patch Manager Administrator Icons	92
Patch Analysis and Reports	92
Filtering Patch Reports with Reporting Server	94
Compliance Reports	95
Research Reports.....	100
Compliance and Research Exception Reports	102

Deleting Devices	103
Managing Vulnerabilities	103
Entitle the FINALIZE_PATCH Service	104
Deploying Automatic and Interactive Patches.....	105
Customizing Reporting Options	106
Disabling Vulnerability Detection and Deployment.....	109
Controlling Patch Deployment (PATCHARG)	109
Preloading Client Automation Proxy Servers	111
Removing a Patch.....	112
Summary.....	114
 A Supported XML Tags for Patch Descriptor Files	115
Bulletin Node	115
Products Node	118
Product Node.....	118
Releases Node	119
Release Node.....	119
Patch Node	119
Patch Signature Node	123
FileChg Node	124
RegChg Node.....	125
HPFileset Node	126
 B Restarting the Managed Device.....	127
Application Events	127
Reboot Types	128
Reboot Modifier: Type of Warning Message	128
Reboot Modifier: Machine and User Options.....	130
Reboot Modifier: Immediate Restart.....	130
Specifying Multiple Reboot Events.....	131

C Policy Server Integration	133
D Patch.cfg Parameters.....	135
Patch Manager Server Configuration Parameters.....	135
Patch Acquisition Parameters	140
Database Synchronization Parameters.....	144
Patch Agent Update Parameters.....	145
Index	147

1 Introduction

At the end of this chapter, you will:

- Know the capabilities of HP Client Automation Patch Manager (Patch Manager).

HP Client Automation Patch Manager

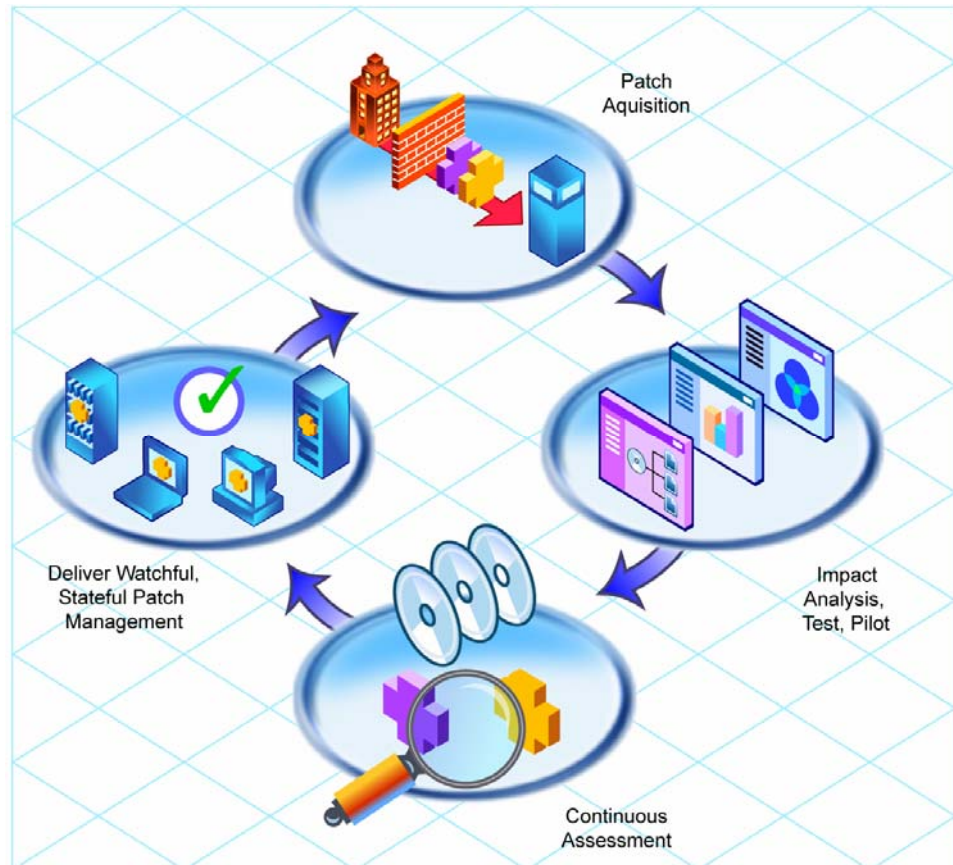
The HP Client Automation Patch Manager (Patch Manager) provides value for business continuity and security initiatives. The Patch Manager is offered as a complete stand-alone solution and can be used as a fully integrated component of the HP Client Automation Suite (HPCA Suite). The HPCA Suite provides 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 permits continued acquisition of security bulletins (advisories) for HP-UX and Sun Solaris (Sparc) for customers upgrading from a previous version of Patch Manager, only.
- **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 Core and Satellite Servers Getting Started Guide as the installation, configuration, and troubleshooting information in that guide may override 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 and Solaris Sun Alerts.

[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, see the *HPCA Configuration Server Guide*.

- **Portal**
Use the HP Client Automation Portal (Portal) to deploy the Patch Manager Agent. See the *HP Client Automation Portal Installation and Configuration Guide (HPCA Portal 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. See 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, see the *HP Client Automation Administrator User Guide (HPCA Administrator Guide)*.

Summary

- Use the Patch Manager to manage security vulnerabilities of applications in your enterprise.
- To use all of the features described in this guide, you must be using Patch Manager Software 7.20 or above.

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 Patch Manager (Patch Manager) environment.
- Know how to modify the Configuration Server and Configuration Server Database.
- Be able to install the Patch Manager.



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

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 Pre-requisites for Microsoft SQL Server or Oracle

The Patch Manager database requires Microsoft SQL Server or Oracle. Verify one of the following supported versions of Microsoft SQL Server or Oracle is already installed in your environment.

- If using Microsoft SQL Server, use one of the following supported versions:
 - SQL Server 2008
 - SQL Server 2005 with Service Pack 2
 - SQL Server 2000 with Service Pack 4 (minimum version supported)
- If using Oracle, the supported Oracle database and ODBC driver versions are listed below. HP recommends using the latest available patch set; the patch sets listed below are the latest as of this writing:
 - Oracle 11g Release 1, patch set 11.1.0.6.0 or later
 - Oracle 10g Release 2, patch set 10.2.0.3 or later (recommended)
 - Oracle 10g Release 1, patch set 10.1.0.5 or later
 - Oracle 9i Release 2, patch set 9.2.0.8 (minimum version supported)

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.

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. 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 on `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. See the *Client Automation Getting Started Guide*.
- ☐ Install the Messaging Server on the Configuration Server. See the *HPCA Messaging Server Installation and Configuration Guide*.
- ☐ Install the Administrator CSDB Editor. See 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 Portal. Optional. See the *HPCA Portal Installation and Configuration Guide*.
 - ☐ Install the Reporting Server. See 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 Microsoft SQL Patch database

- 1 Create a database on your Microsoft SQL Server, with the following recommendations:

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

- 2 Use appropriate Microsoft SQL security recommendations for your enterprise.
- 3 On the computer that will be your Patch Manager Server, create an ODBC DSN called PATCHMGR, or name of your choice, pointing to the

new PATCH database on your SQL Server. If you do not know how to create an ODBC DSN, contact your SQL 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 the Oracle database



Before creating the Oracle database, ensure that the ODBC driver versions of your Oracle server and your Patch Manager server match precisely; the connection to an Oracle database can fail with mismatched ODBC driver versions. For more information, contact your Oracle database administrator.

- 1 Create a tablespace for patchdata on your Oracle Server with the following recommendations:

Tablespace Name	PATCHDATA
Status	Online
Type	Permanent
Datafile	Fully qualified path and name of the datafile such as <code>patchdata.dbf</code>
Storage	Minimum Size 200 M and Max size unlimited
Extent Management	Locally managed with automatic allocation
Segment Space Management	Automatic
Logging	No

- 2 Create a tablespace for patchtemp with the following recommendations:

Tablespace Name	PATCHTEMP
Status	Online
Type	Temporary
Datafile	Fully qualified path and name of the datafile, such as <code>patchtemp.dbf</code>
Storage	Size 1000 M
Extent Management	Locally managed with automatic

	allocation
Segment Space Management	Automatic
Logging	No

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

Username	patch or Create a Username of your choice.
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 UNLIMITED TABLESPACE UPDATE ANY TABLE


- 4 On the computer that will be your Patch Manager Server, create an ODBC DSN called PATCHMGR, or name of your choice, pointing to the new PATCH database on your Oracle Server. If you do not know how to create an ODBC DSN, contact your Oracle database administrator.

Installing the Administrator Workstation

The Configuration Server media contains an Administrator Workstation installation. See the *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 in the accompanying 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 7.20 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**
Installs updated executables and scripts for the Configuration Server to work with Patch Manager.
 - **Configuration Server Database Updates**
Creates the PATCHMGR Domain in the Configuration Server DB.
 - To use the features of Patch Manager 7.20, 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. Refer to page 26.

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**.



Refer to page 104 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 7.20 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.

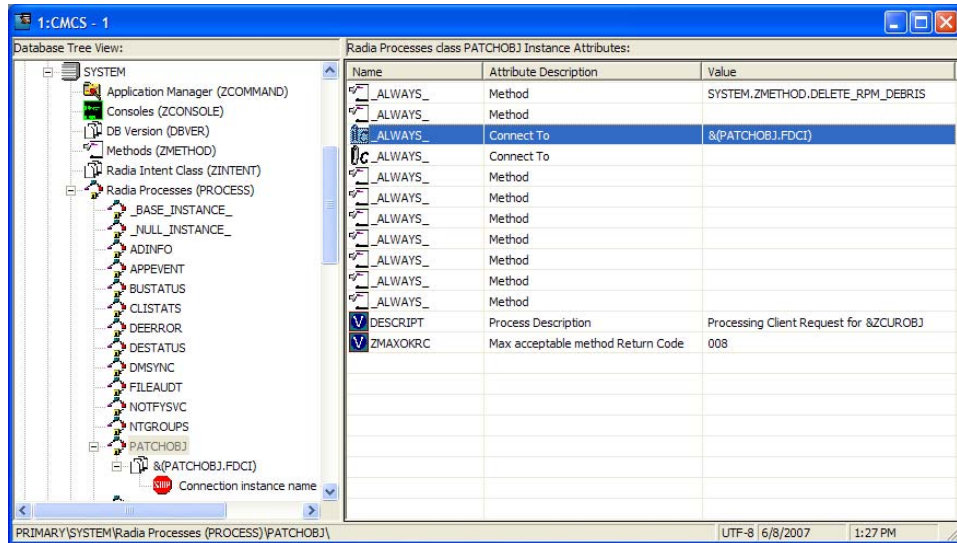
Verify the Contents of the PATCHOBJ Instance in the Configuration Server Database

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).FDCL**. It must be defined as an **_ALWAYS_** Connect To attribute, which looks like this:



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



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 the Patch Manager Server

The HP Client Automation Patch Manager Administrator (Patch Manager Administrator) includes a Configuration Settings area which provides an interface to the Patch Manager Server settings file, `patch.cfg`. The Configuration Settings are divided into five sections, they are: Infrastructure, Network and Proxy, HPCA Patch Agent Updates, Preferences and Vendor Settings. Use the Patch Manager Administrator to modify these settings.

To 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 settings and parameter you want to set. Any setting that ends with an asterisk (*) is *required*. For detailed information on the available settings, see the information following this procedure.
- 3 Click **Save** to apply changes. You will be prompted to restart to allow the changes to take effect.



- 4 Click **Apply Configuration Changes Now** to restart the Patch Manager Server.

Infrastructure Settings

Use the Infrastructure settings 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:

- **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.

ODBC DSN

Name*	LocalServer
User ID*	sa
Password
Database Type	Microsoft SQL Server

Test ODBC Connection Return to Top

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 Patch Manager Update Site

URL*

Return to Top

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.

HP Client Automation Reporting Server

URL

Return to Top

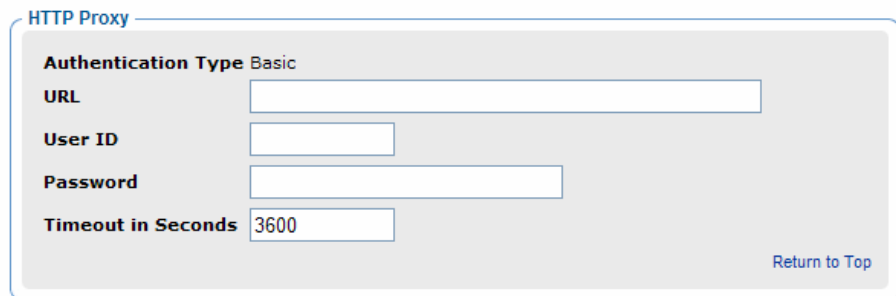
Network and Proxy Settings

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

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 requires 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.



The screenshot shows a configuration window titled "HTTP Proxy". Inside, there are five settings:

- Authentication Type:** Set to "Basic".
- URL:** An empty text input field.
- User ID:** An empty text input field.
- Password:** An empty text input field.
- Timeout in Seconds:** A text input field containing the value "3600".

A "Return to Top" link is located in the bottom right corner of the configuration area.

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.

FTP Proxy

Authentication Type Basic

URL

User ID

Password

Return to Top

HP Patch Agent Updates Settings

Use HP Patch Agent Update settings to configure agent updates.

HP Patch Agent Updates Settings

These settings are used to acquire and apply maintenance for HP Client Automation (HPCA) Patch Manager agent files. For more information on this, see [Updating the Patch Manager Agent](#) on page 79. 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 this parameter from the installation default.

HP Client Automation Patch Agent Updates

Updates
☐ None
☐ Publish
☒ Publish and Distribute

OS
☒ All
☐ Windows
☐ Linux
☐ HP-UX
☐ Solaris

Version
☐ Version 1.2
☐ Version 2
☐ Version 3
☐ Version 5
☒ Version 7

Return to Top

Preferences

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

- **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 specifying 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, by default acquisition and management of Security patches for Microsoft Office, Windows 95, Windows 98, Window Me, Microsoft Office products, and SuSE specific products `*-yast2`, `*-yast2-*`, and `*-liby2` are excluded. 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*,!Powe
rPoint*,!Project 200[023],!Project
98,!Publisher*,!Visio*,!Word*,!Works*"
```

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

Preferences

Enable Patch Management For:

☒ Microsoft ☒ HP-UX

☒ Red Hat ☒ SUSE

☒ Solaris

Save Acquisition Summary

Save History Detail

Patch Data Repository Path*

Retired Bulletins

Excluded Products

- **Default Patch Acquisition Download Language:** Specify the languages for which you want to acquire and manage security patches. The default is en (English).

Vendor Settings

Vendor Settings displays vendor-specific URLs and other options required for patch acquisition and management activities on the agents in your enterprise. You must enable the appropriate vendor and OS selections in the Preferences section.



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.

Microsoft Data Feed Prioritization

Do not change data feed prioritizations until you have read and understood Microsoft's operating system and service pack requirements for Microsoft Update Catalog.

Data Feed Prioritization:

- ☐ MSSecure, Microsoft Update Catalog, Client Automation
- ☒ Microsoft Update Catalog Only - All devices and products managed by Patch Manager must meet minimum service pack levels.
- ☐ Microsoft Update Catalog, Legacy Catalog

[Return to Top](#)

You must select one of the following options:



See [About Microsoft Patch Acquisition and Management](#) and About Microsoft Automatic Updates, starting on page 52, for important information related to Microsoft patch management activities.

- **MSSecure, Microsoft Update Catalog, Client Automation:** 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 website 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 52.

- **Microsoft Update Catalog Only:** (Default option as of Version 7.20) All patches are acquired from the Microsoft Update Catalog. To use this option, *all* devices in the enterprise must meet minimum operating system and product levels as set by Microsoft. Devices not meeting these minimum requirements will not be patched.

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

Microsoft Data Feed Prioritization

Do not change data feed prioritizations until you have read and understood Microsoft's operating system and service pack requirements for Microsoft Update Catalog.

Data Feed Prioritization:

☐ MSSecure, Microsoft Update Catalog, Client Automation

☒ Microsoft Update Catalog Only - All devices and products managed by Patch Manager must meet minimum service pack levels.

☐ Microsoft Update Catalog, Legacy Catalog

The Microsoft Update Catalog Only feed was selected. Only select this option if ALL managed devices in your enterprise meet minimum operating system and service pack levels supported by Microsoft Update Catalog.

By selecting the option Microsoft Update Catalog Only, security bulletin acquisition and management is limited to the operating systems and products supported by Microsoft Update Catalog and Patch Manager. Patch acquisition and management capabilities are NOT provided for Microsoft legacy operating system platforms.

Confirm selection? [More Information](#)

[Return to Top](#)

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

- **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:

- **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 52.

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

Default:

`http://www.msus.windowsupdate.com/msus/v1/auccatalog1.cab`

- **Architecture**: Select the architectures for the acquisition of Microsoft patches. The supported architectures include:
 - **x86** for 32-bit Intel architectures

- **x64** for AMD64 or Intel EM64T. If this target architecture is selected, your Microsoft Data Feed Prioritization must be set to either **Microsoft Update Catalog Only** or **Microsoft Update Catalog, Legacy Catalog**.

Microsoft Feed

MSSecure*

SUS*

Architecture ☒ x86 ☐ x64 (AMD64/Intel EM64T)

[Return to Top](#)

HP-UX Feed Settings

The following settings are configured in the HP-UX Feed section:

- **Security Catalog:** Specifies the url for the data source used to assess HP-UX security vulnerabilities.
Default: **http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=security_catalog2.gz**
- **Patch Description XML:** Specifies the url for the file containing meta data for HP-UX security patches.
Default: **http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=patches.xml**
- **Patch Download:** Specifies the HP-UX url for downloading patches.
Default: **ftp://ftp.itrc.hp.com/**.
- **OS Filter:** Select the operating systems for the acquisition of HP-UX security bulletins. These are the only operating systems that will be available for acquisition for this vendor. Valid values for HP-UX in the patch.cfg file are HPUX::11.00 and HPUX::11.11 for the PA-RISC architectures, and HPUX::11.23 version 2 and HPUX::11.31 for the PA-RISC and IA64 (Itanium) architectures.

HP-UX Feed

Security Catalog

Patch Description XML

Patch Download

OS Filter ☐ 11.00 ☐ 11.11 (11i) ☐ 11.23 (11i v2) ☐ 11.31

[Return to Top](#)

Red Hat Feed Settings

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

- **Red Hat:** Specifies the URL for the Red Hat Network data feed.

Default: **`http://xmlrpc.rhn.redhat.com/XMLRPC`**

- **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 3ES on x86, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/3es`.
- For Red Hat Enterprise Linux 3ES on x86-64, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/3es-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 Versions 2.1, 3, and 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::2.1as, REDHAT::2.1es, REDHAT::2.1ws,`

```
REDHAT::3as,          REDHAT::3es,          REDHAT::3ws,
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::2.1as-x86_64, REDHAT::3as-x86_64,
REDHAT::2.1es-x86_64, REDHAT::3es-x86_64,
REDHAT::2.1ws-x86_64, REDHAT::3ws-x86_64,

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

Red Hat Feed

Red Hat

Publish Package ☐

Dependencies?

OS Filter

x86 ☐ 2.1AS ☐ 2.1ES ☐ 2.1WS ☐ 3AS ☐ 3ES ☐ 3WS ☐ 4AS ☐ 4ES ☐ 4WS ☐ 5 Server ☐ 5 Client

x86-64 ☐ 2.1AS ☐ 2.1ES ☐ 2.1WS ☐ 3AS ☐ 3ES ☐ 3WS ☐ 4AS ☐ 4ES ☐ 4WS ☐ 5 Server ☐ 5 Client

[Return to Top](#)

Solaris Settings

The following settings are configured in the Solaris Feed section to acquire Sun Solaris Sun Alerts (Security patches) and their pre-requisite patches using a Sun Online Account.

Before configuring the Solaris Feed sections, obtain a Sun Online Account.

To obtain a Sun Online Account

- 1 Obtain a **Sun Online Account** User ID and Password through the Sun Microsystems Website. At the time of this writing, this page is located at:
<http://sunsolve.sun.com/pub-cgi/register-user-form.pl?viewmode=newuser&stage=1>
- 2 After reading the **Software License Agreement**, click on the **I Accept** button. According to Sun Microsystems, this is a one time requirement.
- 3 The next page is the **SUNSOLVE ONLINE** Registration form. Fill in the information required by Sun Microsystems.

Note that a **Sun Service Plan** is not required. However, if you have a valid **Sun Service Plan** account number you may enter this when filling out the registration form.

- 4 Finish entering the information, and click on the **Submit Account Info** button. Wait for confirmation that your account has been created.
- 5 Record and maintain the information used to establish the Sun Online Account.

According to information on the Sun Microsystems web site, there are some levels of Solaris OS patches which require a valid Sun Service Plan or Support Contract. If your Sun Online Account is not associated with a Sun Service Plan, the Patch Manager will not be unable to download these patches.

To complete the Solaris Feed Settings using your Sun Online Account

- **SunAlert HTML:** This url provides a list of all available Sun Alerts and the patch ids associated with each Sun Alert. The default is **http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches**.
- **Security Catalog:** This file includes information on all patches, both security and non-security related. The default is **<http://sunsolve.sun.com/private-cgi/pdownload.pl?target=patchdiag.xref>**.

This url provides a list of all Sun Solaris patches as well as meta data concerning Sun Solaris version applicability and the type of patch (recommended or security).

- **Patch Database Reference:** This parameter defines the directory repository for Sun Solaris meta data files. The default is **<https://getupdates1.sun.com/solaris/>**.
- **Patch Database:** This Sun Microsystems url provides meta data concerning Sun Solaris “available” patches. The default is **<https://getupdates1.sun.com/solaris/?action=getFile&name=Database/current.zip>**.
- **Patch Vulnerability Analysis Component:** This auxiliary file is used by Sun Patch Manager Version 2.0 to perform patch applicability and vulnerability assessment. The default is **<https://getupdates1.sun.com/solaris/?action=getFile&name=Database/detectors.jar>**.
- **Patch Download:** This URL provides a reference to the download locations of signed Sun Solaris patches. The default is

`https://sunsolve.sun.com/private-cgi/pdownload.pl?target=%s&method=hs.`

- **User ID:** Supply the User name associated with your Sun Online Account.
- **Password:** Supply the Password associated with your Sun Online Account.
- **OS Filter:** Select operating systems for the acquisition of Solaris patches on the SPARC architecture *only*. Valid values for Solaris in the `patch.cfg` file are: SOLARIS::8, SOLARIS::9, SOLARIS::10 to acquire patches for Solaris versions 8, 9, and 10 on SPARC architecture.

Solaris Feed	
SunAlert HTML	<input type="text" value="http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches"/>
Security Catalog	<input type="text" value="http://sunsolve.sun.com/private-cgi/pdownload.pl?target=patchdiag.xref"/>
Patch Database Reference	<input type="text" value="https://getupdates1.sun.com/solaris/"/>
Patch Database	<input type="text" value="https://getupdates1.sun.com/solaris/?action=getFile&name=Database/current.zip"/>
Patch Vulnerability Analysis Component	<input type="text" value="https://getupdates1.sun.com/solaris/?action=getFile&name=Database/detectors.jar"/>
Patch Download	<input type="text" value="https://sunsolve.sun.com/private-cgi/pdownload.pl?target=%s&method=hs"/>
User ID	<input type="text"/>
Password	<input type="password"/>
OS Filter	<input type="checkbox"/> 8 SPARC <input type="checkbox"/> 9 SPARC <input type="checkbox"/> 10 SPARC

[Return to Top](#)

SuSE Feed Settings

The following settings are configured in the SuSE Feed section.



The default URLs for SuSE meta data Feeds include important case differences:

- SuSE 8 URLs include the term **SuSE** in mixed-case.
- SuSE 9 URLs include the term **SUSE** in uppercase.
- **SuSE 8:** Specifies the secure url to acquire security advisory meta data for SuSE 8.

Default: **`https://you.novell.com/update/i386/update/SuSE-SLES/8/`**

- **SuSE 9:** Specifies the secure url to acquire security advisory meta data for SuSE 9.

Defaults:

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

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

- **SuSE 8-x86_64:** Specifies the secure url for acquiring updates for SuSE 8 on AMD64 or Intel EM64T architectures.

Default: **`https://you.novell.com/update/x86_64/update/SuSE-SLES/8/`**

- **SuSE 9-x86_64:** Specifies the secure url for acquiring updates for SuSE 9 on AMD64 or Intel EM64T architectures.

Defaults:

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

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

- **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 8 and 9 on x86 (32-bit) architectures, as well as SuSE Versions 8 and 9 on x86-64 (AMD64 and Intel EM64T) architectures.

Valid OS Filter values for x86 architectures in patch.cfg are

`suse::8` and `suse::9`.

Valid OS Filter values for x86-64 architectures in patch.cfg are

`suse::8-x86_64` and `suse::9-x86_64`.

The screenshot shows a window titled "SUSE Feed" with several configuration fields:

- SUSE 8:** A text box containing the URL `https://you.novell.com/update/i386/update/SuSE-SLES/8/`.
- SUSE 9:** A text box containing the URL `https://you.novell.com/update/i386/update/SUSE-CORE/9/`. Below it is a dropdown menu with `https://you.novell.com/update/i386/update/SUSE-SLES/9/` selected.
- SUSE 8-x86_64:** A text box containing the URL `https://you.novell.com/update/x86_64/update/SuSE-SLES/8/`.
- SUSE 9-x86_64:** A text box containing the URL `https://you.novell.com/update/x86_64/update/SUSE-CORE/9/`. Below it is a dropdown menu with `https://you.novell.com/update/x86_64/update/SUSE-SLES/9/` selected.
- User ID:** An empty text box.
- Password:** An empty text box.
- OS Filter:** A row of four checkboxes, all of which are checked: `8 x86`, `9 x86`, `8 x86-64`, and `9 x86-64`.

In the bottom right corner, there is a link that says "Return to Top".

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 [Patch.cfg Parameters](#) on page 135 for more information.

Database Synchronization

The patch information that has been sent to the Configuration Server DB must be synchronized with your ODBC Patch Database for assessment and analysis of the patch. The Configuration Server DB and the ODBC Patch Manager 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 ODBC 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.

Usually, this synchronization occurs automatically. There may be circumstances where you may want to run the synchronization manually. You can synchronize using either the Patch Manager Administrator or a command line.

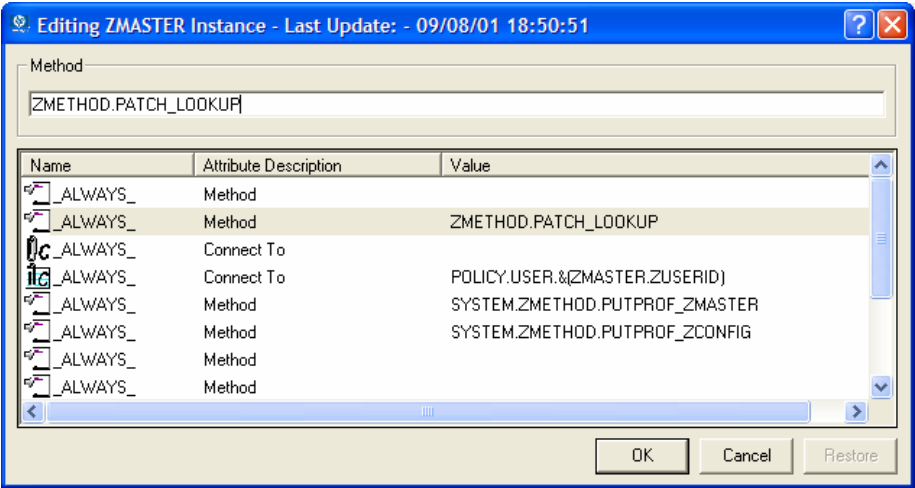
To synchronize the databases using the Patch Manager Administrator

- 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 [Figure 2](#) on page 45.

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

At minimum Reporting Server 5.10 is required to view enhanced reports for Patch Manager; the latest version of the Reporting Server is recommended. 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.

Summary

- Install and modify the Configuration Server and the CSDB.
- Patch Manager requires a SQL Database hosted by SQL Server or Oracle.
- Install the Messaging Server on the Configuration Server with the Patch Data Delivery Agent enabled.
- Install the Patch Manager Server on a computer that can access the Configuration Server and your ODBC Data Source.
- Install the Reporting Server.

3 Patch Acquisition

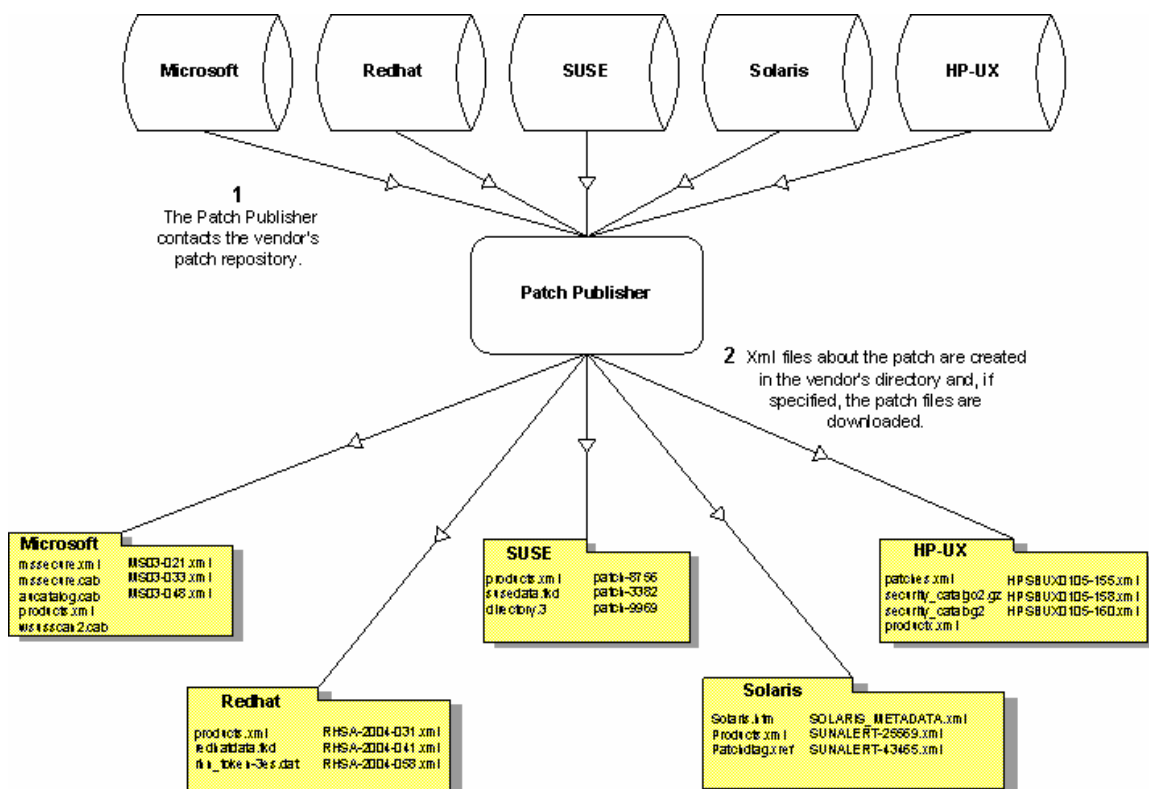
At the end of the chapter, you will:

- Be able to acquire patches.
- Know the parameters available for patch acquisition and database synchronization.

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 supercedence, 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*.

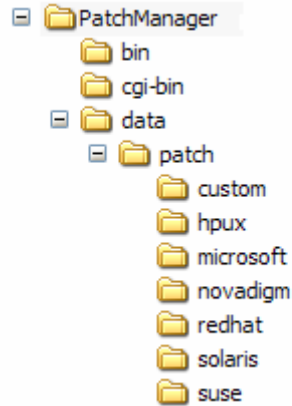
For example, patch descriptor files for Microsoft bulletins would be in: *System Drive:\Program Files\Hewlett-Packard\CM\PatchManager\Data\Patch\Microsoft*

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

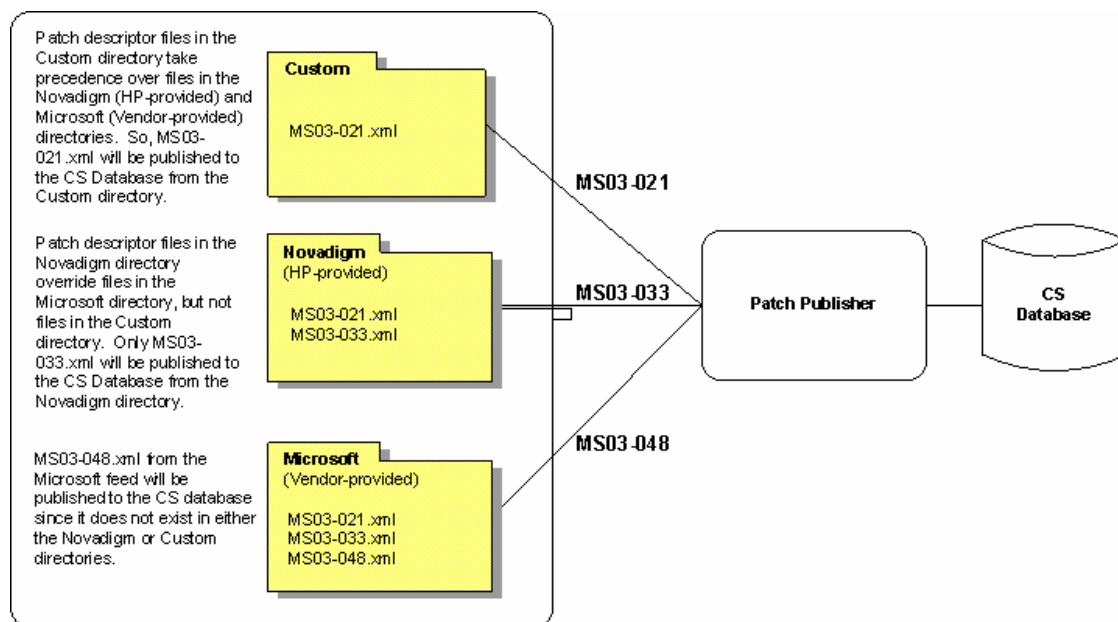


Some of the information acquired from the vendor may need to be altered before the patch can be managed. Therefore, there are two other subdirectories in the `\data\patch` subfolders: `novadigm` and `custom`. HP provides you with some additional patch descriptor files that are located in the `novadigm` 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`, `suse`, `hpux`, `solaris`, and `redhat` 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, HP-UX, SuSE, SUN, and RedHat.

Figure 5 Patch descriptor files



About HP-UX Patch Acquisition



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.

At the time of this writing, keep the following in mind for HP-UX security patches:

- Acquisition and deployment of HP-UX patch bundles is not supported.
- Acquisition does not acquire HP-UX security patch pre-requisites, nor will the deployment of a HP-UX security patch install pre-requisite patches if they found to be missing on the agent.
- Roll back of HP-UX security patches is not supported.

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 35 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, refer to [Detecting and Managing Microsoft Office Security Bulletins](#) on page 83.

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:

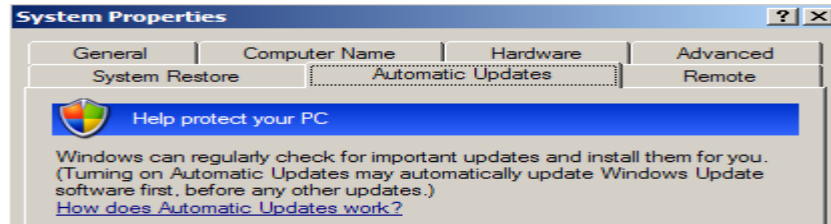
- Deploy the latest MSI 3.1 package manually by downloading it from the Microsoft website. This bulletin is defined for multiple languages. As of this writing, the US-English version is at <http://support.microsoft.com/kb/893803/en-us>,
- or
- Use Patch Manager to acquire, distribute and manage the bulletin 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) Versions 2.1, 3 and 4 on x86 systems only, you will need a Red Hat Network account with at least three Red Hat Network system entitlements, one for each Enterprise Server version. To perform patch acquisitions for Red Hat ES Versions 2.1, 3, and 4 on x86-64 systems, you will need an additional three Red Hat Network system entitlements.

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 3ES on x86, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/3es`.
- For Red Hat Enterprise Linux 3ES on x86-64, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/3es-x86_64`.

When naming the `data/patch/redhat/packages/` subdirectories, refer to the list of **OS Filter Architecture** values on page 39. 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 `rhnclean` 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 `rhnclean` on the command line when logged into the system as root.
- 3 When prompted by the `rhnclean` 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 `rhnclean` tool without applying any patches to the system where you ran `rhnclean`. A file called `systemid` is created.
- 5 Copy the file `/etc/sysconfig/rhn/systemid` produced by the `rhnclean` 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 nine combinations of Red Hat Versions (2.1, 3, or 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 2.1, then rename the `systemid` file to `redhat-2.1es.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 3, then rename the `systemid` file to `redhat-3es-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.

About Solaris Patch Acquisition

At the time of this writing, the Sun Microsystems website requires a secure (SSL) connection for patch acquisition, although it does not require or perform certificate validation. To meet this requirement, the HP-supplied `tls.tkd` module must be present in the `\modules` directory of the Patch Manager Server that you are using to perform secure patch downloads from the Sun Microsystems website.

Acquisition and deployment of Sun Solaris patch clusters is not supported.

Roll back of Solaris patches is supported if roll back of the patch is supported by the patch vendor, and the roll back of the patch does not conflict with another patch's pre-requisite requirements. By default, patch roll back capabilities are disabled.

On November 29, 2005 Sun Microsystems instituted a new policy pertaining to patches for Sun Solaris Release 10. The intent of this new, evolving policy is to require a Sun Solaris 10 customer to obtain a valid Sun Contract to download non-security related *recommended* patches. These patches were freely available before the imposition of this new policy. Because of this new patch policy from Sun, customers may notice HTTP download errors of the type 4XX during acquisition. These errors cause no known problems with the functionality of the Patch Manager for Solaris product. Sun Microsystems has published information on their Web site indicating that their new policy may be extended to other Sun Solaris operating systems.

About SuSE Patch Acquisition Prerequisites

SSL: The Novell website requires a secure (SSL) connection for patch acquisition. To meet this requirement, the HP-supplied `tls.tkd` module must be installed in the `\modules` directory of the Patch Manager Server

that you are using for SuSE 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: For SuSE 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 Interface.

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 profiles that can be saved and used repeatedly. You will need to first create the acquisition file, and then use the Patch Manager Administrator to run the file. Parameters specified in an acquisition profile 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 the Patch Manager Server](#) on page 27 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 parameters that are required depend on your environment.

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 Settings**.
- 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**.

New Acquisition File

Filename	Description
November.acq	November 2004

- 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 set Acquisition Settings.

Acquisition Settings for November

? **Acquisition File Description** November 2004

? **Bulletins**

? **Mode** Both ▼

? **Force** No ▼

? **Replace** No ▼

? **Command Line Overrides**

[Return to Top](#)

- **Acquisition File Description:** Create a description for the acquisition file.
- **Bulletins:** Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. For Red Hat Security advisories, use a hyphen (-) in place of the colon (:) that appears in the Red Hat Security advisory number as issued by Red Hat.
 - Microsoft Security bulletins use the naming convention `MSYY-###`, where `YY` is the last two digits of the year that the bulletin was issued and `###` is a sequential number of the bulletin number being released for this the year specified. Microsoft service pack patch descriptor files supplied by HP are supplied with the following naming convention: `MSSP_operatingsystem_spnumber`. To acquire *sample* Microsoft Operating System service packs, specify `MSSP*`. This will download sample service packs acquired from the `novadigm` or `custom` folders.
 - HP-UX Security bulletins use the naming convention `HPSBUX#####`, where `HP` indicates HP hardware, `SB` indicates security bulletin, and `UX` indicates the HP-UX operating system. At times the HP-UX security bulletin may contain an embedded hyphen.
 - Red Hat Security advisories are issued using the naming convention `RHSA-CCYY:###`, where `CC` indicates the century and `YY` the last two digits of the year when the advisory was issued, and `###` the Red Hat patch number. However, because the colon is a reserved character in products, you must use a hyphen (-) in place of the colon (:) that appears in the Red Hat-issued Security advisory number. Specify

individual Red Hat Security advisories to Patch Manager using the modified naming convention of `RHSA-CCYY-###`.

- SuSE Security patches use the naming convention `SUSE-PATCH-####`, where `###` represents a numbering scheme provided by SuSE.
- Sun Solaris Sun Alerts use the naming convention `SUNALERT-number`, where `number` represents the specific Sun Microsystems Sun Alert ID number, which can be found on the following web page:

`http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches`



If you do not want to download any bulletins, use `-bulletins NONE`.

- **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 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`.



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 [Patch.cfg Parameters](#) on page 135 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.

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.

HP-UX Settings

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

Solaris Settings

- **Acquire Solaris Patches?:** Select **Yes** if you want to acquire Solaris 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 the acquisition using your saved settings.

To run an acquisition from the Patch Manager Administrator

- 1 From your web browser, go to **http://patchserveripaddress:port/patch/manage/admin.tsp**.
- 2 From Operations, click **Start an Acquisition**.
- 3 Select a file by clicking on its name.
- 4 Confirm the settings for this acquisition.

The screenshot displays two configuration panels. The top panel, titled "Acquisition Settings for MS04 ()", contains four settings: "Bulletins" set to "MS04*", "Mode" set to "Both", "Force" set to "NO", and "Replace" set to "NO". The bottom panel, titled "Microsoft Settings", contains one setting: "Languages" set to "English".

Acquisition Settings for MS04 ()	
Bulletins	MS04*
Mode	Both
Force	NO
Replace	NO

Microsoft Settings	
Languages	English

Report Acquisition Status

The screenshot shows a configuration panel titled "Report Acquisition Status". It contains two settings: "Report Acquisition Status" with a dropdown menu currently showing "Periodically", and "Update Acquisition Status every" with a text input field containing the number "1" followed by the label "Minutes".

Report Acquisition Status	
Report Acquisition Status	Periodically ▼
Update Acquisition Status every	1 Minutes

Report Acquisition Status: In addition to the acquisition log, you can specify how frequently you want to update the current acquisition status, viewable in the Patch Manager Administrator.

- **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.

Look at the Patch Acquisition Reports using the HP Reporting Server to check the success of the acquisition. In addition, a log file is created in the Patch Manager's log directory called `patch-acquire.log`. The patch acquisition log includes the version and build number of `patch.tkd`.

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 `hpux`, `microsoft`, `redhat`, `suse`, `solaris` 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* (Doc ID: OV-EN022930). The link is:
<http://openview.hp.com/ecare/getsupportdoc?docid=OV-EN022930>.

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 all (or y)

Manage all installed bulletins, whether installed by Patch Manager or an external source. This is the default behavior.

-mib hppm (or n)

Manage HP Patch Manager-installed bulletins, only; do not manage bulletins installed by an external source.

-mib none

Do not manage any installed bulletins, whether installed by Patch Manager or an external source; manage only bulletins not already installed.

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 Admin CSDB Editor to configure the `-mib` option on the PRIMARY.PATCHMGR.CMETHOD.DISCOVER instance in the Configuration Server Database. The `-mib` option must be added to the current values for the ZCREATE, ZVERIFY, ZREPAIR, and ZDELETE methods. Details follow.

- 1 Use the CSDB Editor and navigate to the PRIMARY.PATCHMGR.CMETHOD.DISCOVER instance.
- 2 Edit each of the values for the ZCREATE, ZVERIFY, ZREPAIR, and ZDELETE methods. Append the following text to the end of each method's current value:

-mib all (or y)

This is the default behavior to continue to manage all installed bulletins. No entry is required to obtain this behavior.

-mib hppm (or n)






Required entry to stop Patch Manager from managing bulletins installed by another source; it will continue to manage bulletins installed by itself.

-mib none

Required entry to stop Patch Manager from managing bulletins installed

by itself or an external source; use **-mib none** to manage only those bulletins not already installed.

The following image shows an example of setting the Manage Installed Option to None to skip the management of any installed bulletins. Notice each method's value ends in **-mib none**.

Client Method class DISCOVER Instance Attributes:		
Name	Attribute Description	Value
 ZCREATE	Create Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)patchagt.tkd discover -mib none
 ZDELETE	Delete Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)patchagt.tkd discover -mib none
 ZVERIFY	Verify Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)patchagt.tkd discover -mib none
 ZUPDATE	Update Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)patchagt.tkd discover -mib none
 ZREPAIR	Repair Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)patchagt.tkd discover -mib none

3 Save your changes.

The next time a Patch Manager agent connects to the Configuration Server, agents will reflect the change of configuration for bulletins already installed and managed through Patch Manager.

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 Manager Reports** to expand the list of reports. For more information, 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 7 View the Acquisition summary report

Acquisition Summary										
				15 items				1 - 15 of 17 items		
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.

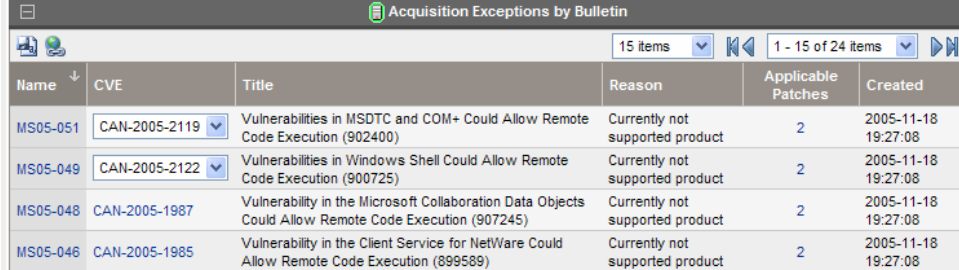
Figure 8 View the acquisition summary by bulletin

Acquisition by Bulletin					
15 items		1 - 15 of 436 items			
Name	CVE	Title	Applicable Patches	Created	Modified
SUSE-PATCH-9960		Recommended update for yast2-http-server	2	2005-11-04 16:59:10	2005-11-04 16:59:10
SUNALERT-57786	CVE-2005-1518	automountd(1M) May Stop When Accessing "/xfn/_x500"	1	2005-10-20 19:17:50	2005-10-31 20:59:48
SUNALERT-57780	CVE-2005-1591	NIS+ Client Users May Be Able to Cause a Denial of NIS+ Service	3	2005-10-20 19:17:50	2005-10-31 20:59:48
SUNALERT-57768		Multiple Security Vulnerabilities in Xsun and Xprt Server Font Handling	3	2005-10-20 19:17:50	2005-10-31 18:15:42
SUNALERT-57766		Certain Network Services Disruptions or "Spoofs" Could Occur as a Result of Possible Network Port Theft	2	2005-10-20 19:17:50	2005-10-20 19:17:50
SUNALERT-57759		UFS Logging on Root Filesystems May Result in Reboot Failures	6	2005-10-20 19:17:50	2005-10-20 19:17:50

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 number. In Figure 8 above, one of the files associated with MS04-001 is not currently supported by Patch Manager.
- 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 9 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 10 View the acquisition by patch



Bulletin	Product / Release	Number	Patch Language	Superceded	Status	Size (bytes)	Date
HPSBUX0011-128	HP-UX Version 11.00	PHSS_32539		N	0	13,007,610	2005-11-02
HPSBUX0011-129	HP-UX Version 11.00	PHSS_27158		N	0	19,836,428	2005-11-02
HPSBUX0011-129	HP-UX Version 11.11	PHSS_27158		N	0	19,836,428	2005-11-02
HPSBUX0011-130	HP-UX Version 11.00	PHCO_22957		N	0	129,159	2005-11-02
HPSBUX0012-133	HP-UX Version 11.00	PHSS_22678		N	0	11,740,044	2005-11-02
HPSBUX0012-133	HP-UX Version 11.11	PHSS_22678		N	0	11,740,044	2005-11-02
HPSBUX0012-134	HP-UX Version 11.00	PHCO_26020		N	0	67,858	2005-11-02
HPSBUX0012-135	HP-UX Version 11.00	PHCO_22665		N	0	793,013	2005-11-02
HPSBUX01002	HP-UX Version 11.00	PHNE_31096		N	0	6,710,014	2005-11-02

Click on an item in the Product/Release column for a specific bulletin to drill down for full details on the patch.

Summary

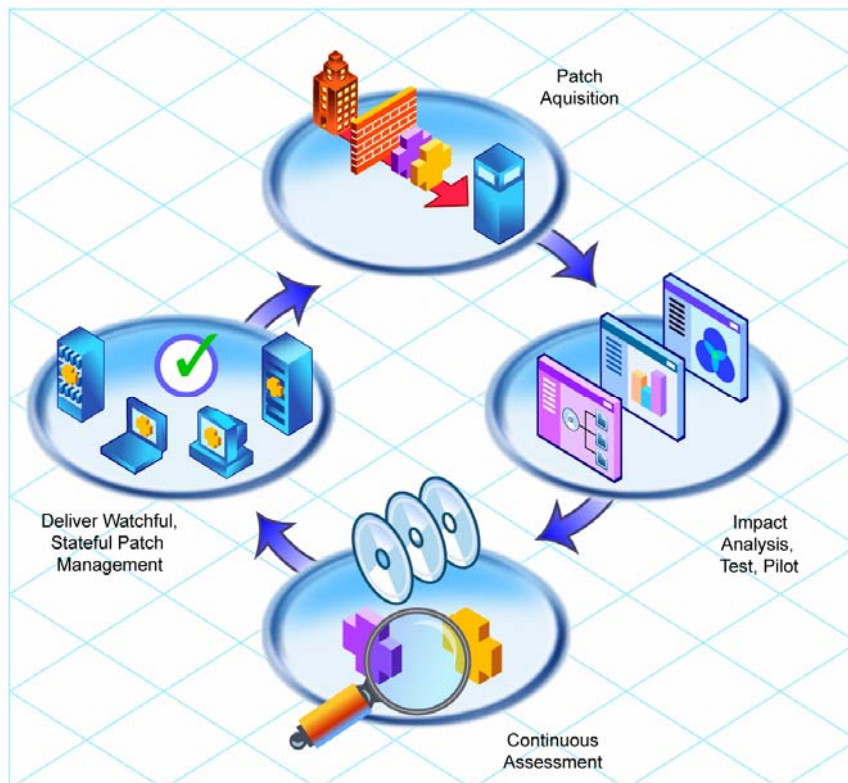
- Run a Client Automation Patch Acquisition to acquire the patches and publish them to the Configuration Server DB.
- The Patch information from the Configuration Server DB automatically synchronizes with the Patch Manager SQL Database.
- To see the status of your acquisition, use the Reporting Server and view the Patch Manager Acquisition reports.

4 Patch Assessment and Analysis

At the end of this chapter, you will:

- Know how to install the Patch Manager agent.
- Know how to manage patches on target devices.
- Be familiar with reports that you can generate for patch files.

Figure 11 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 Portal 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, see either the *HPCA Portal 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 nvdkit build supplied with HP Client Automation v 7.20 media. The absolute minimum nvdkit build required on a Patch Agent is nvdkit build 427; if your target devices do not meet this requirement, see the [HP Support](#) web site.

To install the Patch Manager agent from the Portal

- 1 Use the Portal and the **Install Client Automation Agent** task to begin the installation process.
- 2 On the Client Automation – Agent Opts panel, select **Patch Manager**.

Product	
Application Manager:	<input type="checkbox"/>
Application Self-Service Manager:	<input type="checkbox"/>
Inventory Manager:	<input type="checkbox"/>
OS Manager:	<input type="checkbox"/>
Patch Manager:	<input checked="" type="checkbox"/>

- 3 Complete the remaining information on the panel.
- 4 Schedule the installation and submit the job.



If the Portal Agent is not already installed on the target device, the Portal Agent will be installed along with the Patch Manager Agent.

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 following 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 7.20 functionality is Application Manager Version **5.0**; however, Application Manager Version 7.20 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 7.20.

- **Linux:** Enterprise Versions of Red Hat: versions 2.1, 3, and 4 on releases AS, ES and WS and version 5 on server and client releases, are supported for x86 (32-bit Intel) and x86-64 (Opteron/EMT64) architectures; SuSE Enterprise Server Versions 8 and 9 on x86 (32-bit) architectures, as well as SuSE Versions 8 and 9 on x86-64 (AMD64 and Intel EM64T) architectures.

The Client Automation Version 7.20 Agents for HP-UX and Solaris are not available for installation. However, continued use of Patch Manager v 5.x Agents is presently supported for use with Patch Manager v 7.20 for the following operating systems:

- **HP-UX:** operating system releases 11.00 and 11.11 (11i) for the PA-RISC architecture, and 11.23 (version 2) and 11.31 for the PA-RISC and IA64 (Itanium) architectures.
- **Sun Solaris (SPARC):** operating system releases 8, 9, and 10.

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

- Patch Agent Maintenance\linux\ram
- Patch Agent Maintenance\hpux\ram (*5.x level support*)
- Patch Agent Maintenance\solaris\ram (*5.x level support*)

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 Portal

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, see 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 using the Portal, refer to the *HPCA Portal 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 command line **`./install`** 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*.

Sun Solaris Patch Agent pre-requisites



This topic is retained for reference, only, by Patch Manager customers who have existing Version 5.x Sun Solaris Agents. As of Version 7.20, HP Client Automation no longer provides Agents for managing Sun Solaris devices.

Sun Patch Manager 2.0 is required to use Patch Manager for vulnerability assessment. The Sun Patch Manager 2.0 feature is discussed on Sun's web site. At the time of this writing, the url for this page is **<http://www.sun.com/download/products.xml?id=40c8c2ad>**. This includes information regarding the installation and requirements for Sun Patch Manager software.

Sun Solaris 8 agent OS pre-requisites



This topic is retained for reference, only, by Patch Manager customers who have existing Version 5.x Sun Solaris Agents. As of Version 7.20, HP Client Automation no longer provides Agents for management of Sun Solaris devices.

For Sun Solaris 8, navigate to the above web page and click the Download button at the bottom of the web page next to the **Price: Free** statement. Even though the download is free, you must be a registered on Sun's web site to acquire the Sun Patch Manager 2.0 for Solaris 8 SPARC code.

Once downloaded, follow Sun's recommended instructions on how to install Sun Patch Manager 2.0 on your Solaris 8 SPARC system.

Sun Solaris 9 agent OS pre-requisites



This topic is retained for reference, only, by Patch Manager customers who have existing Version 5.x Sun Solaris Agents. As of Version 7.20, HP Client Automation no longer provides Agents for management of Sun Solaris devices.

For Sun Solaris 9, the Sun Solaris Patch 112945-39 or the latest revision of patch 112945 must be installed. This patch installs Sun Microsystems Patch

Patch Manager Version 2.0. HP recommends this patch be applied using the `-d` option of the Sun Solaris `patchadd` system utility, to prevent the unintentional removal or rollback of the pre-requisite patch required by Patch Manager.

In addition, you must install a particular Java Runtime Environment package, which at the time of this writing is identified by Sun Microsystems as the package `jre-1_5_0_04`. This can be downloaded from Sun Microsystems. This requirement results from Sun Solaris Patch binaries being provided in the form of java archive files (`.jar` extension).

Sun Solaris 10 agent OS pre-requisites



This topic is retained for reference, only, by Patch Manager customers who have existing Version 5.x Sun Solaris Agents. As of Version 7.20, HP Client Automation no longer provides Agents for managing Sun Solaris devices.

Solaris 10 Registration Requirement

When Sun Microsystems introduced their new Sun Connection Update Manager patching facility for the Solaris 10 Operating System, they continued their policy of making security patches freely available. However, because the Solaris 10 Operating System is also freely available, Sun has now adopted a patch policy that explicitly states security patches are “Free with Registration”. This policy requires that every Solaris 10 Operating System must be registered with Sun Microsystems in order to download and apply security patches.

Therefore, to perform patch management activities associated with Patch Manager, Sun Microsystems now requires a Solaris software registration for each Solaris 10 agent device. Failure to register a Solaris 10 Operating System with Sun Microsystems results in an error when performing a vulnerability assessment with Patch Manager.

Sun Solaris 10 agents that are not registered with Sun Microsystems will be displayed in the Patch Management Compliance Device Errors report.

Registering a Solaris 10 system with Sun Microsystems

At the time of this writing, the following Sun Microsystems web page contains Solaris Software Registration instructions:

<http://docs.sun.com/app/docs/doc/817-1985/6mhm8o5u2?a=view>

Minimum Java Development Kit Version

Some earlier versions of the Solaris 10 operating system experienced problems registering Solaris 10 systems with Sun Microsystems if the Solaris 10 system was behind a network firewall. Therefore, Sun Microsystems recommends installing jdk-1.5.0_11 as the *minimum* version of the Java Development Kit (JDK) package to help ensure a successful Solaris 10 system registration. At the time of this writing, the following Sun Microsystems web page can be accessed to download the jdk-1.5.0_11 software and obtain installation instructions:

http://javashopl.m.sun.com/ECOM/docs/Welcome.jsp?StoreId=22&PartDetailId=jdk-1.5.0_11-oth-JPR&SiteId=JSC&TransactionId=noreg

Solaris 10 OS requirements

For Sun Solaris 10, the base Operating system install must include:

- **Developer Software Support Group of Solaris 10**, which provides Sun Patch Manager Version 2.0
- The subsequent patches that update the Solaris 10 patching facility from Sun Patch Manager Version 2.0 to **Sun Update Connection Manager 1.0**. A majority of these patches are available via Sun Alerts, as noted in Table 2 on page 77.

Minimum patch levels to use Sun Update Connection

Sun Solaris 10 managed-devices must have their Sun Update toolset brought to the current patch level in order to use Sun Update Connection Manager 1.0 and Patch Manager. Most are contained in Sun Alerts, which can be applied automatically. Table 2 lists the required patches (as of the date of this writing).

Table 2 Solaris 10 SPARC Patches for Sun Update Connection

Solaris Patch ID	Included in Sun Alert(s)
119254	SUNALERT-101649
119317	SUNALERT-101688
119683	SUNALERT-101688
121296	SUNALERT-101688 SUNALERT-102449
122034	SUNALERT-101688 SUNALERT-102449

Solaris Patch ID	Included in Sun Alert(s)
124630	No

For the latest information on required patch updates for Sun Solaris, check the **Latest Patch Update** topic at the Sun Solve Online page at <http://sunsolve.sun.com/pub-cgi/show.pl?target=home>.

Sun Solaris Single User Patch Installations



This topic is retained for reference, only, by Patch Manager customers who have existing Version 5.x Sun Solaris Agents. As of Version 7.20, HP Client Automation no longer provides Agents for the management of Sun Solaris devices.

Some patches associated with Sun Alerts must be installed in single user mode to apply the patch correctly. It is imperative for installation of those patches that the user applies the supplied shell script `S07radiapm` located in the Patch Agent Maintenance\`solaris\singleuser` folder on the Patch Manager media to the appropriate Sun Solaris agent directory.

For Solaris 8 and 9

Install the script in the `/etc/rc2.d` directory. Change the permissions of the shell script to ensure it is executable by the root user. You can install this file on a Sun Solaris agent using a post installation task during the installation of the Application Manager. For additional information on UNIX agent post-installation tasks, refer to the *HPCA Application Manager and Application Self-service Manager Guide for UNIX*.

For Solaris 10

Install the script in the `/etc/init.d` directory. Change the permissions of the shell script to ensure it is executable by the root user. You can install this file on a Sun Solaris agent using a post installation task during the installation of the Application Manager. You must also install the supplied text file `radia-single.xml` located in Patch Agent Maintenance\`solaris\singleuser` on your Sun Solaris 10 managed device. The introduction of the Service Management Facility (SMF) in Solaris 10 requires this system modification on a Solaris 10 based device for the Patch Manager single user patch installation facility to function properly. Verify that `radia-single.xml` is placed in the Sun Solaris 10 computer's `/var/svc/manifest/site` directory, then execute the following command as root or super user:

```
svccfg import /var/svc/manifest/site/radia-single.xml
```

For additional information on UNIX post-installation tasks, refer to 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 updated product discovery and management scripts. 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 find out the status of updates. To do this, click **View Agent Updates**.

Figure 12 View agent updates

Configuration

- Configuration Settings
- Acquisition Settings

Operations

- Start an Acquisition
- Perform a Synchronization
- View Logs
- View Agent Updates**
- Delete Devices

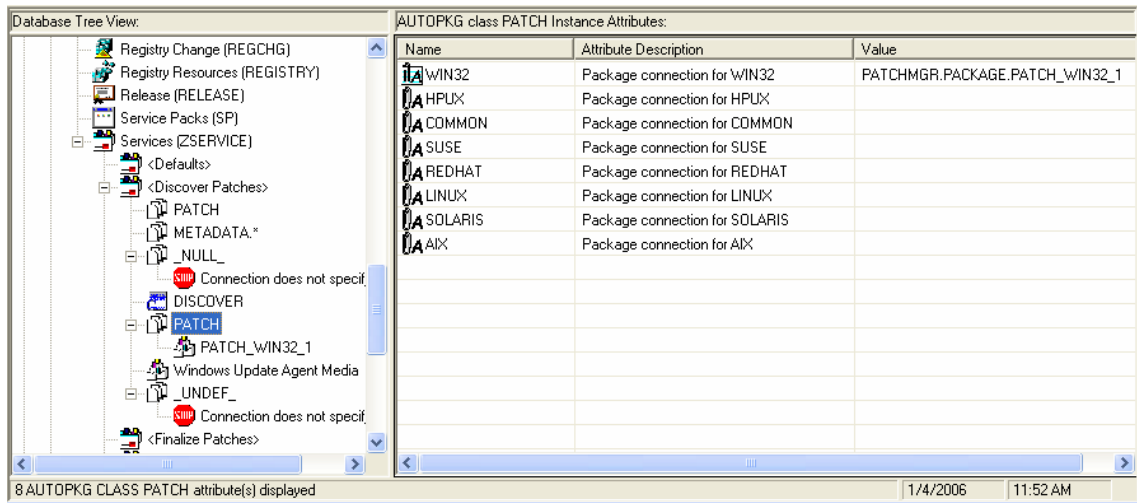
Agent Updates

Patch Manager agent update information.
Select a package name to view agent file details.

Package Name	Package	Release Date	Published
HP-UX Patch Scripts	PATCH_VERSION2_HPUX_3	2.1	08/09/05
HP-UX Patch Scripts	PATCH_VERSION2_HPUX_4	2.1	10/17/05
HPUX Patch Scripts	PATCH_VERSION2_HPUX_1	2.1	05/24/05
HPUX Patch Scripts	PATCH_VERSION2_HPUX_2	2.1	05/25/05
Linux Patch Scripts	PATCH_VERSION2_LINUX_1	2.0	01/04/05
Linux Patch Scripts	PATCH_VERSION2_LINUX_2	2.0	02/18/05
Linux Patch Scripts	PATCH_VERSION2_LINUX_3	2.0	05/02/05
Linux Patch Scripts	PATCH_VERSION2_LINUX_4	2.0.1	05/16/05
Linux Patch Scripts	PATCH_VERSION2_LINUX_5	2.1	08/09/05
Linux Patch Scripts	PATCH_VERSION2_LINUX_6	2.1	10/17/05
Solaris Patch Scripts	PATCH_VERSION2_SOLARIS_2.2.2	10/24/05	
Solaris Patch Scripts	PATCH_VERSION2_SOLARIS_3.2.2	10/24/05	
Solaris Patch Scripts	PATCH_VERSION2_SOLARIS_4.2.2	10/24/05	

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 only to Publish and 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 13 Create connections to the published package



AIX is 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 win32, linux, suse, hpx and solaris.
- **Version:** Select the Patch Manager version for which you would like to acquire the agent updates. You can only publish one version to one 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 7.20, specify 7. This is the default for new Patch Manager 7.20 installations. This is also the default value if you migrated from an earlier release and removed the existing `patch.cfg` before performing the migration.



When you specify Version 7, existing HP-UX and Sun Solaris Patch Manger agents are maintained at the latest available 5.1x level.

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 strongly 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 7.20, and maintain any existing HP-UX and Sun Solaris Patch Agents at the latest available 5.1x level. 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, when Microsoft discontinues further updates to their legacy catalog called `MSSecure`. 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 since 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 `dtype` parameter be set to **PATCH**. This will keep the resolution of services for the Patch Manager agent separate 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 look like:

```
radskman ip=<ConfigurationServerIPAddress>,  
  
port=<ConfigurationServerport>,dname=patch,catexp=runmode:auto  
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, since Microsoft Office applications utilize Windows Installer technology, both patching and self-healing are provided inherently. 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 or AIP) or a Client Automation 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, it is necessary to discontinue the use of an ACP or an Client Automation management application for distributing *updates* to your Microsoft Office applications. You may continue to use an ACP or a Client Automation application to *deploy* Microsoft Office applications; however, updates must be managed solely by Patch Manager.



Once Patch Manager is used to distribute Microsoft Office application updates, both ACP-managed and Client Automation-managed Microsoft Office applications will no longer be capable of receiving updates through those respective 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 utilize desired-state technology to distribute updates to Microsoft Office applications. Therefore, before enabling Patch Manager for the purpose of updating Microsoft Office applications, please be sure 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, below
- Best Practices with Microsoft Update Catalog Enabled on page 88
- Enabling Microsoft Office Updates in Patch Manager (Versions 3.0.2 or above) on page 89

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 above 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 Administrative Installation Point (AIP). For details on Microsoft best practices, see the article “Distributing Microsoft Office 2003 Product Updates” on the Microsoft Web site. At the time of this posting, the location is

<http://Office.microsoft.com/en-us/ork2003/HA011402381033.aspx>.

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 deploy patches for Microsoft Office applications **only** when you no longer want to publish or deploy patches for Microsoft Office using another solution, including 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 of the following:

- The Microsoft Office product was installed from compressed media (CD-ROM), or,
- The Microsoft Office product was installed from an AIP, but you have decided to no longer use the AIP synchronization process for updating Microsoft Office products, or,
- The Microsoft Office product was installed from 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 sync 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, read the article [Updating Microsoft Office XP Agents from a Patched Administrative Image](http://Office.microsoft.com/en-us/assistance/HA011525721033.aspx) on the Microsoft Web site. At the time of this posting, the location is **<http://Office.microsoft.com/en-us/assistance/HA011525721033.aspx>**.

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 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, you are advised to publish Office patches using the Admin Publisher and deploy and manage Office patches using Application Manager or Application Self-service Manager.



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 Office XP, Office 2003, and Office 2007, as well as their stand-alone products. For example, the stand-alone products for Office 2007 that can be patched using Patch Manager with the Microsoft Update Catalog are listed below:

- Access 2007
- Excel 2007
- Groove 2007
- Publisher 2007
- OneNote 2007
- Outlook 2007

- Access 2007
- InfoPath 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. See [About Microsoft Patch Acquisition and Management](#) on page 52.

► Customers 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 PatchManager 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 the Patch Manager to use new technology including the Microsoft Update Catalog data feed and the Windows Update Agent. For more information about Microsoft Update Catalog, please refer to the following website. At the time of this posting, the location is

<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 OS platforms 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 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 or above)

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* available on the [HP Support](http://openview.hp.com/ecare/getsupportdoc?docid=OV-ENKB01192) website at:
<http://openview.hp.com/ecare/getsupportdoc?docid=OV-ENKB01192>.



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` (for Windows)
- `/opt/HP/CM/ConfigurationServer/data/patch` (for 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 the Reporting Server.

Figure 14 Click an icon

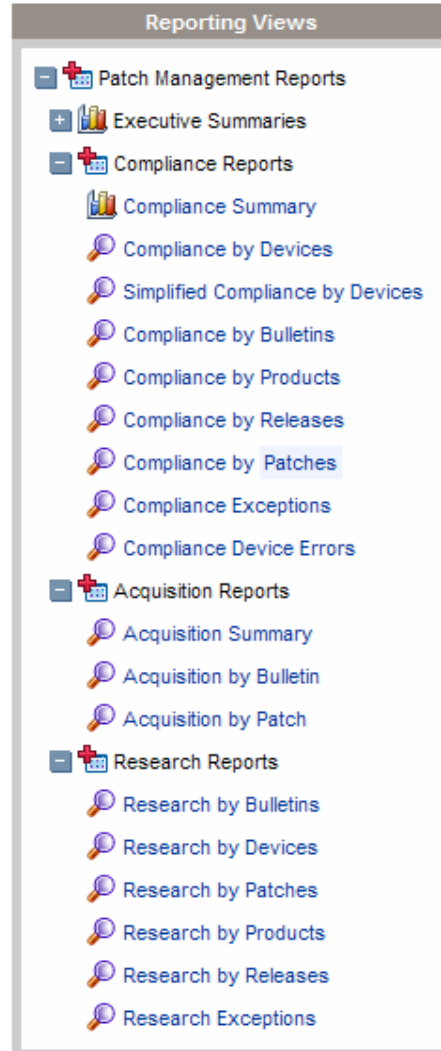


- Click the  icon to refresh the page.
- Click the  icon to return to Patch Manager Administrator Home Page.
- Click the  icon to print the currently viewed page.
- Click the  icon to go to Patch Manager Reporting using the Reporting Server.
- Click the  icon to see the latest Bulletin correction information.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

Patch Analysis and Reports

Reporting Server v 5.0 and above provides web-based reports for Patch Manager. For installation and configuration instructions for the Reporting Server, refer to the *HPCA Reporting Server Guide*. The Reporting Server installation media is with the Client Automation Infrastructure media. To view the reports, first access your Reporting Server. Then, under Reporting Views, click **Patch Manager Reports** to expand the list of reports.

Figure 15 View the list of Patch Manager reports

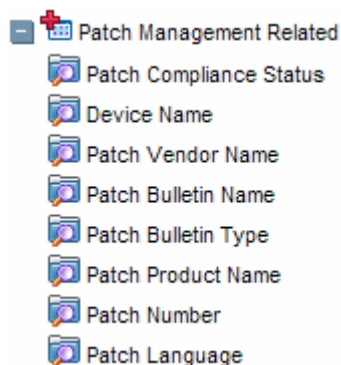


There are three types of Patch Manager Reports, Compliance, Acquisition, and Research. For information on the Acquisition Reports, see Chapter 3, [Patch Acquisition](#).

Filtering Patch Reports with Reporting Server

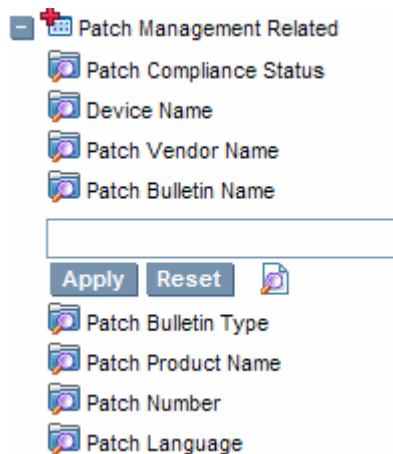
Reporting Server also provides filtering capabilities. To access the filters, expand Patch Management Related in the Search Controls section of the Reporting Server page.

Figure 16 View the Patch Management Related Data Filters



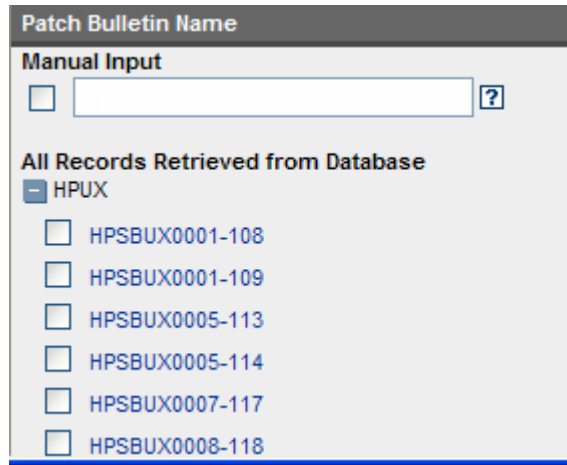
Some filters only allow a text entry. Others have a Show available options button or magnifying glass to open a filter lookup window.

Figure 17 Expand a filter



Click the magnifying glass to open the filter lookup window.

Figure 18 Select the filter.



The screenshot shows a window titled "Patch Bulletin Name". It contains two main sections. The first section, "Manual Input", has a checkbox and a text input field with a help icon (?). The second section, "All Records Retrieved from Database", has a minus sign icon and a list of patch bulletins. The bulletins are: HPSBUX0001-108, HPSBUX0001-109, HPSBUX0005-113, HPSBUX0005-114, HPSBUX0007-117, and HPSBUX0008-118. Each bulletin has a checkbox to its left.

Click any of the available criteria check boxes to select the criteria you would like to use in your filter. For additional information on creating filters refer to the *HPCA Reporting Server Guide*.

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. Compliance reports show only the information applicable to detected devices in your environment.

- **Compliance by Device**

Use this report to see the vulnerabilities for devices under Client Automation patch management. The date of the last scan is listed in the last column. Each row contains information relating to a specific device and an icon.

- A check mark indicates all applicable vulnerabilities have been patched.
- 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.

- 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.

Compliance by Devices										
15 items										
1 - 3 of 3 items										
Details	Status	Device	Last Scanned	Applicable Products	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending
		VMXPSP1	2005-11-18 21:00:44	5	33	0	0	33	0	0
		sunpatch10	2005-11-07 19:21:40	1	29	33	0	0	0	0

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 patches that were installed.
- 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.
- 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.
- Click the number in the Total column to see all patches that are relevant to this device.

- **Simplified Compliance by Device**

Use this report to see the vulnerabilities for devices under Client Automation patch management. This report is the same as the Compliance by Devices report, discussed on page 95, except that its limited filtering options provide for quicker response times. It only supports filtering for Patch Compliance Status and Device Name. To apply additional filters, use the Compliance by Device Report.

simplified Compliance by Devices											
				15 items		1 - 15 of 9109 items					
Details	Status	Device	Last Scanned ↓	Applicable Products	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending	Total
		WS2K23VW782	2005-03-01 09:52:06	10	28	11	9	8	0	0	28
		WS2K237YB75	2004-12-25 10:38:23	10	28	12	7	9	0	0	28

- For each device, you can perform the same operations as discussed with the **Compliance by Device** report, on page 95.

- **Compliance by Bulletin**

Use this report to see the vulnerabilities listed by bulletin. 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 device will display with a red X to show.

- 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.

Status	Bulletin	CVE	Title	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pending	Total
⚙️	MS04-040	CAN-2004-1050	Cumulative Security Update for Internet Explorer (889293)	25	2	0	22	0	1	2
❌	MS04-030	CAN-2004-0718	Vulnerability in WebDav XML Message Handler Could Lead to a Denial of Service (824151)	8120	268	0	7852	0	0	268
❌	MS04-031	CAN-2004-0206	Vulnerability in NetDDE Could Allow Remote Code Execution (841533)	8120	438	0	7682	0	0	438
⚙️	MS04-032	CAN-2004-0207	Security Update for Microsoft Windows (840987)	8126	6871	0	1254	0	1	6871

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 a title in the Title column to see all patches for that bulletin.
- 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.
- Items in the Reboot Pending column represent patches that will be complete after the device is rebooted.
- Click the number in the Total column to see all patches that are relevant to this bulletin.

- **Compliance by Products**

This report displays one row for each product. For each product, you can

- Click the number in the Applicable Devices column to see the devices affected by the vulnerability.
- Click the number in the Applicable Bulletins column to see bulletins for the product.
- View detected vulnerabilities.

Compliance by Products										
		15 items		1 - 7 of 7 items						
Status	Product	Applicable Devices	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending	Total	
✗	.NET Framework 1.1	1	1	0	0	1	0	0	1	
✗	Internet Explorer 6	1	2	0	0	2	0	0	2	
✗	Outlook Express 6.0	1	1	0	0	1	0	0	1	
✓	Solaris Version 10 SPARC	1	29	33	0	0	0	0	33	
✓	Solaris Version 9 SPARC	1	202	218	0	0	0	0	218	
✗	Windows Messenger 4.7	1	1	0	0	1	0	0	1	
✗	Windows XP Professional	1	28	0	0	28	0	0	28	

- **Compliance by Releases**

This report lists products by release. There is one row for each release of each product. Click to see Applicable Bulletins.

Compliance by Releases									
				15 items	1 - 7 of 7 items				
Status	Product	Release ↑	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗	.NET Framework 1.1	.NET Framework 1.1 Gold	1	0	0	1	0	0	1
✗	Outlook Express 6.0	Internet Explorer 6 SP1	1	0	0	1	0	0	1
✗	Internet Explorer 6	Internet Explorer 6 SP1	2	0	0	2	0	0	2
✓	Solaris Version 10 SPARC	Solaris Version 10 SPARC	29	33	0	0	0	0	33
✓	Solaris Version 9 SPARC	Solaris Version 9 SPARC	202	218	0	0	0	0	218
✗	Windows Messenger 4.7	Windows Messenger 4.7 Gold	1	0	0	1	0	0	1
✗	Windows XP Professional	Windows XP Service Pack 1	28	0	0	28	0	0	28

- **Compliance by Patches**

This report lists products by patch. There is one row for each patch. Click to see Applicable Products and Applicable Devices.

Compliance by Patches

15 items

1 - 15 of 15 items

Status	Name	CVE	Patch Name	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pending	Total
<div></div>	MS07-053	C100860D9741_C00514A851C1_2		1	1	0	0	0	0	1
<div></div>	MS07-050	C100860D63C1_C00514A851C1_16		1	0	0	1	0	0	1
<div></div>	MS07-050	C100860D63C1_C00514A852C3_11		1	0	0	1	0	0	1
<div></div>	MS07-047	C100860CFBC0_C00514A851C1_4		1	0	0	1	0	0	1
<div></div>	MS07-047	C100860CFBC0_C00514A852C3_2		1	0	0	1	0	0	1
<div></div>	MS07-046	C100860CF1C2_C00514A851C1_6		1	0	0	1	0	0	1

- **Compliance Device Errors**

This report provides details for 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 on page 104.

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.

- **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.

Research by Bulletin								
15 items 1 - 15 of 435 items								
Name	CVE	Title	Source	Posted	Revised	Applicable Products	Applicable Patches	
HPSBUX0001-108		AudioSubsystem July 2001 Periodic Patch	HPUX	20010817	20010817	1	1	
HPSBUX0001-109		AudioSubsystem July 2001 Periodic Patch	HPUX	20010817	20010817	1	1	
HPSBUX0005-113		patch for shutdown(1M)	HPUX	20000420	20000420	1	1	
HPSBUX0005-114		Bind 4.9.7 components	HPUX	20030708	20030708	1	1	
HPSBUX0007-117		ftpd(1M) and ftp(1) patch	HPUX	20041222	20041222	1	1	
HPSBUX0008-118		cumulative newgrp(1) patch	HPUX	20040217	20040217	1	1	
HPSBUX0008-119		OV NNM6.1 Consolidated Patch 4	HPUX	20010906	20010906	1	1	
HPSBUX0009-121		OV NNM6.1 Consolidated Patch 4	HPUX	20010906	20010906	1	1	
HPSBUX0009-122		OV NNM6.1 Consolidated Patch 4	HPUX	20010906	20010906	1	1	

- **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.

Research by Devices			
15 items 1 - 3 of 3 items			
Device	Last Scanned	Applicable Products	Applicable Bulletins
VMXPSP1	2005-11-18 21:00:44	5	42
sunpatch10	2005-11-07 19:21:40	1	32

- **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.

Research by Patches											
15 items 1 - 15 of 1434 items											
Number	Bulletin	CVE	Lang	Product / Release	Probe	Down	Super	Arch	Status	Size (bytes)	Date
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Professional / Windows 2000 Service Pack 4	i	▼	N		0	1,417,720	2005-10-07 07:54:53
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Server / Windows 2000 Service Pack 4	i	▼	N		0	1,417,720	2005-10-07 07:54:53
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Advanced Server / Windows 2000 Service Pack 4	i	▼	N		0	1,417,720	2005-10-07 07:54:53
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Datacenter Server / Windows 2000 Service Pack 4	i	▼	N		0	1,417,720	2005-10-07 07:54:53

- **Research by Products**

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

Research by Patches											
Number	Bulletin	CVE	Lang	Product / Release	Probe	Down	Super	Arch	Status	Size (bytes)	Date
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Professional / Windows 2000 Service Pack 4			N		0	1,417,720	2005-10-07 07:54:53
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Server / Windows 2000 Service Pack 4			N		0	1,417,720	2005-10-07 07:54:53
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Advanced Server / Windows 2000 Service Pack 4			N		0	1,417,720	2005-10-07 07:54:53
896424	MS05-053	CAN-2005-2123	en	Windows 2000 Datacenter Server / Windows 2000 Service Pack 4			N		0	1,417,720	2005-10-07 07:54:53

- **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					
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 now delete Patch Manager compliance data for specific devices using the Patch Administrator. To remove compliance data from the Patch Manager ODBC database, click **Delete Devices** under Operations.

Figure 19 Delete devices



Specify the device criteria below

? Device Name(s):

? Days since last scan:

Next > Cancel

Enter 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.

The Patch Manager Administrator allows you to preview the devices that match the selection filters before removing them from the database. Click **Delete** to remove the devices from the Patch Manager ODBC database.



Once this operation is performed it 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. See 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.

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 the **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.
- 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.

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.

Notes for Solaris:

The Patch Manager Agent will not apply a Solaris patch which conflicts with a currently installed Solaris patch.

The management of a Solaris patch may require an immediate reboot to complete patch installation. As a result, the machine running the Patch Manager Agent may require a number of successive reboots to install all pre-requisite patches required by a Sun Alert.

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
```



To deploy Solaris patches, the `catexp` parameter must be set to `runmode:automatic` on your `radskman` line in the agent connect.

For more information on radskman, refer to the *HPCA 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 three new attributes. The three new patch descriptor xml attributes are:

- **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.

- **ReportThreshold**

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, 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 purposes 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 if the file or registry key exists.
 - Use state !E (does not exist) if your only criterion for status is if 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 meet 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.

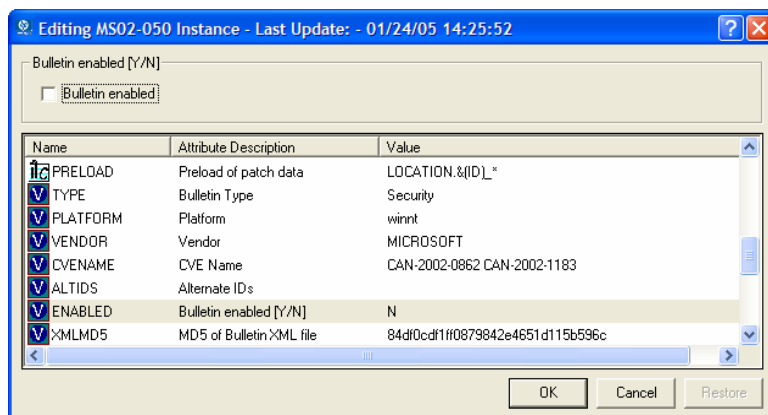
- 3 Set a REPORT threshold. The properties of the file or registry key will be sent to the Patch Manager based on this value. If the return code is greater than or equal to the value of the REPORT attribute, the file and registry information will be sent to the Patch Manager and will be available in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

Disabling Vulnerability Detection and Deployment

You may want to disable the detection or deployment of a specific 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 20 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 only want to disable 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.

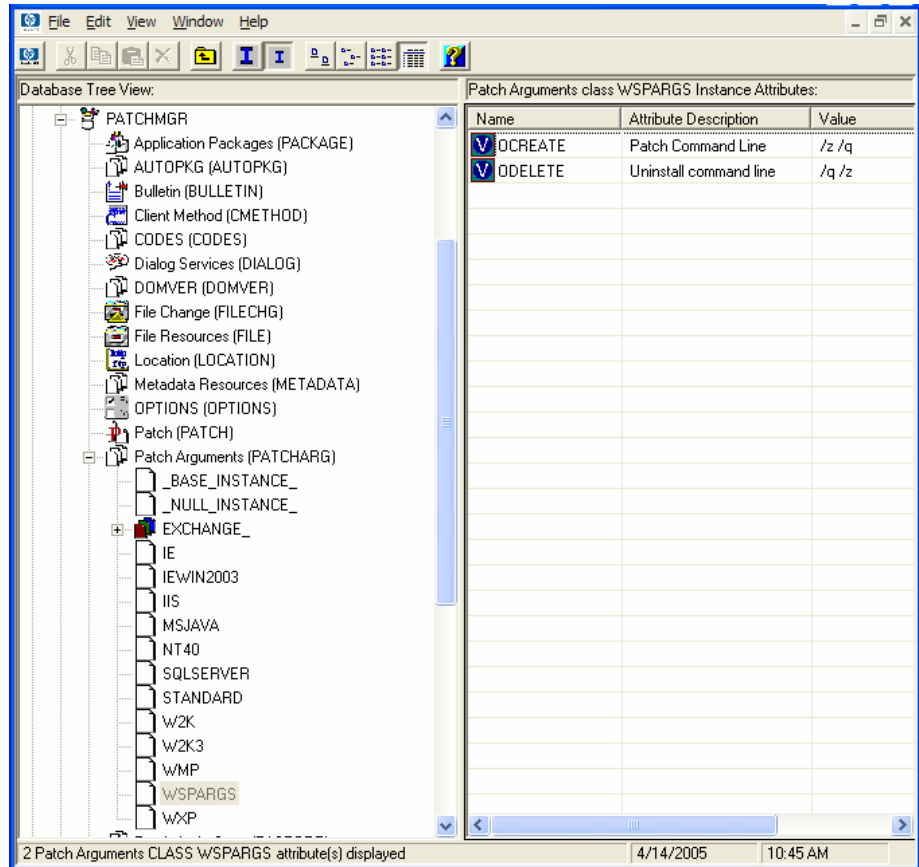


PATCHARG options apply only to patches downloaded using **MSSECURE.XML** not Microsoft Update. When patches are acquired from Microsoft Update, the **Source** column in the report will show "Microsoft Update" instead of "Microsoft".

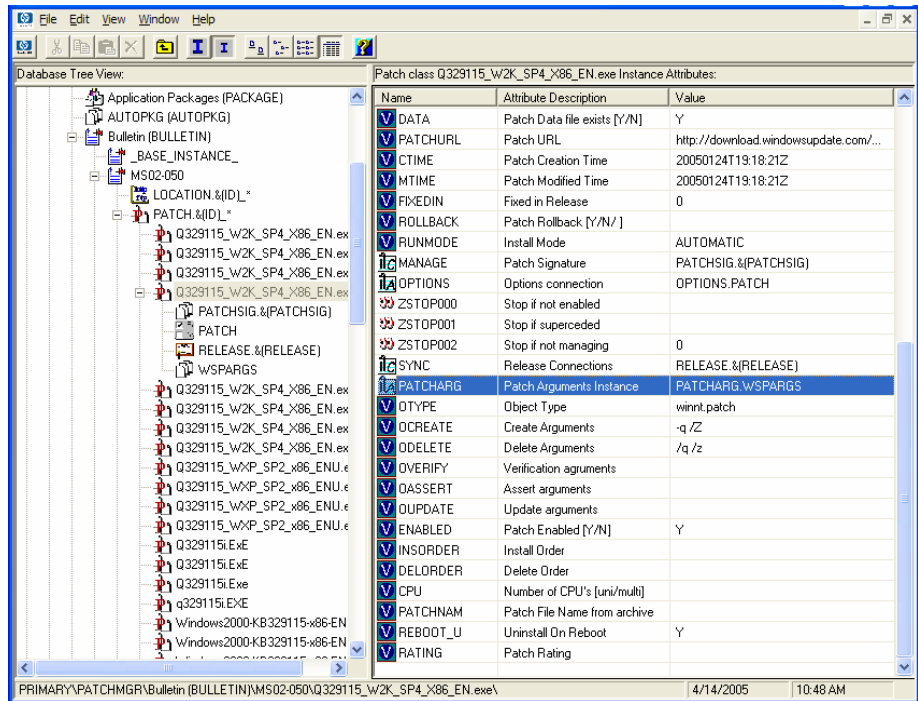
You may want to change the command line parameters for installing and uninstalling the patch file. To do this, use the **PATCHARG** class to create an instance and connect it to the appropriate patch file.

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 figure below.



- 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.



5 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 both 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, if you wanted to preload only the MS03-039 bulletin, you would 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 (HPCA 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.

At the time of this writing, Patch Manager does not support removal of HP-UX patches or HP-UX patch bundles.



Acquisition and deployment of HP-UX patch bundles is not supported. Acquisition does not automatically acquire HP-UX security patch pre-requisites, nor will the deployment of a HP-UX security patch install pre-requisite patches if they are missing on the agent. Roll back of HP-UX security patches is not supported.

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.

Roll back of Solaris patches is supported if roll back of the patch is supported by the patch vendor, *and* the roll back of the patch does not conflict with another patch's pre-requisite requirements. By default, patch roll back capabilities are disabled. See [Removing a Patch](#) on page 112 for additional information.

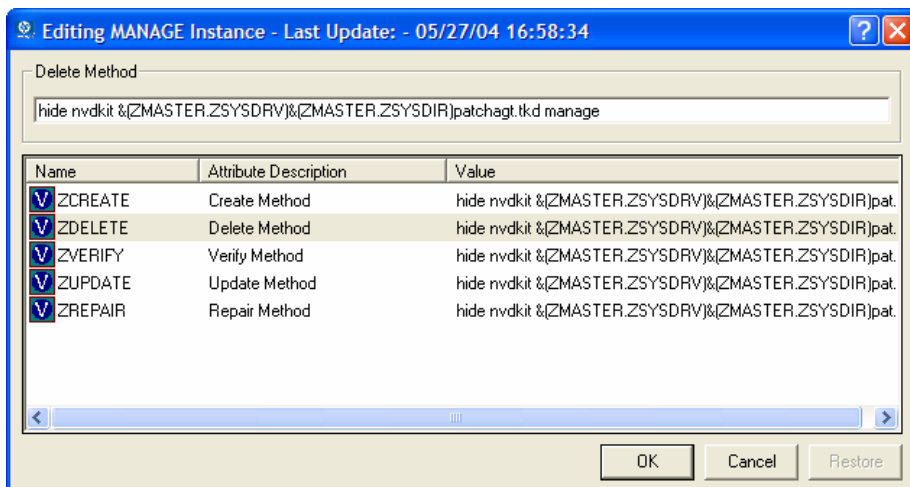
To remove a patch when a user is no longer assigned the service

- 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.

3 In the text box, type:

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



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

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

6 The Patch Manager Agent must make a connect 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 21 below.

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 21 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_7BCAD659FA326D4979A3CE9034300EA83A30F5EC.EXE"
        Architecture="" Reboot="Y" InstallCmdline="-q /Z" Language="en"
        MSSUSName="com_microsoft.810833_W2K_SP4_5936" SuperscededByBulletin=""
        SuperscededByMSPatch="" OSVersion=""
        MSSecureName="Q810833_W2K_SP4_X86_EN.exe" ObjectType="winnt.patch"
        QNumber="810833" ProbeCmdline="" Supersceded="N" OSType="" OSSuite=""
        Platform="winnt" UninstallCmdline="">
```

Bulletin Node

Node name: Bulletin

Parent node: None

Children: Products

Table 3 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, HP, Sun Solaris, 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, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
Source	SOURCE	Source [MICROSOFT NOVADIGM CUSTOM HPUX SOLARIS REDHAT SUSE] Directory from which the patch descriptor file was published.
Vendor	VENDOR	MICROSOFT/HPUX/SOLARIS/REDHAT/SUSE

XML Tag	HPCA Attribute	Description
Type	TYPE	Type of Bulletin Security/ServicePack/Other
Platform	PLATFORM	winnt/hpux/solaris/redhat/suse
Name	NAME	External ID Source: MSSECURE.XML, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
Title	TITLE	Title Bulletin title. Source: MSSECURE.XML, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
DatePosted	POSTED	Bulletin Posted On Date the bulletin was posted in YYYYMMDD format. Source: MSSECURE.XML, HP, Sun Solaris, 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.
	CTIME	Time the instance was created in the CSDB.
	ID	Internal instance ID.
HPPosted	HPPOSTED	Date the bulletin was initially posted by HP.
HPRevised	HPREVISED	Date the bulletin was revised by HP.

XML Tag	HPCA Attribute	Description
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 4 XML Tags in the PRODUCT class

XML Tag	HPCA Attribute	Description
Name	NAME	Source: MSSECURE.XML, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
FixedInRelease	FIXEDIN	Source: MSSECURE.XML

Releases Node

Node name: Releases
Parent node: Product
Children: Release
Attributes: None

Release Node

Node name: Release
Parent node: Releases
Children: Patch

Table 5 XML Tags in the RELEASE class

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

Patch Node

Node name: Patch
Parent node: Release
Children: Package

Table 6 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, HP, Sun Solaris, 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, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
Architecture	ARCH	x86 i64 Source: MSSECURE.XML/SUS, HP, Sun Solaris, 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
SupercededByBulletin	SUPERBU	The bulletin name that supersedes this patch. Source: MSSECURE.XML, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
SupercededByMSPatch	SUPERMSS	The MSSECURE patch name that supercedes this patch. Source: MSSECURE.XML

XML Tag	HPCA Attribute	Description
Superceded	SUPERCED	Specifies if the patch has been superseded. Valid values are Y or N. Source: MSSECURE.XML, HP, Sun Solaris, 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,hpux,solaris,redhat,suse
InstallCmdline	OCREATE	This is the arguments that are passed to the create procedure. Source: SUS, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds
VerifyCmdline	OVERIFY	The Verify Arguments.
UninstallCmdline	ODELETE	The Uninstall Arguments.

XML Tag	HPCA Attribute	Description
ObjectType	OTYPE	<p>Format: namespace=script filename Default: winnt.patch</p> <p>This specifies the type of the object and the name of the script file that would have the following procedures defined</p> <p>verify create delete assert</p> <p>The procedures should have the namespace as part of the name, e.g., winnt.patch::create.</p> <p>If the script filename is not specified then the filename is {namespace}.tcl.</p> <p>Source: Novadigm</p>
ProbeCmdline	OVERIFY	<p>The probe command line.</p> <p>Source: Novadigm</p>
	ID	<p>The unique ID created in the HPCA-CSDB for this patch.</p>
	PATCHSIG	<p>The name of the Patch Signature instance.</p> <p>Source: Novadigm</p>
	LOCATION	<p>The name of the LOCATION instance that contains the patch data.</p>
	BULLETIN	<p>The bulletin name set during publishing.</p> <p>Source: MSSECURE.XML, HP, Sun Solaris, Red Hat Network, Novell (SuSE) data feeds</p>

XML Tag	HPCA Attribute	Description
	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

Children: None

Table 7 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
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

XML Tag	HPCA Attribute	Description
	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 8 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

XML Tag	HPCA Attribute	Description
		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
	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
	USE	Not used. Source: Novadigm

HPFileset Node

Node name: HPFileset

Parent node: PatchSignature

Children: None

Table 9 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.

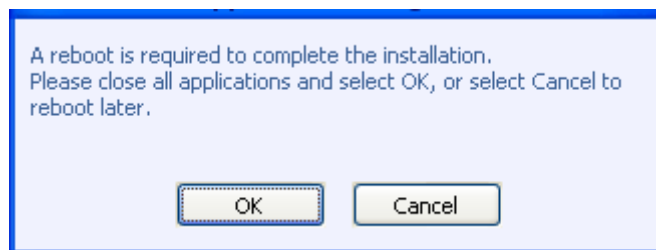
- **OK and Cancel Button (Y)**

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.

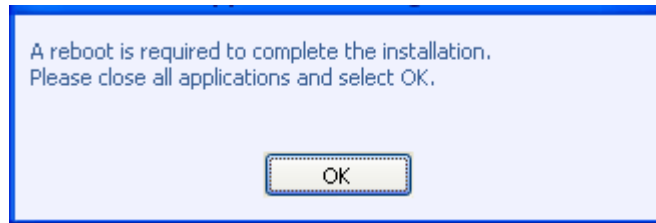
For example, the default Reboot panel displays both an OK and Cancel as shown in the figure below.

Figure 22 View the default reboot panel.



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 23 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 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 format:

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

Where the DOMAIN NAME is the value passed in `dname` by RADISH. In the case of an 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 as denoted by the use of "!". 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 and `oracle` for Oracle. `Mssql` is the default value. 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 **ftp://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 long in 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, and 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.
- **hpux_patch_url:** Specify the HP-UX url for downloading the patches. This is the same as the `hpux_patch_url` parameter in `patch.cfg`. The default is **ftp://ftp.itrc.hp.com/**.
- **hpux_url:** Specify the url for the data source used to assess HP-UX security vulnerabilities. This is set in the `hpux_url` parameter in `patch.cfg`. The default is **http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=security_catalog2.gz**
- **hpux_xml_url:** Specify the url for the file containing data on every HP-UX patch. This is set in the `hpux_xml_url` parameter in `patch.cfg`. The default is **http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=patches.xml**
- **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.

Http_timeout is displayed in the `setup.tsp` page in seconds. 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, you would 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`**.
- **nvdn_url:** Specify the URL to connect to the Patch Update web site provided by HP. This is the same as the nvdn_url parameter in `patch.cfg`. The default is **`http://managementsoftware.hp.com/Radia/patch_management/data`**.
- **purge_errors:** Specify how long in 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, and 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. Default: 7.
- **rds_pass:** If authentication has been enabled on your Configuration Server, specify the password for the rds_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 3ES on x86 devices, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/3es`.
- For Red Hat Enterprise Linux 3ES on x86-64 devices, place the baseline operating system rpm files supplied on Red Hat installation media in `data/patch/redhat/packages/3es-x86_64`.

When naming the `data/patch/redhat/packages/` subdirectories, refer to the list of **OS Filter Architecture** values on page 39. 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`**.
- **solaris_patchpro_base_url:** This parameter defines the directory repository for Sun Solaris meta data files. The default is **`https://patchpro.sun.com/database/`**.
- **solaris_patchpro_db_url:** This url provides meta data concerning Sun Solaris “available” patches. The default is **`https://patchpro.sun.com/database/patchdb.zip`**.
- **solaris_patchpro_jar_url:** This auxiliary file is used by Sun Patch Manager Version 2.0 to perform patch applicability and vulnerability assessment. The default is **`https://patchpro.sun.com/database/detectors.jar`**.

- **solaris_patch_url**: This url provides a reference to the download locations of signed Sun Solaris patches. The default is **http://sunsolve.sun.com/search/pdownload.pl?target=%s&method=hs**,
- **solaris_pdiag_url**: This file includes information on all patches, both security and non-security related. This url provides a list of all Sun Solaris patches as well as meta data concerning Sun Solaris version applicability and the type of patch (recommended or security).The default is **http://sunsolve.sun.com/pub-cgi/pdownload.pl?target=patchdiag.xref**.
- **solaris_sunalerts_url**: This url provides a list of all available Sun Alerts and the patch ids associated with each Sun Alert. The default is **http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches**.
- **suse_pass**: Specify the password Novell web site hosting SuSE patches.
- **suse_urls**: Specify the urls for Novell web site hosting SuSE patches. The defaults are:
 8:
 {https://you.novell.com/update/i386/update/SuSE-SLES/8/}
 9:
 {https://you.novell.com/update/i386/update/SUSE-CORE/9/}
 {https://you.novell.com/update/i386/update/SUSE-SLES/9/}
 8-x86_64:
 {https://you.novell.com/update/x86_64/update/SuSE-SLES/8/}
 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 hosting SuSE 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 `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 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`.
 - HP-UX Security bulletins use the naming convention `HPSBUX#####`, where `HP` indicates HP hardware, `SB` indicates security bulletin, and `UX` indicates the HP-UX operating system. At times the HP-UX security bulletin may contain an embedded hyphen
 - 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 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.
- Sun Solaris Sun Alerts use the naming convention `SUNALERT-number`, where `number` represents the specific Sun Alert ID number, which can be found on the following web page:
- http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches

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*,!Pr
oject 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.
- **superceded_patches:** Set superceded_patches to Y if you want to publish the data even if a patch is marked as superceded. 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 filters for x86_64 architectures use the format :
vendor::operatingsystem-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::10

- HP-UX examples: HP-UX::11.00, HP-UX::11.11, HP-UX::11.23
- 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 rpadmin -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 ↵
-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 ↵
-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 79. 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`, `suse`, and `hpux`. Note that RedHat, SuSE, Solaris, and HP-UX agent updates are only available starting with version 2.0.

- **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 7.2
    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 {7.20.000}
}
```

Index

A

- acquire command, 64
- Acquire Microsoft Patches acquisition setting, 62
- Acquire RedHat Patches acquisition setting, 62
- acquisition settings, 60
- agent_os parameter, 80
- agent_version parameter, 80
- Applicable Bulletins column, 96, 99, 102
- Applicable Devices column, 98, 99
- Applicable Patches column, 100
- Applicable Products column, 96, 101
- ARCH attribute, 120
- arch parameter, 141
- Architecture tag, 120
- automatic patch, definition, 105
- AUTOPKG class, 79
- AUTOPKG.PATCH instance, 79

B

- bandwidth optimization, 82
- Browse by Bulletin, 100
- Browse by Device, 101
- Browse by Patch, 101
- Browse by Product, 101
- Browse by Release, 102
- BULLETIN attribute, 122
- Bulletin column, 98
- Bulletin node, 115
- bulletin, definition, 14
- Bulletins acquisition setting, 60

- bulletins parameter, 141

C

- catexp parameter, 105
- CHECKSUM attribute, 124
- Checksum tag, 124
- Compliance and Research Exception Reports, 102
- compliance assessment, 12
- Compliance by Bulletin, 97
- Compliance by Device, 95
- Compliance by Patches, 100
- Compliance by Product, 99
- Compliance by Release, 99
- compliance data
 - removing, 103
- Compliance Device Errors, 100
- compliance reports, 95
- config parameter, 142
- Configuration Server Component Updates, 24
- Configuration Server Database Updates, 24
- Configuration Server Database, synchronizing, 44
- CRC32 attribute, 124
- CRC32 tag, 124
- CTIME attribute, 117
- custom xml file, creating, 106
- customer support, 6
- CVE column, 98, 101

D

- DATA attribute, 123
- data_dir parameter, 135, 142

- databases
 - synchronizing manually, 144
 - synchronizing with an Oracle database, 144

- DatePosted tag, 117

- DateRevised tag, 116

- db_type parameter, 135

- deployment, 12

- Deployment tag, 118, 123

- descriptor file, creating, 64

- DesiredState attribute, 106

- DISCOVER_PATCH instance, 32, 145

- DISCOVER_PATCH Service, 79

- dsn parameter, 136

- dsn_pass parameter, 136

- dsn_user parameter, 136

- DSTATE

- valid values, 108

- DSTATE attribute, 106, 123, 124, 126

E

- exclamation point, 96

F

- FAQURL attribute, 116

- FAQURL tag, 116

- FILECHG class, 106

- FILECHG instance, 107

- FileChg node, 124

- filter bar, 100

- filtering patch reports, 94

- FINALIZE_PATCH, 104

- FIXEDIN attribute, 118

- FixedInRelease tag, 118

- Force acquisition setting, 61

- force parameter, 142

- ftp_proxy_pass parameter, 136

- ftp_proxy_url parameter, 136

- ftp_proxy_user parameter, 136

G

- GMTDATE attribute, 124

- Gmtdate tag, 124

- GMTTIME attribute, 124

- Gmttime tag, 124

H

- hard reboot, 128

- history parameter, 136

- HPCA Core, 14

- HPCA Satellite, 14

- HPFileset node, 126

- HPPOSTED attribute, 117

- HPPosted tag, 117

- HPREVISD attribute, 117

- HPRevised tag, 117

- HPUX Security bulletins, 60

- http_proxy_pass parameter, 136

- http_proxy_url parameter, 136

- http_proxy_user parameter, 137

- http_timeout parameter, 31, 137

I

- ID attribute, 117, 122

- impact analysis, 12

- IMPACT attribute, 116

- ImpactSeverityID tag, 116

- Install Agent task, 72

- install.ini file, 73

- InstallCmdline tag, 121

- interactive patch, definition, 105

L

LANG attribute, 120
lang parameter, 137
Language tag, 120
LDAP directory, 15
LOCATION attribute, 122

M

magnifying glass, 96
Microsoft Automatic Updates, 53
Microsoft feed settings, 37
Microsoft MSDE, 96, 98
Microsoft Office Bulletins

- best practices, 84
- best practices with Microsoft Update Catalog, 88
- detecting and managing, 83
- enabling in Patch Manager, 84, 89

Microsoft Security bulletins, 60
Microsoft SQL server, 18, 96, 98
Microsoft SQL Server

- supported versions, 18

microsoft_sus_url parameter, 137
microsoft_url parameter, 137
MITIGATE attribute, 116
MitigateSeverityID tag, 116
Mode acquisition setting, 61
mode parameter, 142
MSSECURE.XML file, 37
MSSecureName tag, 121
MSSNAME attribute, 121
MSSUSName tag, 120
MTIME attribute, 117
multiple reboot events, 131

N

NAME attribute, 117, 118, 119, 124, 125, 126

Name tag, 117, 118, 119, 124, 125, 126
no reboot, 128
Not Patched column, 97, 99
not-patched status, 96
nvd_attributename attribute, 44
nvd_classname table, 44
nvdm_url parameter, 137

O

O/S Filter acquisition setting, 39
ObjectType tag, 122
OCREATE attribute, 109, 121
ODELETE attribute, 109, 121
OPTIONS class, 106
OPTIONS instance, 107
Oracle

- roles and system privileges, 22

Oracle Patch database, creating, 21
Oracle Patch database, failed connection, 21
OSSUITE attribute, 121
OSSuite tag, 121
OSTYPE attribute, 121
OSType tag, 121
OSVER attribute, 121
OSVersion tag, 121
Other column, 97, 99
OTYPE attribute, 122
OVERIFY attribute, 121, 122

P

passport registration, 6
patch

- definition, 14
- removing, 112

Patch Acquisition Reports, 67

- summary by bulletin, 68

- summary by session, 67
 - summary of errors, 68
- patch analysis, 92
- patch descriptor file, 49
- patch discovery, performing, 82
- Patch Manager
 - components
 - Patch Manager Agent, 15
- Patch Manager
 - components, 14
 - features
 - compliance assessment, 12
 - deployment, 12
 - impact analysis, 12
 - pilot testing, 12
 - vulnerability assessment, 12
- Patch Manager
 - components
 - Administrator CSDB Editor, 15
- Patch Manager
 - reports
 - Patch Acquisition
 - Summary, 67
- Patch Manager
 - reports
 - compliance, 95
- Patch Manager
 - reports
 - Compliance
 - by Device, 95
- Patch Manager
 - reports
 - Simplified Compliance
 - by Device, 97
- Patch Manager
 - reports
 - Compliance
 - by Bulletin, 97
- Patch Manager
 - reports

- Vulnerability Assessment
 - by Product, 99
- Patch Manager
 - reports
 - Vulnerability Assessment
 - Compliance
 - by Release, 99
- Patch Manager
 - reports
 - Vulnerability Assessment
 - Compliance
 - by Patches, 100
- Patch Manager
 - reports
 - Compliance Device Errors, 100
- Patch Manager
 - reports
 - Research, 100
- Patch Manager
 - reports
 - Research
 - Browse by Bulletin, 100
- Patch Manager
 - reports
 - Research
 - Browse by Device, 101
- Patch Manager
 - reports
 - Research
 - Browse by Patch, 101
- Patch Manager
 - reports
 - Research
 - Browse by Product, 101
- Patch Manager
 - reports
 - Research
 - Browse by Release, 102

- Patch Manager
 - reports
 - compliance, 103
- Patch Manager Agent
 - installing from HP Client Automation media, 73
 - installing from HP Client Automation Media, 74
- Patch Manager Server
 - description, 15
 - installing, 24
 - System Requirements, 23
- Patch Manager settings file, 27
- Patch node, 119
- patch reports, 92
- Patch signature node, 123
- PATCHARGS class, 109
- patchdata, 21
- Patched column, 96, 98
- PATCHMGR domain, 44, 49
- PATCHOBJ instance
 - verifying, 26
- PATCHSIG attribute, 122
- patchtemp, 21
- PATCHURL attribute, 120
- PatchURL tag, 120
- PATH attribute, 124, 125
- Path tag, 124, 125
- pending reboot status, 96
- pilot testing, 12
- PLATFORM attribute, 117, 121
- Platform tag, 117, 121
- POPULAR attribute, 116
- PopularitySeverityID tag, 116
- Portal, description, 15
- POSTED attribute, 117
- PREREQ attribute, 116
- PreReqSeverityID tag, 116

- probe, definition, 64
- ProbeCmdline tag, 122
- Product node, 118
- product parameter, 143
- Products node, 118
- Proxy Server, preloading, 111
- purge_errors parameter, 137

Q

- QNUMBER attribute, 121
- QNumber tag, 121
- question mark, 96

R

- RadDBUtil, 65
- radskman, 82
- radskman command line, 105
- rds_pass parameter, 137
- rds_url parameter, 138
- rds_user parameter, 138
- reboot
 - modifiers, 127, 128
 - multiple events, 131
 - types, 127, 128
- REBOOT attribute, 120
- Reboot Pending column, 97, 99
- Reboot tag, 120
- Red Hat Security advisories, 60
- Red Hat systemid file, creating, 57
- red X, 96
- REGCHG class, 106
- REGCHG instance, 107
- RegChg node, 125
- Release node, 119
- Releases node, 119
- Replace acquisition setting, 61, 62

- replace parameter, 143
- report acquisition status, 63
- REPORT attribute, 106, 123, 125, 126
- REPORT threshold, 108
- reporting options, customizing, 107
- Reporting Server
 - filtering patch reports, 94
 - overview, 15
- reporting_url parameter, 138
- ReportThreshold attribute, 106
- Research Reports, 100
 - Browse by Bulletin, 100
 - Browse by Device, 101
 - Browse by Patch, 101
 - Browse by Product, 101
 - Browse by Release, 102
- retire parameter, 138
- REVISED attribute, 116
- rh_depends parameter, 139
- rhn_register tool, 57
- rhn_url parameter, 140
- RUNMODE attribute, 118, 123

S

- Schema Version tag, 117
- security advisory, definition, 14
- Simplified Compliance by Device, 97
- SIZE attribute, 124
- Size tag, 124
- soft reboot, 128
- Solaris Feed
 - required Sun Online Account, 40
- Solaris patches, 58
- SOURCE attribute, 116
- Source tag, 116
- SQL Patch database, creating, 20
- Sun Alert, 105

- Sun Online Account
 - how to obtain, 40
- Sun Solaris 10, 76, 77
- Sun Solaris 9, 75
- Sun Solaris Sun Alerts, 61, 142
- SUPERBU attribute, 120
- SUPERCED attribute, 121
- Superceded tag, 121
- superceded_patches parameter, 143
- SupercededByBulletin tag, 120
- SupercededByMSPatch tag, 120
- SUPERMSS attribute, 120
- support, 6
- SUPPORT attribute, 116
- Supported, 64, 116
- Supported tag, 116
- SuSE security patch acquisition, 59
- SuSE Security patches, 61
- SUSNAME attribute, 120
- sync parameter, 140
- systemid file, 57

T

- tablespace, creating, 21
- technical support, 6
- TITLE attribute, 117
- Title column, 98
- Title tag, 117
- Total column, 97
- Total link, 99
- TYPE attribute, 117, 125
- Type tag, 117, 125

U

- UninstallCmdline tag, 121

URL attribute, 116
URL tag, 116
USE attribute, 106, 123, 125, 126

V

VALUE attribute, 125
Value tag, 125
VENDOR attribute, 116
Vendor tag, 116
vendor_os_filter parameter, 143
vendors parameter, 143
VerifyCmdline tag, 121
VERSION attribute, 124
Version tag, 124
vulnerabilities
 assessing, 12

 managing, 103

W

Warning column, 96, 98
Windows Update Agent, 54

X

XML tags
 BULLETIN class, 116
 FILECHG class, 124
 PATCH class, 120
 PRODUCT class, 118
 REGCHG class, 125, 126
 RELEASE class, 119

Z

ZDELETE attribute, 112
ZSERVICE.REBOOT attribute, 127

