HP OpenView Patch Manager Using Radia

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

Software Version: 2.2

Installation and Configuration Guide

November 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

© Copyright 2004-2005 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

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.

Acknowledgements

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

This manual's title page contains the following identifying information:

- Version number, which indicates the software version.
- Print date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://ovweb.external.hp.com/lpe/doc_serv/

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 since the last released edition.

Table 1 Document Changes

Chapter	Version	Changes
All	2.2	Support has been added for Sun Solaris Operating System versions 9 and10 for the SPARC architecture. Information regarding Solaris has been added throughout this book.
Chapter 2	2.0.1	Page 22, Patch Manager Implementation Tasks: Patch Manager includes significant performance improvements to the Reporting Server patch reports. These improvements disable the patch reports rendered through the Radia Integration Server.
Chapter 2	2.0	Page 27, To install the Patch Manager Components: For version 2.0, the Patch Manager no longer includes an option for the installation of the Messaging Server.
Chapter 2	2.0	Page 31, Configuring the Patch Manager Server: The Radia Patch Administrator provides an interface to modify Patch Manager settings.
Chapter 2	2.2	Page 32, Configuration Server Settings: Use the Test Configuration Server Connection command to test connectivity to your Configuration Server.

Chapter	Version	Changes
Chapter 2	2.0	Page 32, Patch Manager Settings: The URL to connect to the Radia Patch Update web site provided by HP has changed to **http://managementsoftware.hp.com/Radia/patch_management/data**. This URL is the value for the nvdm_URL parameter in `patch.cfg`. Furthermore, the nvdm_user and nvdm_password parameters are not required for use with the new location.
Chapter 2	2.0	Page 34, Red Hat Feed Settings: Specify the URL and OS Filter for the Red Hat Network data feed using the Patch Manager Administrator. The OS Filter was added to the settings in Version 2.1. This URL is the value for the rhn_url parameter in `patch.cfg`.
Chapter 2	2.0.1	Page 35, SuSE Feed Settings: This version of the Patch Manager supports SuSE Linux Enterprise Server Versions 8 and 9. Specify the URL and operating systems. The OS Filter was added to the settings in Version 2.1.
Chapter 2	2.1	Page 35, HP-UX Feed Settings: This version of the Patch Manager supports HP-UX Versions 11.00 and 11.11.
Chapter 2	2.2	Page 36, Solaris Settings: This version of the Patch Manager supports Solaris versions 9 and 10 for the SPARC architecture.
Chapter 2	2.2	Page 39, Patch Agent Settings: A checkbox was added for Solaris. Checkboxes for Linux and HP-UX were added in 2.1.
Chapter 2	2.0	Page 39, Reporting Settings: Specify the location of the Reporting Server in the Patch Manager Administrator. Click the Reporting icon in the Patch Manager Administrator to view Patch Reports. This URL is the value for the reporting_url parameter in `patch.cfg`.
Chapter 2	2.0.1	Page 33, ODBC DSN Settings: A new option has been made for Database Type, either Microsoft SQL Server or Oracle. This is the same as the db_type parameter in `patch.cfg`.
Chapter 2	2.2	Page 33, ODBC DSN Settings: Use the **Test ODBC Connection** command to test connectivity to your DSN.

Chapter	Version	Changes
Chapter 2	2.0.1	Page 41, See Table 2: The db_type option has been made for Database Type. Possible values are Microsoft SQL Server or Oracle.
Chapter 2	2.1	Page 42, See Table 2: The hpux_patch_url, hpux_url, and hpux_xml_url parameters have been added for HP-UX support.
Chapter 2	2.2	Page 46, See Table 2: Six new parameters have been added for Solaris support.
Chapter 2	2.0.1	Page 47, See Table 2: The suse_pass, suse_urls, and suse_user parameters have been added for SuSE support.
Chapter 3	2.2	Page 58, See Figure 3: Shows that security patches can now be acquired for Solaris.
Chapter 3	2.0.1	Page 68, SuSE Settings: Specify if you want to acquire SuSE Security Advisories.
Chapter 3	2.1	Page 68, HP-UX Settings: Specify if you want to acquire HP-UX Security Bulletins.
Chapter 3	2.2	Page 68, Solaris Settings: Specify if you want to acquire Solaris Security Bulletins.
Chapter 3	2.0	Page 70, See Table 4: Use ARCH to specify for which machine architectures you want to acquire patches.
Chapter 3	2.0	Page 77, See Table 4: Use SUPERCEDED_PATCHES to specify if you want to download the data for superceded patches.
Chapter 3	2.0	Page 78, See Table 4: Use VENDORS to specify for which vendors you want to acquire patches.
Chapter 3	2.0	Page 78, See Table 4: Use VENDOR_OS_FILTER to specify for which operating systems you want to acquire patches. This does not apply to Microsoft Operating systems, as Microsoft considers its operating systems products.
Chapter 3	2.0	Page 79, Patch Acquisition Reports: Patch Manager uses the Reporting Server for patch acquisition reports.

Chapter	Version	Changes
Chapter 4	2.0	Page 95, Updating the Patch Manager Client Agent: Use AGENT_OS to specify for which operating systems you want to get Patch Manager client agents updates.
Chapter 4	2.2	Page 95, Updating the Patch Manager Client Agent, Use View Agent Updates to see if there are any updates the client agent.
Chapter 4	2.0	Page 95, Updating the Patch Manager Client Agent: Use AGENT_VERSION to specify for which Patch Manager client version you want to get updates.
Chapter 4	2.1	Page 96, Detecting and Managing Microsoft Office Security Bulletins: Patch Manager has the ability to detect Microsoft Office vulnerabilities for installed Microsoft Office applications. It can also manage those vulnerabilities on locally installed Microsoft Office applications. Patch Manager does not support patch management for Office 95 and Office 97.
Chapter 4	2.0	Page 99, Patch Analysis and Reports: Patch Manager now uses the Reporting Server for patch compliance and research reports.
Chapter 4	2.0.1	Page 111, 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.
Chapter 4	2.0	Page 115, Deploying Automatic and Interactive Patches: Patch Manager can detect vulnerabilities for interactive and automatic patches. Use the catexp parameter of radskman if you want to limit deployment only to automatic patches.
Chapter 4	2.2	Page 111, Deleting Devices: Use the Delete Devices command to remove devices from the Patch Manager ODBC database.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

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

HP OpenView 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 valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction 13

HP OpenView Patch Manager Using Radia 14

Terminology 16

Radia Patch Management Components 16

Summary 19

2 Creating the Patch Manager Environment 21

Patch Manager Implementation Tasks 22

Creating the ODBC Patch Database 23

Installing the Administrator Workstation 25

Installing the Patch Manager Server 25

Configuring the Patch Manager Server 31

Configuration Server Settings 31

Patch Manager Settings 32

ODBC DSN Settings 33

Microsoft Feed Settings 33

Red Hat Feed Settings 34

SuSE Feed Settings 35

HP-UX Feed Settings 35

Solaris Settings 36

HTTP Settings 37

Acquisition History Settings 38

Patch Agent Settings 39

Reporting Settings 39

Default Settings 40

Patch Configuration Settings File 40

Database Synchronization 50

Adding a Method Connection 52

Messaging Server 52

Reporting Server 53

Configuration Analyzer Installation Tasks (Optional) 53
Installing and Configuring the Knowledge Base Manager (Optional) 53
Summary 55

3 Patch Acquisition 57

Radia Patch Acquisition 58
Patch Acquisition Overview 59
About Patch Descriptor (XML) Files 59
About Red Hat Patch Acquisition Prerequisites 61
About SuSE Patch Acquisition Prerequisites 63
About HP-UX Patch Acquisition 63
About Solaris Patch Acquisition 63
Performing a Patch Acquisition 64
Creating Custom Patch Descriptor Files 78
Patch Acquisition Reports 80
Analyzing Microsoft Patch Files 83
Summary 85

4 Patch Assessment and Analysis 87

Installing the Patch Manager Client 88
Sun Solaris Patch Agent pre-requisites 91
Sun Solaris 9 client OS pre-requisites 91
Sun Solaris 10 client OS pre-requisites 92
Sun Solaris Single User patch installations 92
Updating the Patch Manager client agent 93
Product Discovery and Analysis 95
Detecting and Managing Microsoft Office Security Bulletins 96
About ZOBJSTAT 98
Patch Manager Administrator Icons 98
Patch Analysis and Reports 99
Filtering Patch Reports with Reporting Server 100
Compliance Reports 103
Research Reports 108
Compliance and Research Exception Reports 111

Deleting Devices 111
Managing Vulnerabilities 112
Notes on Solaris Patch Management 113
Deploying Automatic and Interactive Patches 115
Customizing Reporting Options 116
Disabling Vulnerability Detection and Deployment 119
Controlling Patch Deployment (PATCHARG) 120
Preloading Proxy Server and Staging Servers 122
Removing a Patch 123
Summary 126

A Supported XML Tags for Patch Descriptor Files 127
Bulletin Node 128
Products Node 130
Product Node 130
Releases Node 131
Release Node 131
Patch Node 132
Patch Signature Node 136
FileChg Node 136
RegChg Node 137
HPFileset Node 138

B Restarting the Client Computer 141
Reboot Types 143
Reboot Modifier: Type of Warning Message 143
Reboot Modifier: Machine and User Options 145
Reboot Modifier: Immediate Restart 146
Specifying Multiple Reboot Events 146

C Policy Server Integration 147

Index.....149

1 Introduction

At the end of this chapter, you will:

- Know the capabilities of HP OpenView Patch Manager Using Radia (Patch Manager).

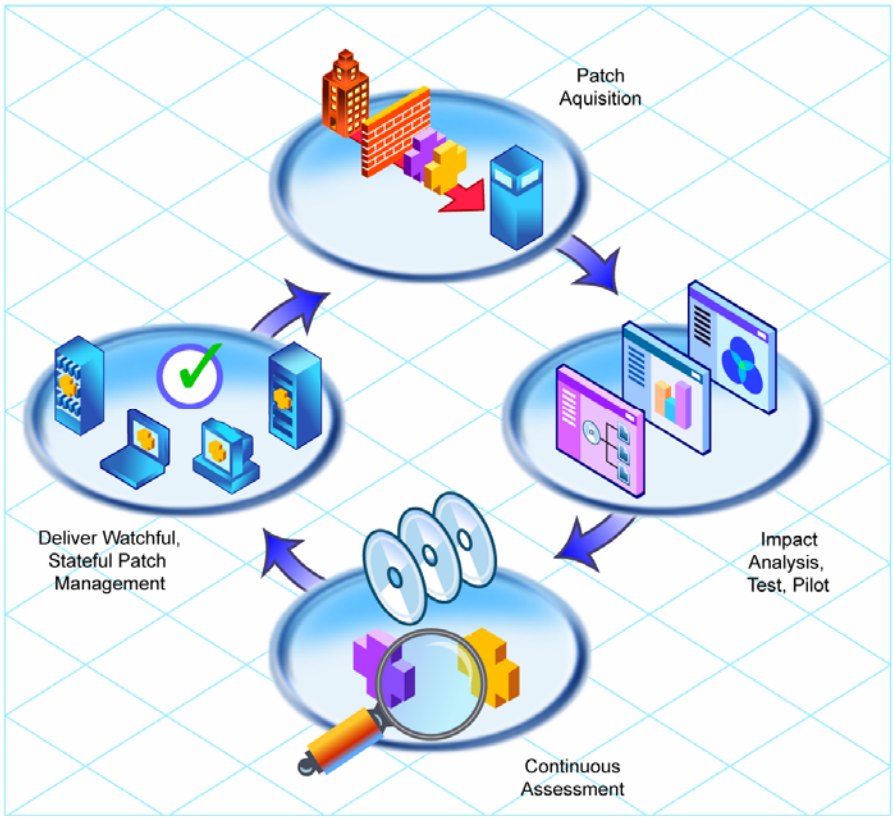
HP OpenView Patch Manager Using Radia

The 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 Radia Management Suite, which 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 patches and service packs directly from Microsoft, HP-UX, Red Hat, Solaris, and SuSE web-based depositories.
- **Impact Analysis and Pilot Testing**:
  identification of affected applications, devices, and users to determine configuration impact before security patches are deployed. Patch Manager also allows IT administrators to select target pilot groups based on usage or critical need. Radia is the only solution with these unique impact analysis and 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 collected security patches that are already applied to each software product, and identification of software products that the device actually executes. 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. Radia 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. In addition, if patches are corrupted in any way Radia provides self-healing for connected and disconnected users.

Figure 1 Patch Management life cycle



Terminology

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

bulletin or security advisory

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

patch

The patch is the actual file to be deployed and executed to fix the vulnerability. A bulletin can have multiple patches depending on affected products, platforms, architectures, and languages.

qnumber

A qnumber is equivalent to the ticket opened by Microsoft Support. One bulletin can have multiple qnumbers.

Radia Patch Management Components

Patch Manager uses existing components of the Radia Infrastructure in addition to the Patch Manager Server. The following Radia components are required:

- **HP OpenView Configuration Server Using Radia**
  Applications and information about the subscribers and client computers are stored in the Radia Database on the HP OpenView Configuration Server Using Radia (Configuration Server). The PATCHMGR domain in the Radia Database contains instances for patch management. The Configuration Server processes information received from the Patch Manager client. The Configuration Server manages vulnerabilities based on policies established by the Radia administrator using the System Explorer for the HP OpenView Administrator Workstation Using Radia (System Explorer). For more information, see the *User's Guide for the HP OpenView Configuration Server Using Radia (Configuration Server Guide).*
- **HP OpenView Management Portal Using Radia**
  Use the Management Portal to configure the Patch Manager Server and

deploy the Patch Manager client. The Management Portal is a module of the Radia Integration Server, and runs under the Radia Integration Server service. See the *Installation and Configuration Guide for the HP OpenView Management Portal Using Radia (Management Portal Guide)* for more information.

- **HP OpenView Patch Manager Server Using Radia**
  The Patch Manager Server acquires security patches from the Internet, loads them into the Radia Database, and then synchronizes them with an SQL or Oracle Database. The information on the patches and the vulnerabilities in your environment can be analyzed using Patch Manager reports. Patch Manager is a module of the Radia Integration Server, and runs under the Radia Integration Server service.
- **HP OpenView Patch Manager client Agent Using Radia**
  Install the Patch Manager client on devices for which you want to manage vulnerabilities. The client discovers products and patches on managed devices.
- **HP OpenView Reporting Server Using Radia**
  As part of the Radia extended infrastructure, the web-based Reporting Server allows you to query the combined data in existing Radia Inventory Manager, Patch Manager, and Radia Usage Manager 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 Radia SQL data for reporting and overall environmental assessment.
- **System Explorer for the HP OpenView Administrator Workstation**
  The Radia administrator uses the System Explorer to view and manage vulnerabilities stored in the Radia Database. For more information, see the *System Explorer Guide for the HP OpenView Administrator Workstation Using Radia (System Explorer Guide).*

You also have the option of using the HP Openview Configuration Analyzer Using Radia and HP OpenView Knowledge Base Manager Using Radia for the analysis and importing of state files. State files represent the current state of an application or a patch. Patch Manager provides a utility to create state files for Microsoft patches.

- **Configuration Analyzer**
  The Configuration Analyzer allows you to view, store, and compare Microsoft patches and application data. Application or Patch data are imported into the Configuration Analyzer in the form of state files. State files represent the current state of an application or a patch. The Patch

Manager can automatically generate state files for Microsoft patches. In addition, it allows you to not only analyze the contents of a patch, but also perform some cross analysis to verify how a patch may impact your environment or how a patch may intersect with another patch. See the *Installation and Configuration Guide for the HP OpenView Configuration Analyzer Using Radia* (*Configuration Analyzer Guide)* for more information.

- **Knowledge Base Manager**
  The Knowledge Base Manager performs automated import processing of Radia state files into a database allowing you to compare state files. See the *Installation and Configuration Guide for the HP OpenView Knowledge Base Manager Using Radia (Knowledge Base Manager Guide)* for more information.

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 version 2.0 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 Patch Manager environment.
- Know how to modify the Radia Database and Configuration Server.
- Be able to install the Patch Manager.

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 Microsoft SQL Server 2000 Service Pack 3a or greater. If using Oracle, the minimum database and driver version is Oracle 9i Release 2, patch set 2 (9.2.0.3). Unless otherwise noted, all components that are added to the Radia infrastructure are contained on the Patch Manager main CD-ROM.

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 Configuration Server. See the *Getting Started Guide for HP OpenView Using Radia.*
- ❑ Install the Messaging Server 3.0. See the *Messaging Server Guide*.
- ❑ Install the System Explorer. See the *System Explorer Guide.*
- ❑ Run the Patch Manager installation. This installation includes:
  - Modifying the Radia Database.
  - Modifying the Configuration Server executables.
  - Installing the Patch Manager Server.
  - Configuring Patch Manager to use your DSN.
  - Synchronizing the Radia Database with the SQL or Oracle Database.
- ❑ Add a Method Connection to your Radia Database.
- ❑ Install the Management Portal. See the *Management Portal Guide*.
- ❑ Install the Reporting Server 4.1.2. See the *Reporting Server Guide*.
- ❑ Optional: Install and configure the Configuration Analyzer.
- ❑ Optional: Install and configure the Knowledge Base Manager.

This version of Patch Manager includes significant improvement to the performance of Reporting Server patch reports. The change will cause Patch Manager reports rendered through the Radia Integration Server to be disabled. Compliance, Research, and Acquisition reports will be available through the Reporting Server Version 4.1.1 and above with the patch manager object pack applied.

Creating the ODBC Patch Database

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

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 `patchdata.dbf`
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 `patchtemp.dbf`
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	radiapatch
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)

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 Radia v4 Configuration Server CD-ROM contains a Radia Administrator installation. See the *Application Manager Guide* or the *Software Manager Guide* for more information on installation. Instructions for using the System Explorer can be found in the *System Explorer Guide*.

Installing the Patch Manager Server

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 may be installed on Windows 2000, Windows XP, or Windows 2003 Server. See the operating system's documentation for system requirements.

The Configuration Server Components and Radia Database 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.

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, minimum version 9.2.0.3, not those supplied by Microsoft.

If you have previously installed the Patch Manager, rename the `patch.cfg` file.

To install the Patch Manager Components

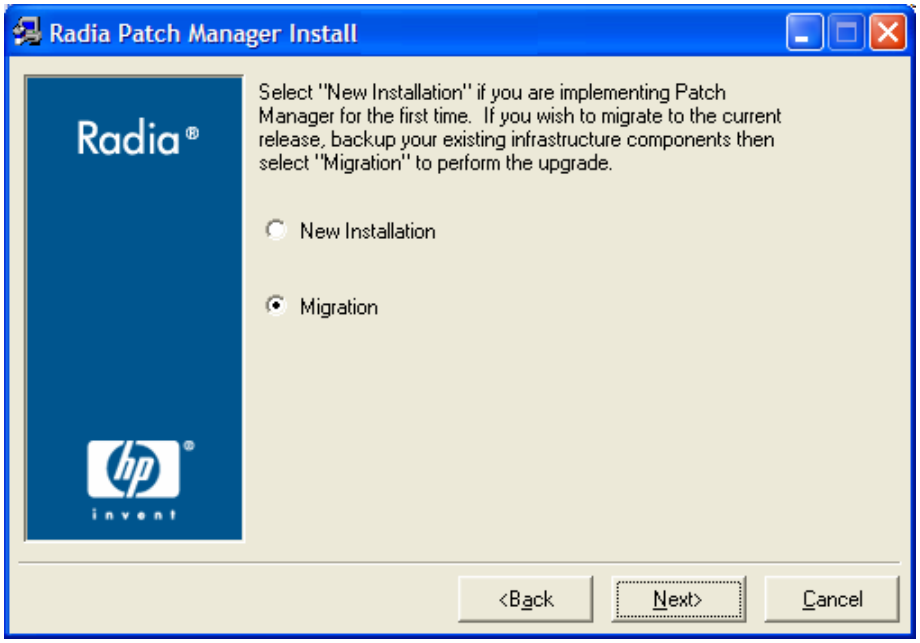
1 From the `extended_infrastructure\patch_manager_server\win32` directory on the Patch Manager installation media, double-click **setup.exe**.

The minimum build of nvdkit required for Patch Manager Version 2.2 is 159. This is included with the installation materials.

The Welcome window opens.

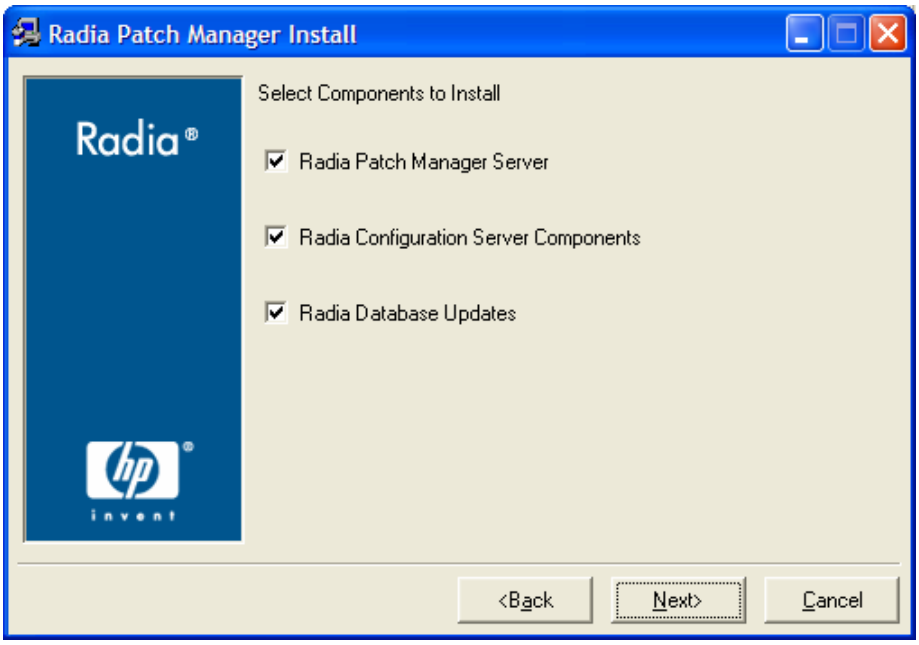
2 Click **Next**.

3 Click **Accept** for the HP Software License Terms.



4 Select **New Installation** if this is a new installation of the Patch Manager. If you want to migrate from Patch Manager Version 1.2, Release 1.2.2 to Patch Manager Version 2.0, select **Migration.** 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.



5 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 Radia Integration Server.

— **Configuration Server Components**
Installs updated executables and scripts for the Configuration Server to work with Patch Manager.

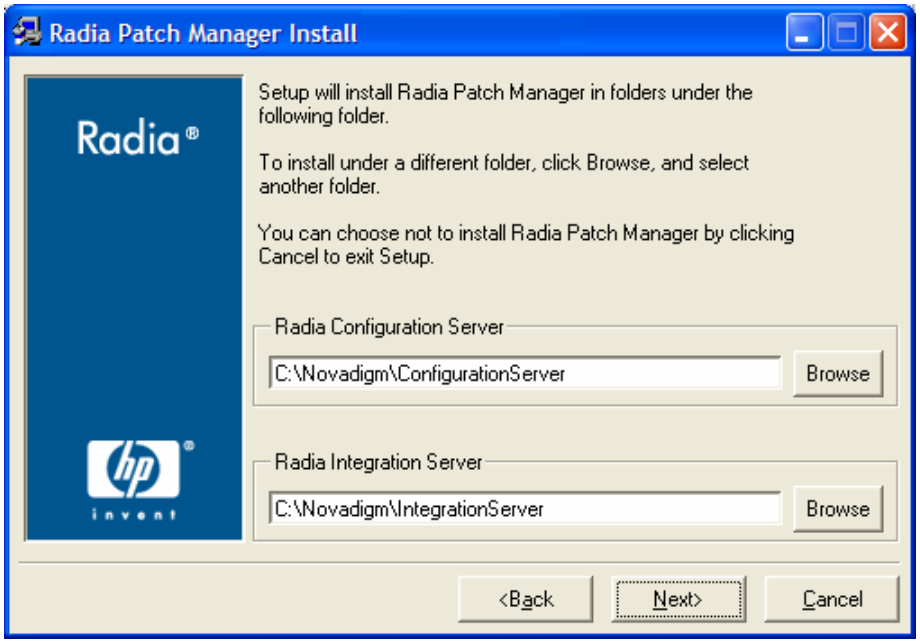
> To use the features of Patch Manager Version 2.0, you must select **Radia Database Updates**. The PATCHMGR domain, and only the PATCHMGR domain, will be replaced, and all data in that domain removed.

— **Radia Database Updates**
Creates the PATCHMGR domain in the Radia Database.

> The Configuration Server Components and Radia Database 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 making your selections, click **Next**. The Warning window opens.

6 Click **Next** in the warning window.



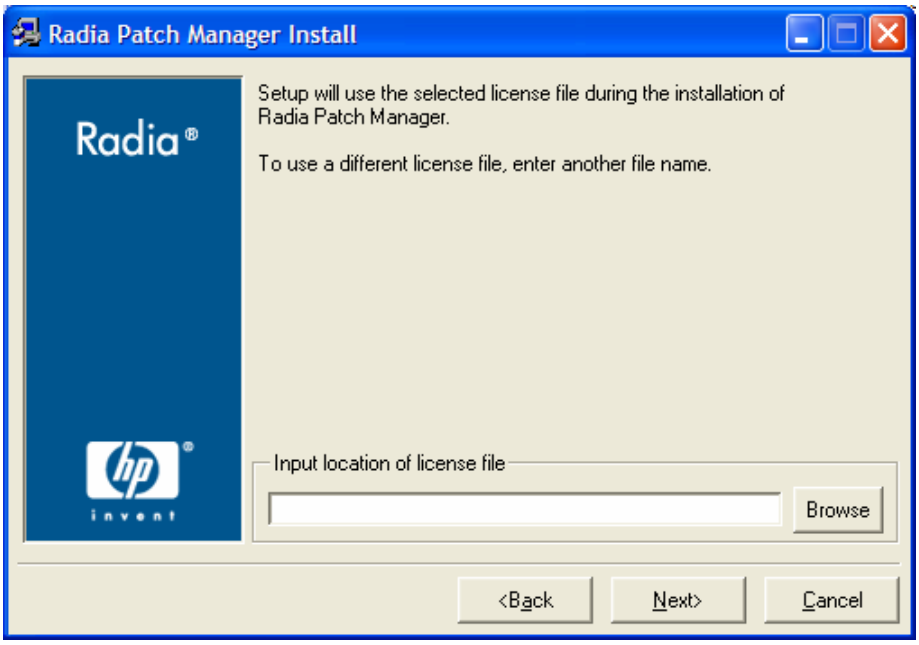
7 Type the location where the Configuration Server is installed, or click **Browse** to navigate to the location.

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

Where possible, accept the defaults for these directories.

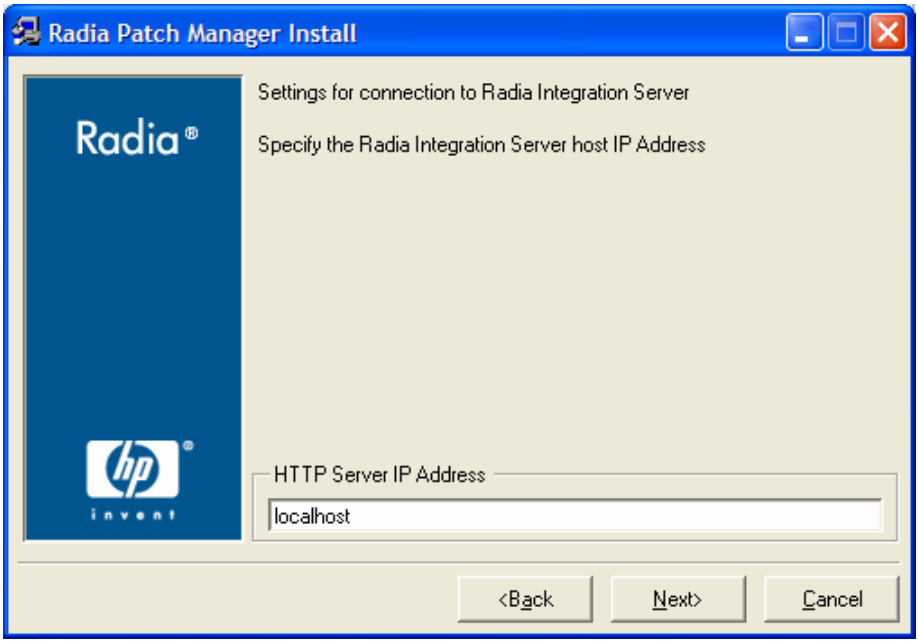
8 Click **Next**.

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

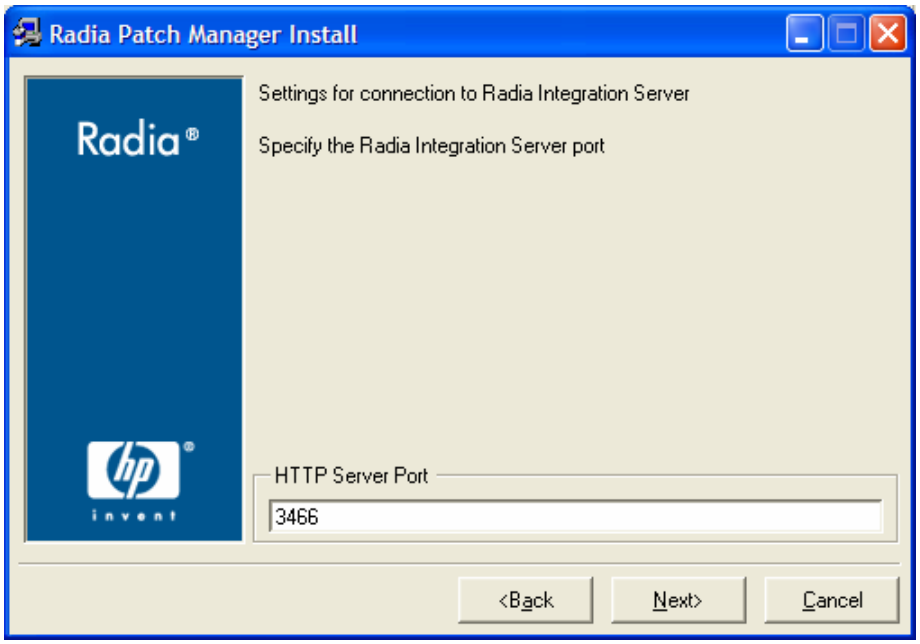


10 Type the location of your license file or click **Browse** to navigate to it.

11 Click **Next**.



12 Type the IP address of the Radia Integration Server, and click **Next**. The Radia Integration Server is the service that hosts the Patch Manager module.



13 Type the port of the Radia Integration Server, and click **Next**.

The summary window opens.

14 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.

15 Click **Finish**.

The Configuration Server and the Radia Database have been updated. The Messaging Service and the Patch Manager have been installed.

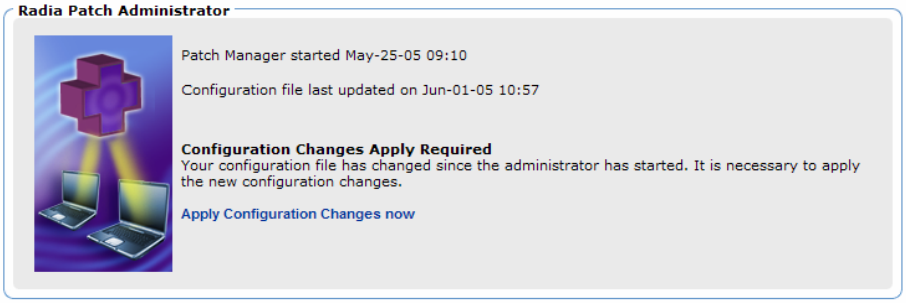
You should be directed to the Radia Patch Administrator page for final configuration and database synchronization. If you are not, go to **http://<*patchserveripaddress*>:<*port*>/patch/manage/admin.tsp**, set your configuration, and run a database synchronization.

Configuring the Patch Manager Server

The Radia Patch Administrator page provides an interface to the Patch Manager settings file, `patch.cfg`. `Patch.cfg` includes settings such as passwords, server locations, and DSN information. Use the Patch Manager Administrator to modify these settings or you can edit this file manually. The Patch Manager Administrator is divided into twelve areas described below: Configuration Server, Patch Manager, ODBC DSN, Microsoft Feeds, RedHat Feeds, SuSE Feeds, HPUX Feeds, Solaris Feeds, HTTP, Acquisition History, Patch Agent, Reporting, and Default.

To use the Patch Manager Administrator

1. From your web browser, go to **http://***patchserveripaddress***:***port* **/patch/manage/admin.tsp**.
2. Type the values for the 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 and Table 4 on page 70.
3. Click **Save** to apply changes. You will be prompted to restart for the changes to take effect.

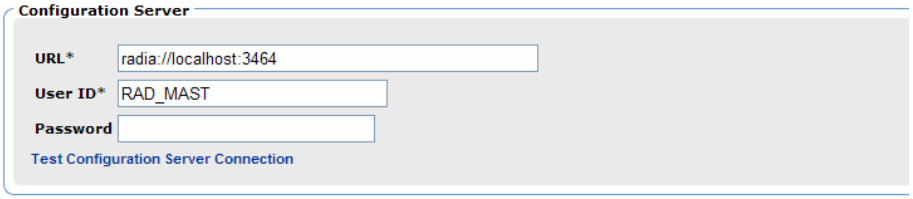


4. Click **Apply Configuration Changes now** to restart the Patch Manager Server.

Configuration Server Settings

The following settings are configured in the Configuration Server section:

- **URL**: Specify the location of your Configuration Server using the format: radia://*ipaddress* or *hostname*:*port*. This is the same as the rcs_url parameter in `patch.cfg`.
- **User ID**: If authentication has been enabled on your Configuration Server, specify the user. This is the same as the rcs_user parameter in `patch.cfg`.
- **Password**: If authentication has been enabled on your Configuration Server, specify the password for the rcs_user. This is the same as the rcs_pass parameter in `patch.cfg`.
- **Test Configuration Server Connection**: You can test your Configuration Server connection from the Patch Administrator. To do this, click **Test 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 Manger Server.



Patch Manager Settings

The following settings are configured in the Patch Manager section:

- **URL***: Specify the URL to connect to the Radia Patch Update web site provided by HP. This is the same as the nvdm_url parameter in `patch.cfg`. The default is: **http://managementsoftware.hp.com/Radia/patch_management/data**

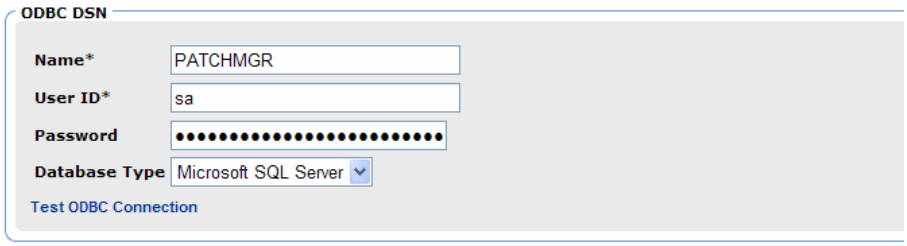
This is a new location for Version 2.0. The nvdm_user and nvdm_password parameters are no longer used.

ODBC DSN Settings

The following settings are configured in the ODBC DSN section:

- **Name***: Specify the Data Source Name (DSN) for the Patch SQL or Oracle database. This is the same as the dsn parameter in `patch.cfg`.
- **User ID***: Specify the user for the dsn for the Patch ODBC database. This is the same as the dsn_user parameter in `patch.cfg`.
- **Password**: Specify the password for the user of the Patch ODBC database. This is the same as the dsn_pass parameter in `patch.cfg`.
- **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.

  Note: If you are using Oracle, change this value to oracle before doing a patch acquisition or a 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 Manger Server.



Microsoft Feed Settings

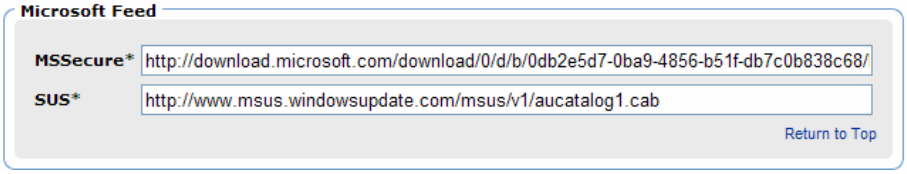
The following settings are configured in the Vendor Feeds section:

- **MSSecure***: Specify the URL for the Microsoft `MSSECURE.XML` file. This is the same as the microsoft_url parameter in `patch.cfg`.

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

- **SUS***: Specify the URL for the Microsoft SUS data feed. This is the same as the microsoft_sus_url parameter in `patch.cfg`.

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



Red Hat Feed Settings

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

- **RedHat**: Specify the URL for the Red Hat Network data feed. This is the same as the rhn_url parameter in `patch.cfg`.

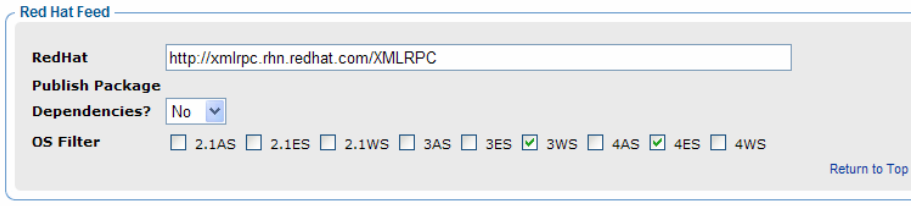
  Default: **http://xmlrpc.rhn.redhat.com/XMLRPC**

- **Publish Package Dependencies**: Specify **`yes`** if you want to publish additional Red Hat packages that downloaded security advisories may depend on. You can override this setting for a specific acquisition by setting it in Acquisition Settings. This is the same as the rh_depends parameter in `patch.cfg`.

  Default: No

- **OS Filter**: Select operating systems for the acquisition of Red Hat patches. This is the same as the vendor_os_filter parameter in `patch.cfg`.

  If you remove one operating system in your OS Filter from one acquisition to the next, all patches from the operating system that you removed from the OS Filter will be erased from the patch repository. This applies to all *vendors*. OS Filters are specified either in the Configuration Settings page or in the vendor_os_filter parameter in patch.cfg.



SuSE Feed Settings

The following settings are configured in the SuSE Feed section:

- **SuSE 8**: Specify the url for acquiring updates for SuSE 8. This is set in the suse_urls parameter in `patch.cfg`.

  Default: **http://sdb.suse.de/download/i386/update/SUSE-SLES/8/**

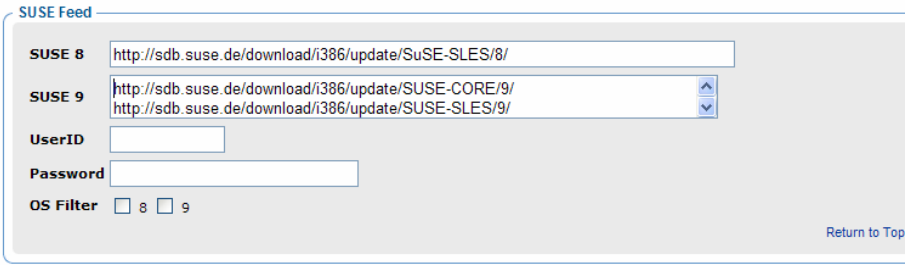
- **SuSE 9**: Specify the url for acquiring updates for SuSE 9. This is set in the suse_urls parameter in `patch.cfg`.

  Defaults: **http://sdb.suse.de/download/i386/update/SUSE-CORE/9/ http://sdb.suse.de/download/i386/update/SUSE-SLES/9/**

- **UserID**: Specify your SuSE user ID. This is the same as the suse_user parameter in `patch.cfg`. Obtain a user id from the vendor.

- **Password**: Specify the password for the SuSE UserID. This is the same as the suse_pass parameter in `patch.cfg`.

- **OS Filter**: Select operating systems for the acquisition of SuSE Linux Enterprise Server patches. This is the same as the vendor_os_filter parameter in `patch.cfg`.



HP-UX Feed Settings

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

- **Security Catalog**: 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`.

  Default: **http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=security_catalog2.gz**

- **Description XML**: 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`.

Default: **http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=patches.xml**

- **Patch Download**: Specify the HP-UX url for downloading the patches. This is the same as the hpux_patch_url parameter in `patch.cfg`.

  Default: **ftp://ftp.itrc.hp.com/**.

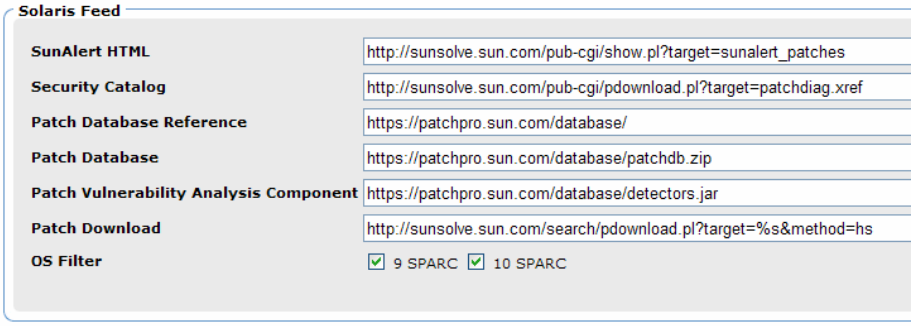
- **OS Filter**: Select operating systems for the acquisition of HP-UX security bulletins. This is the same as the vendor_os_filter parameter in `patch.cfg`. These are the only operating systems that will be available for acquisition for this vendor.

Solaris Settings

The following settings are configured in the Solaris Feed section:

- **SunAlert HTML**: This is set in the solaris_sunalerts_url parameter in patch.cfg. The default is **http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches.** This url provides a list of all available Sun Alerts and the patch ids associated with each Sun Alert.
- **Security Catalog**: This file includes information on all patches, both security and non-security related. This is set in the solaris_pdiag_url parameter in patch.cfg. The default is **http://sunsolve.sun.com/pub-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 is set in the solaris_patchpro_base_url parameter in patch.cfg. The default is **https://patchpro.sun.com/database/.** This parameter defines the directory repository for Sun Solaris meta data files.
- **Patch Database**: This is set in the solaris_patchpro_db_url parameter in patch.cfg. The default is **https://patchpro.sun.com/database/patchdb.zip**. This Sun Microsystems url provides meta data concerning Sun Solaris “available” patches.

- **Patch Vulnerability Analysis Component**: This is set in the solaris_patchpro_jar_url parameter in `patch.cfg`. The default is **https://patchpro.sun.com/database/detectors.jar**. This auxiliary file is used by Sun Patch Manager Version 2.0 to perform patch applicability and vulnerability assessment.
- **Patch Download**: This is set in the solaris_patch_url parameter in `patch.cfg`. The default is **http://sunsolve.sun.com/search/pdownload.pl?target=%s&method=hs**, This URL provides a reference to the download locations of signed Sun Solaris patches.
- **OS Filter**: Select operating systems for the acquisition of Solaris patches. This is the same as the vendor_os_filter parameter in `patch.cfg`. Valid values for Solaris are SOLARIS::9, SOLARIS::10 to acquire patches for Solaris versions 9 and 10 for the SPARC architecture *only*.

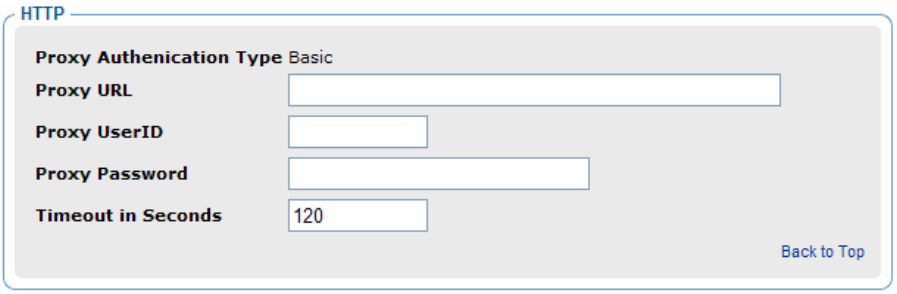


HTTP Settings

The following settings are configured in the HTTP Settings section:

- **Proxy Authentication Type**: Basic. This parameter is not configurable.
- **Proxy URL**: If you use a proxy server for http traffic, specify its URL in the format **http://ip:port**. This is the same as the http_proxy_url parameter in `patch.cfg`.
- **Proxy User ID**: If you use a proxy server for http traffic, specify your user ID. This is the same as the http_proxy_user parameter in `patch.cfg`.
- **Proxy Password**: If you use a proxy server for http traffic, specify your password. This is the same as the http_proxy_pass parameter in `patch.cfg`.
- **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. This is the same as the http_timeout parameter in `patch.cfg`.



Acquisition History Settings

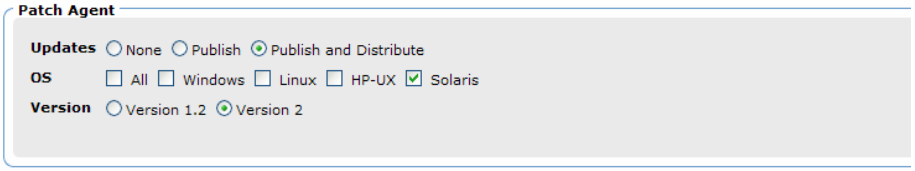
The following settings are configured in the Acquisition History section:

- **Save History Summary**: 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 here, and not on the command line. If history has a smaller value than Save History Detail, then Save History Detail will be set to the value for Save History Summary. 0 means never to delete any history of Patch Acquisition. This is the same as the history parameter in `patch.cfg`.
- **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. HP recommends specifying this here, and not on the command line. This is the same as the purge_errors parameter in `patch.cfg`.

Patch Agent Settings

These settings are for the maintenance of the Patch Manager client agent files. For more information on this, see Updating the Patch Manager Client Agent on page 93. The following settings are configured in the Patch Agent section:

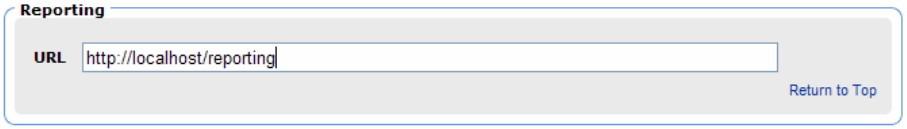
- **Updates**: If you select Publish, the updates will be published to the PATCHMGR domain, but will not be connected for distribution (deployment) to Patch Manager client computers. You will need to create these connections. If you select Publish and Distribute, the updates will be published to the PATCHMGR domain and connected to the Discover Patch instance. This option will distribute the updates to your Patch Manager client computers. This is the same as the agent_updates parameter in `patch.cfg`.
- **OS**: Specify for which operating systems to acquire the agent updates. This is the same as the agent_os parameter in `patch.cfg`.
- **Version**: Select which Patch Manager version you would like to acquire the agent updates for. You can only publish one version to one Configuration Server. This is the same as the agent_version parameter in `patch.cfg`.



Reporting Settings

This setting is for the location of the Reporting Server. Click the Reporting icon in the Patch Manager Administrator to view Patch Reports:

- **URL**: Specify the location of the Reporting Server you are using for your Patch Manager. Click on the **Reporting** icon in the Patch Manager Administrator to view Patch Reports. This is the same as the reporting_url parameter in `patch.cfg`.



Default Settings

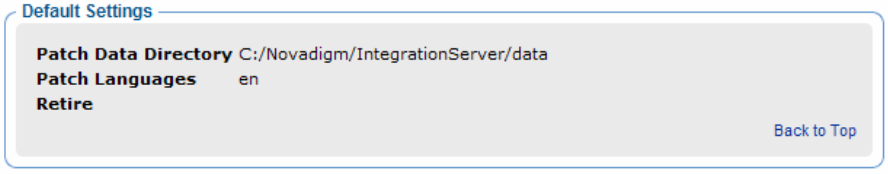
The following settings are for informational purposes only. They can only be changed in `patch.cfg` or explicitly in an acquisition command line. Be careful to back up and type in the correct settings when manually editing the `patch.cfg`.

- **Patch Data Directory**: The directory where patches are downloaded to before they are sent 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 a different directory in this parameter. This is the same as the data_dir parameter in `patch.cfg`.
- **Language**: Patch Manager supports non-double byte languages. This parameter shows the abbreviation of the languages for which you will acquire patches. This is the same as the lang parameter in `patch.cfg`.
- **Retire**: Shows the bulletins to retire separated by commas. This parameter works on the bulletin level, not at the product or release level.

  This is the same as the retire parameter in `patch.cfg`. The retire function:

  — Deletes specified bulletins if they exist in the Radia Database during the current publishing session.

  — Does not publish the bulletins specified in the retire parameter to the Radia Database during the current publishing session. The use of the Retire option supersedes the Bulletins option.



Patch Configuration Settings File

If you are unable to use the Patch Manager Administrator, you can make changes directly in the `patch.cfg` file. The default location is *`System Drive`*`:\Novadigm\IntegrationServer\etc`. Settings in `patch.cfg` that are directly related to the Patch Manager Server are listed below. There are additional parameters that are only used for patch acquisition. See Chapter 3, Patch Acquisition for more information.

Table 2 Patch Manager Server Configuration Parameters

Parameter	Description
data_dir	Specify the directory to which you want the security patches downloaded 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. Default: `{IntegrationServer}\data\patch` (a directory structure off the directory from which you are running the command).
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. Note: If you are using Oracle, change this value to oracle before doing a patch acquisition or a database synchronization.
dsn	Specify the Data Source Name (DSN) the Patch SQL database. Note: 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.** Note: 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.

Parameter	Description
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. Default: 0 means never to 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`. Default: **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`. Default: **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`. Default: **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**. Note: 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.

Parameter	Description
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. For example, the default as seen in the `setup.tsp` is 120 second. This is reflected in `patch.cfg` as 120000. 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 (!). Default: en (English). Example: - lang fr, en.
microsoft_sus_url	Specify the URL for the Microsoft SUS feed. Default: **http://www.msus.windowsupdate.com /msus/v1/aucatalog1.cab**.
microsoft_url	Specify the URL for the Microsoft `MSSECURE.XML` file. Default: **http://download.microsoft.com /download/0/d/b/0db2e5d7-0ba9-4856-b51f-db7c0b838c68/MSSecure_1033.CAB.** Note: As of this printing, Microsoft has changed the location of `mssecure.xml`. If you are using a release of Patch Manager previous to 1.2.2, you must specify this path on the acquisition command line. This path is hard coded into Patch Manager 1.2.2.

Parameter	Description
nvdm_url	Specify the URL to connect to the Radia Patch Update web site provided by HP. This is the same as the nvdm_url parameter in `patch.cfg`. Default: **http://managementsoftware.hp.com /Radia/patch_management/data** Note: This is a new location for Version 2.0. The nvdm_user and nvdm_password parameters are no longer used.
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.
rcs_pass	If authentication has been enabled on your Configuration Server, specify the password for the rcs_user.
rcs_url	Specify the location of your Configuration Server in URL format. 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. Note: This parameter is required.
rcs_user	If authentication has been enabled on your Configuration Server, specify the rcs_user.
reporting_url	Specify the URL of your Reporting Server.

Parameter	Description
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. Notes: 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. Caution: 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 client devices. Example: -retire MS00-001,MS00-029

Parameter	Description
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 by setting it in Acquisition Settings. This is the same as the rh_depends parameter in `patch.cfg`. 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, the baseline operating system rpm files supplied on Red Hat installation media should be placed in `data/patch/redhat/packages/3es`. 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. Default: No
rhn_url	Specify the URL for the Red Hat Security Network Default: **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.**

Parameter	Description
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 for the user for the SuSE web site.
suse_urls	Specify the urls for the SuSE network. Default: **8 {http://sdb.suse.de/download/i386/update/SuSE-SLES/8/}** **9 {http://sdb.suse.de/download/i386/update/SUSE-CORE/9/ http://sdb.suse.de/download/i386/update/SUSE-SLES/9/}**
suse_user	Specify the user for the SuSE web site.
sync	Specify the targets that need to be synchronized. Default: rcs.

See the sample `patch.cfg` file below. Note the use of brackets for parameters. If you are specifying any of these from a command line for acquisition, be sure to use quotes around values containing spaces. See Chapter 3, Patch Acquisition for more information on running an acquisition command line.

If you have previously installed the Patch Manager, rename the `patch.cfg` file as a backup precaution. Its default location is *`System_Drive`*`:\Novadigm\IntegrationServer\etc`.

```
patch::init {
        ADMIN_DATE_FMT %Y-%m-%d
        AGENT_OS *
        AGENT_UPDATES PUBLISH,DISTRIBUTE
        AGENT_VERSION VERSION2
        ALERT_DAYS 14
        BUILD 399
        BULLETINS *
        COMMIT_INTERVAL 5000
        CVENAME Y
        DATA_DIR C:/Novadigm/IntegrationServer/data
        DB_TYPE mssql
        DL_DATEFMT {%Y-%m-%d %T}
        DSN LocalServer
        DSN_ATTEMPTS 3
        DSN_DATEFMT {%Y-%m-%d %H:%M:%S}
        DSN_DELAY 10
        DSN_PASS {}
        DSN_PING 60
        DSN_TRACE 0
        DSN_USER sa
        ETC C:/Novadigm/IntegrationServer/etc/patch
        FORCE no
        FTP_PASS {{DES}Z4WefDOU43Grvr7MygliwA==:14}
        FTP_PROXY_AUTHENTICATION basic
        FTP_PROXY_PASS {}
        FTP_PROXY_SCRIPT {}
        FTP_PROXY_URL {}
        FTP_PROXY_USER {}
        FTP_USER anonymous
        HISTORY 0
        HOME C:/Novadigm/IntegrationServer/modules/patch.tkd
        HPUX_PATCH_URL ftp://ftp.itrc.hp.com/
        HPUX_URL
        http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=security_catalog2.gz
        HPUX_XML_URL http://itrc.hp.com/service/patch/securityPatchCatalog.do?item=patches.xml
        HTTP_PROXY_AUTHENTICATION basic
        HTTP_PROXY_PASS {}
        HTTP_PROXY_SCRIPT {}
        HTTP_PROXY_URL {}
```

```
HTTP_PROXY_USER {}
HTTP_RETRIES 2
HTTP_TIMEOUT 120000
LABEL PATCH
LANG en
LANGUAGE {}
LOG C:/Novadigm/IntegrationServer/logs
MICROSOFT_ASP_EXT mspx
MICROSOFT_PASS {}
MICROSOFT_SUS_URL http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab
MICROSOFT_TECHNET http://www.microsoft.com/technet/security/bulletin
MICROSOFT_URL http://download.microsoft.com/download/0/d/b/0db2e5d7-0ba9-4856-b51f-
db7c0b838c68/MSSecure_1033.CAB
MICROSOFT_USER {}
MODE both
MODULE patch
NVDM_PASS {}
NVDM_URL http://managementsoftware.hp.com/Radia/patch_management/data
NVDM_USER {}
N_WORKERS 2
PRODUCT {!Windows 95,!Windows 98*,!Windows Me,SUSE::!sles*-yast2,SUSE::!sles*-yast2-
*,SUSE::!sles*-liby2*}
PURGE_ERRORS 7
RCS_PASS {}
RCS_URL radia://localhost:3464
RCS_USER RAD_MAST
REPLACE N
REPORTING_URL http://localhost/reportingserver
REPORT_TZ LOCAL
RETIRE {}
RHN_URL http://xmlrpc.rhn.redhat.com/XMLRPC
RH_DEPENDS N
ROOT C:/Novadigm/IntegrationServer
SOLARIS_PATCHPRO_BASE_URL https://patchpro.sun.com/database/
SOLARIS_PATCHPRO_DB_URL https://patchpro.sun.com/database/patchdb.zip
SOLARIS_PATCHPRO_JAR_URL https://patchpro.sun.com/database/detectors.jar
SOLARIS_PATCH_URL http://sunsolve.sun.com/search/pdownload.pl?target=%s&method=hs
SOLARIS_PDIAG_URL http://sunsolve.sun.com/pub-cgi/pdownload.pl?target=patchdiag.xref
SOLARIS_SUNALERTS_URL http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches
STATUS_INTERVAL 600
STATUS_RESET {12:00 am}
SUPERCEDED_PATCHES N
SUSE_PASS {}
SUSE_URLS {8 http://sdb.suse.de/download/i386/update/SuSE-SLES/8/ 9
{http://sdb.suse.de/download/i386/update/SUSE-CORE/9/
http://sdb.suse.de/download/i386/update/SUSE-SLES/9/}}
SUSE_USER {}
TITLE {Radia Patch Manager Reporting}
URL /patch
VENDORS microsoft
VENDOR_OS_FILTER {}
VERSION 2.2.0
WORKER_RETRY 3
WORKER_TIMEOUT 180
```

}

Database Synchronization

The patch information that has been sent to the Radia Database on the Configuration Server must be synchronized with your ODBC Patch Database for assessment and analysis of the patch. The Radia Database and the ODBC Patch database house identical information.

- Each class in the PATCHMGR domain becomes a class 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. For example, you may want to identify what differences may exist between the two databases without committing the changes or only update one class. You can synchronize using either the Radia Patch Administrator or a command line.

To synchronize the databases using the Radia Patch 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**.

To synchronize the databases from a command line

- Run the following command line from the Radia Integration Server directory:

  ```
  nvdkit ./modules/patch.tkd sync -dsn patch -dsn_user
  rpmadmin -dsn_pass rpmdb -host localhost:3464 -class
  "*"
  ```

  `dsn` is a required parameter.

  For example, if you only wanted to update the PRODUCT class, you would type:

```
nvdkit ./modules/patch.tkd sync -dsn PATCH -host ↲
localhost:3464   -class "PRODUCT"
```

where the `dsn` is called PATCH and the Configuration Server is the local machine.

See Table 3 below.

Table 3 `Patch.tkd` synchronization parameters

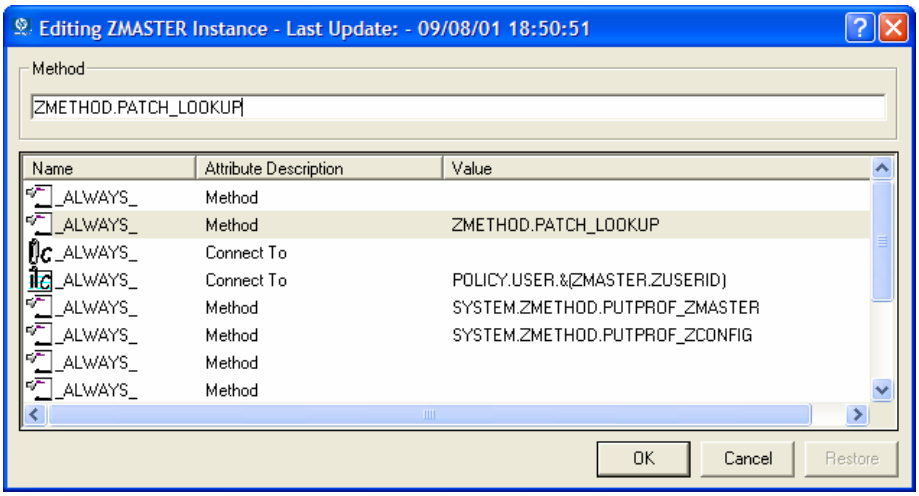
Parameter	Description
dsn	Specify the Data Source Name (DSN) the Patch ODBC database. Note: This parameter is required.
dsn_user	Specify the user for the dsn for the Patch ODBC database.
dsn_pass	Specify the password for the user of the Patch ODBC database.
host	Specify the location of your Configuration Server in URL format. 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. Note: This parameter is required.
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. Default: class = "*" (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. Default: All changes are committed.

Parameter	Description
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.

Adding a Method Connection

Use the System Explorer to add an _ALWAYS_ Method connection to the PRIMARY.SYSTEM.PROCESS.ZMASTER instance as shown in the figure below.

Figure 2 Edit the ZMASTER instance.



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

Messaging Server

Install Messaging Server Version 3.0. This includes updates to the Messaging Server for use with Patch Manager. When messaging Server is installed the Patch Manager Data Delivery Agent must be enabled.

Reporting Server

The Reporting Server version 4.1.2 is required to view enhanced reports for Radia Patch Manger. Obtain the Reporting Server from the HP Support web site, and review the release notes prior to installing. The Reporting Server Guide also includes instructions on how to use the Reporting Server.

Configuration Analyzer Installation Tasks (Optional)

The Configuration Analyzer provides a powerful console for viewing, storing, and comparing application data. Backed by an SQL database, the Configuration Analyzer allows you to import state files. A state file is a highly tuned file format that is used to store information about an application or workstation at a particular point in time.

If you are using Oracle with the Configuration Analyzer, you must use Oracle version 8i or 9i with SQL Loader (part of the Oracle client/admin toolset) on computers that will be performing imports. This includes the Configuration Analyzer and Knowledge Base Manager computers. It is recommended that you use the same version of driver and database to prevent any version mismatch issues.

For information regarding the Configuration Analyzer, see the *Configuration Analyzer Guide*.

Installing and Configuring the Knowledge Base Manager (Optional)

The Knowledge Base Manager performs automated import processing of Radia state files into the Radia Application Knowledge Base allowing you to compare state files. The Knowledge Base Manager automated import server runs independent of the Configuration Server to import files found in the AutoImport directories that you specify. The Knowledge Base Manager can be controlled as a Windows service. The service name is RadKBMgr and it may be stopped and started through Administrative Tools\Services of the Control Panel.

For information regarding the Knowledge Base Manager, see the *Knowledge Base Manager Guide* available on the HP OpenView web site.

If you are using Oracle with the Knowledge Base Manager, you must use Oracle version 8i or 9i with SQL Loader (part of the Oracle client/admin toolset) on computers that will be performing imports. This includes the Configuration Analyzer and Knowledge Base Manager computers. We recommend that you use the same version of driver and database to prevent any version mismatch issues.

Summary

- Install and modify the Configuration Server and the Radia Database.
- Patch Manager requires an SQL or Oracle database.
- Install the Patch Manager on a computer that can access the Configuration Server and your ODBC Data Source.
- Install the Configuration Analyzer and the Knowledge Base Manager if you want to create and analyze state files.

3 Patch Acquisition

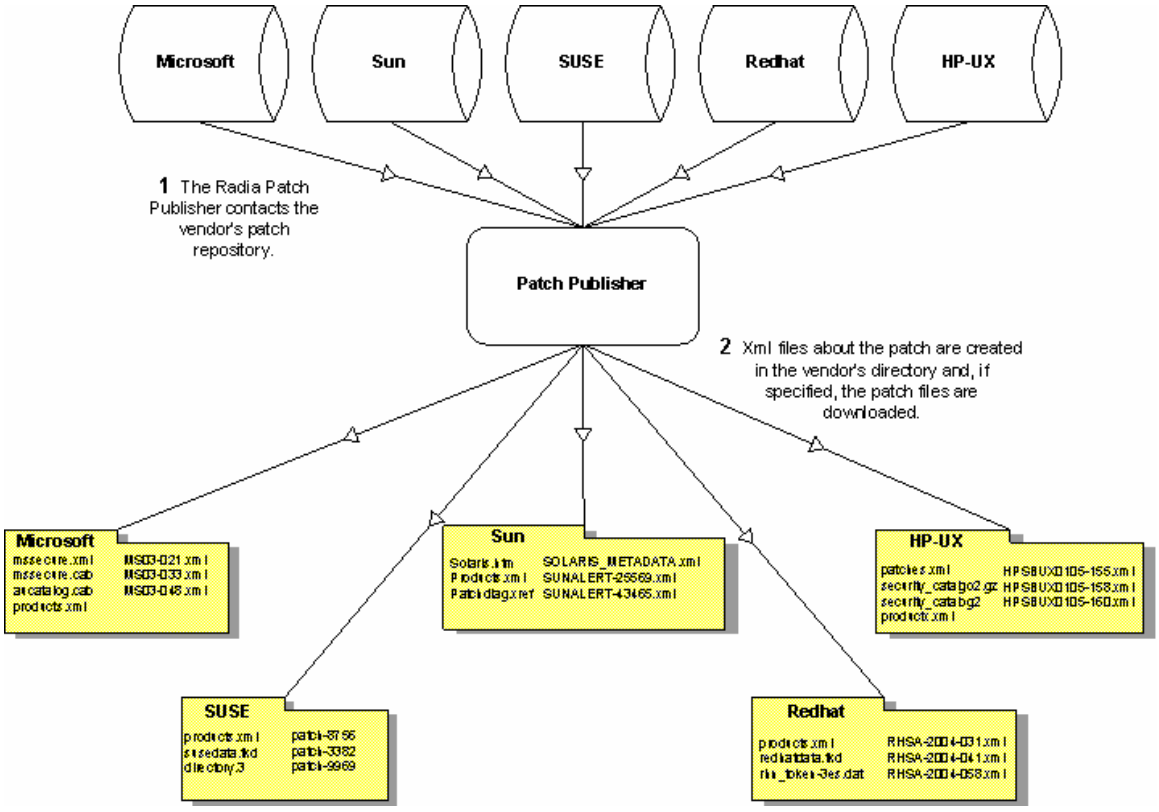
At the end of the chapter, you will:

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

Radia 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 Radia Database. The acquisition process fetches security patches from the vendor *and* publishes this information to the Radia Database.

Figure 3 Vendor's patch repository is contacted



Patch Acquisition Overview

Patch Manager is used to acquire security patches and to synchronize the patch information in the Radia Database 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 Microsoft 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.

  Microsoft security bulletins are automatically acquired provided that they are found in Microsoft's data feed file, `mssecure.xml`.

- An xml file is created for each bulletin acquired and is put in the vendor's folder in the Radia Integration Server's directory. These files are called patch descriptor files.
- The Radia 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.

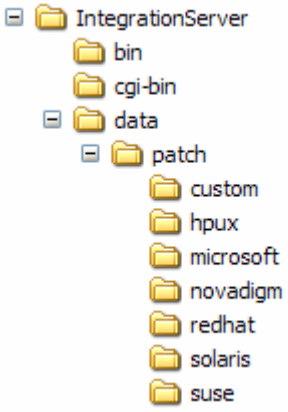
The syntax for the acquisition includes a verb that describes the action that Patch Manager, `patch.tkd`, is to perform and a list of parameters for that action. Each parameter should be preceded by a hyphen with the value for the parameter following. Examples are provided for patch collection and database synchronization in the following sections.

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 `\\Novadigm\IntegrationServer\Data\Patch`. For example, patch descriptor files for Microsoft bulletins would be in `\\Novadigm\IntegrationServer\Data\Patch\Microsoft` while those for Red Hat are located in `\\Novadigm`

\IntegrationServer\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

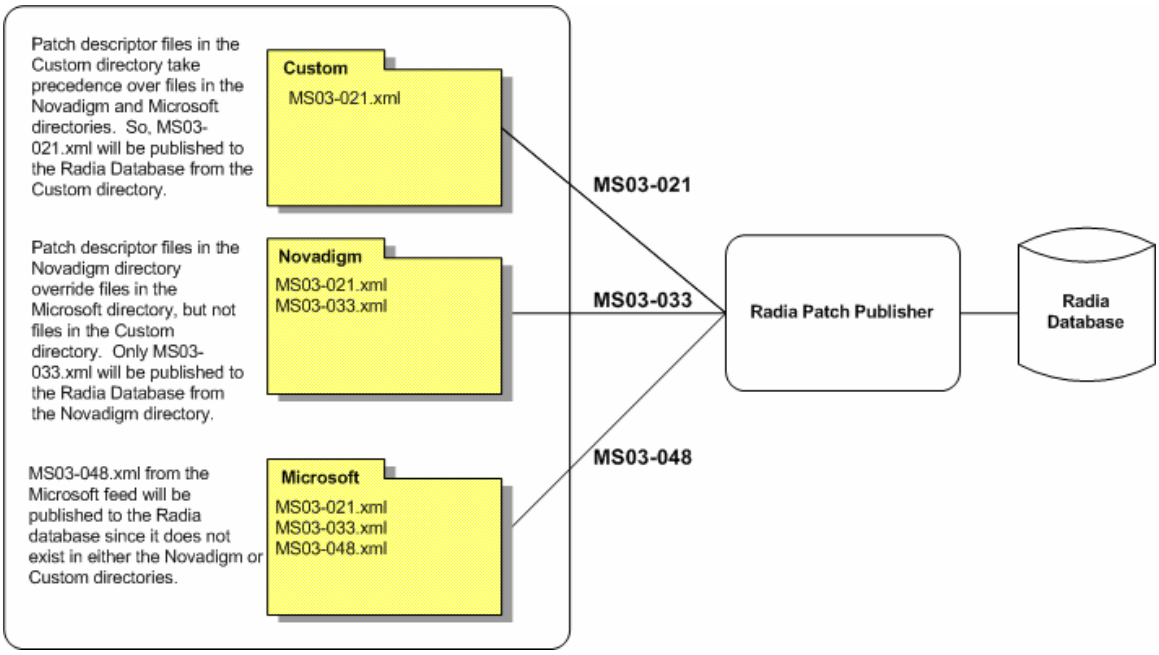


Some of the information acquired from the vendor may need to be altered before the patch can be managed. Therefore, there are two other subdirectories in \\Novadigm\IntegrationServer\Data\Patch. HP provides you with some additional patch descriptor files that are located in the Novadigm subdirectory. Patch descriptor files located in the Novadigm directory override patch descriptor files in the relevant vendor's directory. You can also create or modify your own patch descriptors that 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 in Custom override those in Novadigm and Microsoft.



About Red Hat Patch Acquisition Prerequisites

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 entitlement for each of the Red Hat Enterprise Server OS versions for which you want to acquire and manage patches.

To perform patch acquisitions for Red Hat Enterprise Server Versions 2.1, 3 and 4, you will need a Red Hat Network account with at least three Red Hat Network system entitlements, one for each Enterprise Server version.

- 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, the baseline operating system rpm files supplied on Red Hat installation media should be placed in `data/patch/redhat/packages/3es`. If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, HP recommends copying the dependency packages to the appropriate packages directory from your Linux installation media. The Red Hat RPM packages can be found on the installation media under the RedHat/RPMS directory.
- Use the rhn_register tool to create a Red Hat Network (RHN) `systemid` file. This file will be used to pass RHN credentials during acquisition. See the procedure below for details.

To create a Red Hat systemid file

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

Enterprise Server V 2.1, then rename the `systemid` file to `redhat-2.1es.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 in `patch.cfg`.

About SuSE Patch Acquisition Prerequisites

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.

About HP-UX Patch Acquisition

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 are missing on the agent.
- Roll back of HP-UX security patches is not supported.

About Solaris Patch Acquisition

The HP OpenView Adapter for SSL Using Radia (SSL Adapter) must be installed on the Patch Manager Server that you are using for Solaris Patch Acquisition. The minimum version required for the SSL Adapter is version 2.1, including `tls.tkd` build 8. The SSL Adapter is included in the HP OpenView Using Radia media. The need for a secure connection within Patch

Manager is only required on the Integration Server that is used 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.

Performing a Patch Acquisition

You can acquire patches either using the Radia Patch Administrator or using a command line. The Radia Patch Administrator 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 Radia Patch Administrator to run the file. Parameters specified in an acquisition profile or on an acquisition command line override parameters set in the `patch.cfg` file. Be sure to use quotes around values containing spaces. You may want to specify required parameters in the `patch.cfg` file. See Configuring the Patch Manager Server on page 31 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 increasing the HTTP Timeout parameter to value greater than 1200 seconds.

The parameters that are required depend on your environment.

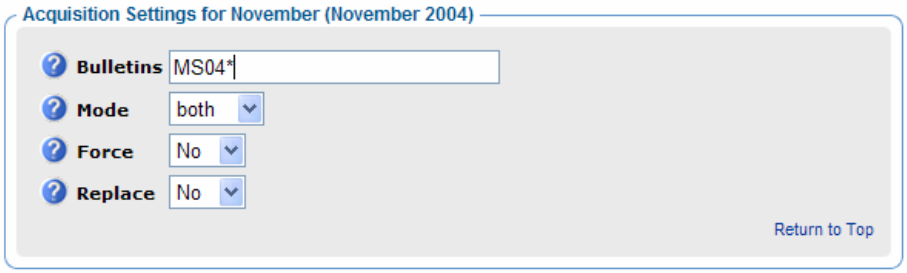
To create or edit an acquisition profile using the Radia Patch Administrator

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**.

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



- **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 an asterisk (*) for filtering.
  - 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.
  - HPUX 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 use the naming convention `RHSA-CCYY-###`, where `CC` indicates the century and `YY` the last to digits of the year when the advisory was issued, and `###` the Red Hat patch number. Red Hat Security advisories, use a hyphen (-) in place of an asterisk (*) for filtering.
  - 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-patchid-revision`, where patch-id represents the specific Sun

Microsystems patch number, and revision is the revision identifier of the patch.

- Microsoft example: -bulletins MS00-001,MS00-029
- Note: 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 Qnumbers 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 client devices. This is the same as the mode parameter in `patch.cfg`.
- **Force**: Use force when:
  - 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. This is the same as the replace parameter in `patch.cfg`.

Microsoft Settings

- **Acquire Microsoft Patches**: Select **Yes** if you want to acquire Microsoft Patches. A list of languages will appear.
- **Languages**: Click the languages for the acquisition of Microsoft patches. This is the same as the lang parameter in `patch.cfg`.

RedHat Settings

- **Acquire RedHat Patches**: Select **Yes** if you want to acquire RedHat Patches. A list of possible architectures and operating system filters appears.
- **Publish Package Dependencies**: 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 by setting it in Acquisition Settings. This is the same as the rh_depends parameter in `patch.cfg`.

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, the baseline operating system rpm files supplied on Red Hat installation media should be placed in `data/patch /redhat/packages/3es`. 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.

Default: No

- **Architecture**: Select architectures for the acquisition of Red Hat patches. This is the same as the arch parameter in `patch.cfg`.

SuSE Settings

- **Acquire SUSE Patches?**: Select **Yes** if you want to acquire SuSE Patches. Select the operating systems using the OS Filter option for SuSE Feed Settings on the Configuration Settings Page.

HP-UX Settings

- **Acquire HP-UX Patches?**: Select **Yes** if you want to acquire HP-UX Patches. Select the operating systems using the OS Filter option for HP-UX Feed Settings on the Configuration Settings Page.

Solaris Settings

- **Acquire Solaris Patches?**: Select **Yes** if you want to acquire Solaris Patches. Select the operating systems using the OS Filter option for Solaris Feed Settings on the Configuration Settings Page.

If you remove one operating system in your OS Filter from one acquisition to the next, all patches from the operating system that you removed from the OS Filter will be erased from the patch repository. OS Filters are specified either in the Configuration Settings page or in the vendor_os_filter parameter in `patch.cfg`.

6 Click **Next** to go to Step 3 where you will select products.

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 Radia Patch Administrator to run the acquisition using your saved settings.

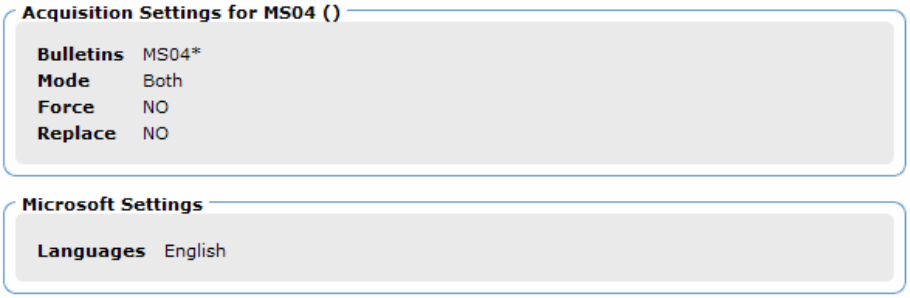
To run an acquisition from the Radia Patch Administrator

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

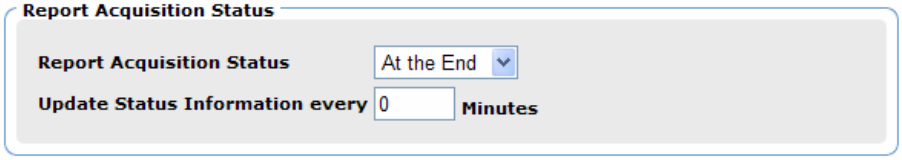
2 From **Operations**, click **Start an Acquisition**.

3 Select a file by clicking on its name.

4 Confirm the settings for this acquisition.



Report Acquisition Status



- **Report Acquisition Status**: In addition to the acquisition log, you can specify how frequently you want to update the current acquisition status, 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.

To acquire patches from a command line

1 From a command prompt on your Patch Manager Server, navigate to the Radia Integration Server's directory. The default location is

System Drive:\Novadigm\IntegrationServer

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 Table 4 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.

Table 4 Patch Acquisition Parameters

Parameter	Description
arch	Specify the computer architecture for which you want to acquire patches separated by a comma. Valid values for Microsoft acquisitions is x86. Valid values for Red Hat acquisitions are i386,i486,i586,i686,athlon,noarch. Default: x86,i386,i486,i586,i686,athlon,noarch.
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 an asterisk (*) for filtering. • 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

Parameter	Description
	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. • HPUX 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 use the naming convention `RHSA-CCYY-###`, where `CC` indicates the century and `YY` the last to digits of the year when the advisory was issued, and `###` the Red Hat patch number. Red Hat Security advisories, use a hyphen (-) in place of an asterisk (*) for filtering. • 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-patchid-revision`, where patch-id represents the specific Sun Microsystems patch number, and revision is the revision identifier of the patch. Microsoft example: -bulletins MS00-001,MS00-029 Note: If you do not want to download any bulletins, use –bulletins NONE.

Parameter	Description
config	Use this parameter to append an alternate configuration file for acquisition to override settings in `patch.cfg`. Example: `-config c:\acq.cfg` Default: `patch.cfg`.
data_dir	Specify the directory 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. Default: `{IntegrationServer}\data\patch` (a directory structure off of the directory where you are running the command from).
force	Use force when: • 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. Note: If replace is set to Y, the bulletins will be removed and reacquired, regardless of the value of force. Default: N.

Parameter	Description
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**. Note: 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. Default: 0 means never to delete any history of Patch Acquisition.
http_proxy_pass	If you use a proxy server for http traffic, specify your password.
http_proxy_url	If you use a proxy server for http traffic, specify its URL in the format **http://ip:port**. Note: 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.

Parameter	Description
http_timeout	If the acquisition session is unable to open the http location 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. For example, the default as seen in the `setup.tsp` is 120 seconds. This is reflected in `patch.cfg` as 120000. 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 (!). Default: en (English). Example: - lang fr, en.
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 Qnumbers 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 client devices. Default: BOTH.

Parameter	Description
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. Example: To include all Windows products except Windows 95, type **{Microsoft::Windows*, Microsoft::!Windows 95}**. Default: Windows 95, Windows 98 and Window Me, and SuSE specific products *-yast2, *-yast2-*, and *-liby2 are excluded since these platforms and SuSE OS specific products are not supported by Patch Manager. Note: If specifying on the command line, surround the complete product string filters in quotes.
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.

Parameter	Description
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. Default: N.
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. Notes: 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. Caution: If you have enabled patch removal capabilities, and retire bulletins that are currently under management in your

Parameter	Description
	enterprise, the retired security patches may be removed from your Patch Manager client devices. Example: -retire MS00-001,MS00-029
Solaris_patch_url	This is the path for Solaris Patch Download. Default: **http://sunsolve.sun.com/search/pdownload.pl?target=%s&method=hs**
Solaris_patchpro_base_url	This is the path to the Solaris Patch Database Reference. Default: **https://patchpro.sun.com/database/**
Solaris_patchpro_db_url	This is the path to the Solaris Patch Database. Default: **https://patchpro.sun.com/database/patchdb.zip.**
Solaris_patchpro_jar_url	This is the path to the Solaris Patch Vulnerability Analysis Component. Default: **https://patchpro.sun.com/database/detectors.jar.**
Solaris_pdiag_url	This file includes information on all patches, both security and non-security related. Default: **http://sunsolve.sun.com/pub-cgi/pdownload.pl?target=patchdiag.xref**
Solaris_sunalerts_url	This is the path to the Solaris SunAlert HTML. Default: **http://sunsolve.sun.com/pub-cgi/show.pl?target=sunalert_patches.**
superceded_patches	Set superceded_patches to Y if you want to publish the data even if a patch is marked as superceded. Default: N

Parameter	Description
vendors	Specify the vendors to acquire patches from. Example: -vendors Microsoft, RedHat, SuSE, HPUX, SOLARIS Default: Microsoft.
vendor_os_filter	Specify a filter for the vendor's operating systems in the format *vendor*::*operating system*. RedHat example: Redhat::2.1es,Redhat::3es,Redhat::4es SuSE example: Suse::8,Suse:9 HP-UX example: HPUX::11.00,HPUX:11.11 Note: 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.

Look at the Patch Acquisition Reports on the Patch Manager web site to check the success of the acquisition. In addition, a log file is created in the Radia Integration Server'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 Microsoft, RedHat, SuSE, or Novadigm directories. Below is an example of creating a custom descriptor file for a Microsoft bulletin.

To create a custom descriptor file

1 Copy the Microsoft version of the XML file located in `C:\Novadigm\IntegrationServer\data\patch\microsoft` directory

generated during an acquisition into the `C:\Novadigm\IntegrationServer\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`.

```
<!-- XML file built using Novadigms Page Scraper -->

<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 client 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.

4 Use the following command line to publish the custom patch descriptor file. If the bulletin were MS02-065, the command line would be:

```
nvdkit ./modules/patch.tkd acquire -rcs_url radia:
//localhost:3464

   -mode BOTH -dsn patch -bulletins MS02-065 -sync rcs -
replace y
```

5 View the `patch-acquire.log` to see where the publishing process obtained the xml from:

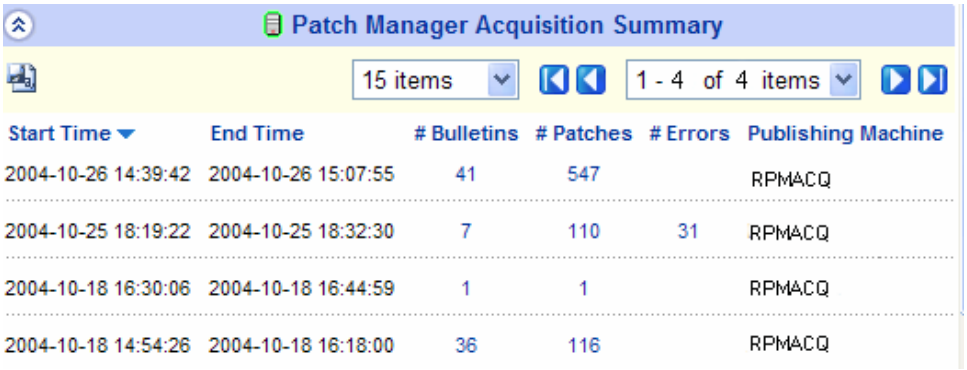
```
20040116 15:11:24 Info: Publishing MS02-065 1 of 1

20040116 15:11:24 Info: Using bulletin from custom
C:/Novadigm/IntegrationServer/data/patch/custom/MS02-065.xml

20040116 15:11:24 Info: Loading XML file
C:/Novadigm/IntegrationServer/data/patch/custom/MS02-065.xml

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

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 version 4.1 or above. Installation and configuration information can be found in the *Reporting Server Guide*. Under **Reporting Views**, click **Software Patch Reports** to expand the list of reports.

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

Figure 6 View the Acquisition summary report

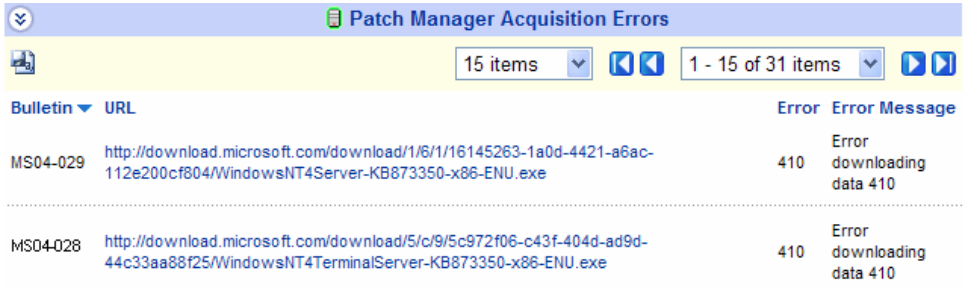


Start Time	End Time	# Bulletins	# Patches	# Errors	Publishing Machine
2004-10-26 14:39:42	2004-10-26 15:07:55	41	547		RPMACQ
2004-10-25 18:19:22	2004-10-25 18:32:30	7	110	31	RPMACQ
2004-10-18 16:30:06	2004-10-18 16:44:59	1	1		RPMACQ
2004-10-18 14:54:26	2004-10-18 16:18:00	36	116		RPMACQ

Click **# Bulletins** to see the acquisition summary sorted by bulletin or **# Patches** to see the acquisition summary sorted by patch files.

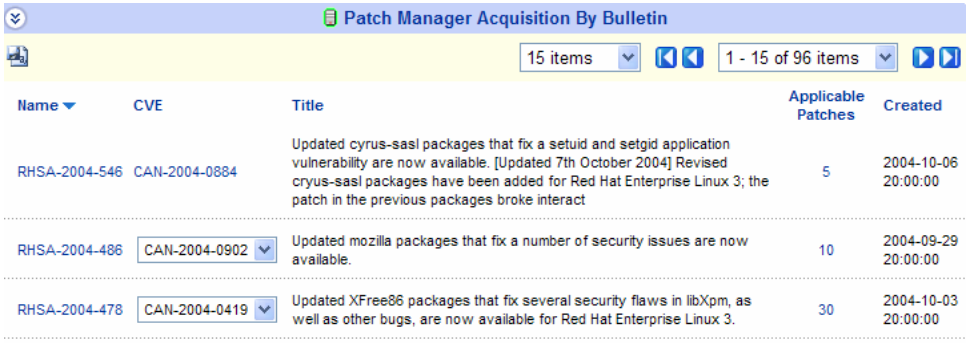
Click **# Errors** to see further explanations of why the acquisition failed. Numeric error codes displayed in the error reports are standard http status codes. For additional details on these codes, search for "HTTP Status Codes" on the World Wide Web.

Figure 7 View the acquisition error summary



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

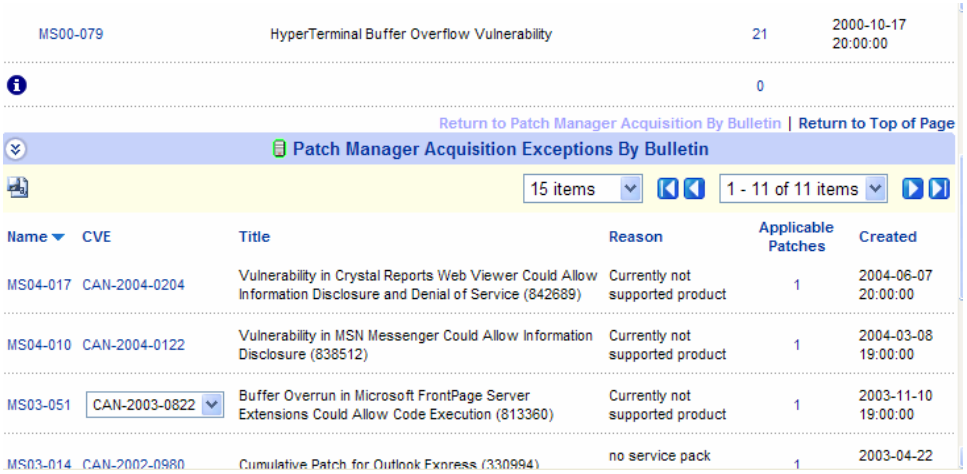
Figure 8 View the acquisition summary by bulletin



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

- 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



MS00-079	HyperTerminal Buffer Overflow Vulnerability	21	2000-10-17 20:00:00
		0	

Return to Patch Manager Acquisition By Bulletin | Return to Top of Page

Patch Manager Acquisition Exceptions By Bulletin

15 items | 1 - 11 of 11 items

Name	CVE	Title	Reason	Applicable Patches	Created
MS04-017	CAN-2004-0204	Vulnerability in Crystal Reports Web Viewer Could Allow Information Disclosure and Denial of Service (842689)	Currently not supported product	1	2004-06-07 20:00:00
MS04-010	CAN-2004-0122	Vulnerability in MSN Messenger Could Allow Information Disclosure (838512)	Currently not supported product	1	2004-03-08 19:00:00
MS03-051	CAN-2003-0822	Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)	Currently not supported product	1	2003-11-10 19:00:00
MS03-014	CAN-2002-0980	Cumulative Patch for Outlook Express (330994)	no service pack	1	2003-04-22

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

Figure 10 View the acquisition summary by patch

Patch Manager Acquisition By Patch

15 items | 16 - 30 of 528 items

Bulletin	Product / Release	QNumber	Patch Language	Superceded	Status	Size (bytes)	Date
MSSP-WIN2K_4	Windows 2000 Datacenter Server / Windows 2000 Gold		en	N	0	135,477,136	2004-09-15 11:54:17
MSSP-WIN2K_4	Windows 2000 Datacenter Server / Windows 2000 Service Pack 1		en	N	0	135,477,136	2004-09-15 11:54:17
MSSP-WIN2K_4	Windows 2000 Datacenter Server / Windows 2000 Service Pack 2		en	N	0	135,477,136	2004-09-15 11:54:17
MSSP-WIN2K_4	Windows 2000 Datacenter Server / Windows 2000 Service Pack 3		en	N	0	135,477,136	2004-09-15 11:54:17

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

Analyzing Microsoft Patch Files

If you are using the Configuration Analyzer to compare Microsoft patches, you will need to create patch state files. A state file is a highly tuned file format that is used to store information about an application or workstation at a particular point in time. Patch Manager allows you to generate state files only for Microsoft patches that have already been acquired in the Radia Database. Each parameter should be preceded by a hyphen with the value for the parameter following it. The parameters are described in Table 5 below. Parameters set on the command line will override those from the `patch.cfg` file.

Table 5 State File Creation Parameters

Parameter	Description
bulletins	Specify specific bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. Example: -bulletins MS00-001,MS00-029. Default: All bulletins.
rcs_pass	If authentication has been enabled on your Configuration Server, specify the password for the rcs_user.
rcs_url	Specify the location of your Configuration Server in URL format. 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. Note: This parameter is required.
rcs_user	If authentication has been enabled on your Configuration Server, specify the rcs_user.
state_dir	Specify the location to place the state files. Default: `C:\Novadigm\IntegrationServer\states`.

To create state files

1. From a command prompt on your Patch Manager computer, navigate to the Radia Integration Server's directory. The default location is

   ```
   System Drive:\Novadigm\IntegrationServer
   ```

2. Using the parameters listed in Table 5 on page 83, create a command line similar to the following:

   ```
   nvdkit ./modules/patch.tkd state -bulletins MS04-003
   ```

   This will create a state file for Microsoft Bulletin MS04-003.

Log files called `patch2state.log` and `advmnfst.log` are created in the current folder.

See the *Configuration Analyzer Guide* for instructions on how to use the state files.

Summary

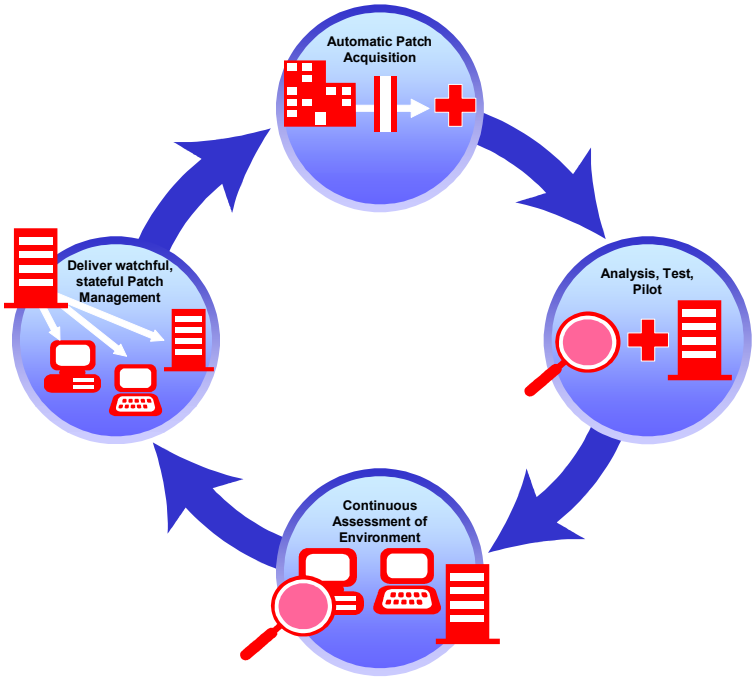
- Run Radia Patch Acquisition to acquire the patches and publish them to the Radia Database.
- The Patch information from the Radia Database automatically synchronizes with the Patch SQL Database.
- Use the Patch Acquisition reports to see the status of your acquisition.

4 Patch Assessment and Analysis

At the end of this chapter, you will:

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

Figure 11 Product discovery and analysis



Installing the Patch Manager Client

The Patch Manager client must be installed on any client computer that you want to manage vulnerabilities for. You can do this using the Management Portal or using the installation from the CD-ROM provided. For detailed installation instructions, see the *Management Portal Guide* or the *Application Manager Guide*. For minimum system requirements, see the *Application Manager Guide* for the appropriate operating system.

The minimum required version of nvdkit is 145 for the Patch Manager clients. If your client computers do not meet this requirement, see the technical support web site.

The directions shown below for installation through the Management Portal version 2.0. These screens and instructions may change in future versions. See the *Management Portal Guide* for additional information.

To install the Patch Manager client from the Management Portal

1. Copy the client maintenance files from the Patch Manager CD-ROM to the `\Novadigm\IntegrationServer\media\client\default\win32\maint` directory on the Management Portal computer.
2. Use the Management Portal's Install Client task to begin the installation process.
3. In the Management Portal's Client-opts screen, select **Patch Manager**.

4. Complete the remaining information in the Client-Opts screen.
5. Schedule the installation and submit the job.

If the Radia Management Agent is not already installed on the client computer, the Agent will be installed as part of the Patch Manager client installation.

To install from the CD-ROM for Windows clients

- Navigate to the appropriate subdirectory for you operating system on the Radia v4 applications CD-ROM. Double-click **setup.exe**. When prompted, select the Patch Manager client feature.

To use the install.ini file for Windows Clients

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

After installing the client, you will need to assign the appropriate services to the client computers.

To install from the CD-ROM for RedHat and SuSE Linux and HP-UX clients

- Navigate to the appropriate subdirectory for you operating system on the Radia v41 applications CD-ROM. Select the Patch Manager client feature during client installation.

To install the Patch Manager Agent on a UNIX operating system

The recommended minimum version of the Radia client that supports Patch Manager Agent Version 2.2 functionality is Radia Application Manager Version **4.1**. The absolute minimum build of `nvdkit` on the client, is build 145. The Patch Manager's maintenance file, `maint.tar`, must be applied to the client in order to enable the Patch Manager Agent. At the time of this writing; The Patch Manager Agent is supported on the following operating systems.

- **Linux**: Red Hat Enterprise Server versions 2.1, 3, and 4; and SuSE Enterprise Server versions 8 and 9.
- **HP-UX**: operating system releases 11.00 and 11.11 (11i).
- **Sun Solaris (SPARC)**: operating system releases 9 and 10.

The maintenance file (`maint.tar`) is located on the HP OpenView Patch Manager using Radia CD-ROM in the following operating system-specific directories.

- `Patch Agent Maintenance\linux\ram`
- `Patch Agent Maintenance\hpux\ram`
- `Patch Agent Maintenance\solaris\ram`

The supplied `maint.tar` files provided in the operating system specific folders on the CD-ROM are not interchangeable between client platforms.

To install the UNIX Patch Manager client from the Management Portal

These instructions are applicable to the UNIX Operating Systems noted in the section above. In these instructions, the operating system-specific

directories have been replaced with *XXXX*; in your environment this value will be `linux`, `hpux`, or `solaris`, depending on the operating system.

- Examine the contents of the Management Portal's sub-directory `IntegrationServer/media/client/`*XXXX*`/ram`.
  - If this sub-directory contains the file `client31.tar`, then copy the file `maint.tar` from `Patch Agent Maintenance\`*XXXX*`\ram` on the CD-ROM to it and **rename** the file, `maint31.tar`.
  - If this sub-directory contains the file `client41.tar`, then copy the file `maint31.tar` from `Patch Agent Maintenance\`*XXXX*`\ram` on the CD-ROM to it and **rename** the file, `maint41.tar`.

At minimum, HP OpenView using Radia client version 4.1 is required to enable reboot management capabilities, and resume patch management processing after a reboot. To use this feature, the Radia Scheduler (radsched) must be enabled as a system Service. Installation of the Radia client daemons as system services can be performed as a post installation task during the installation of the Radia Application Manager client. For additional information on UNIX client post installation tasks, please see the HP OpenView Radia Application Manager Installation and Configuration Guide.

Sun Solaris Patch Agent pre-requisites

Sun Patch Manager 2.0 is required to use HP OpenView Using Radia 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 9 client OS pre-requisites

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 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 HP OpenView Patch Manager.

In addition, you are required to 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 client OS pre-requisites

For Sun Solaris 10, the base Operating system install must include the **Developer Software Support Group of Solaris 10,** which provides Sun™ Patch Manager Version 2.0, which is used to perform Sun Alert Vulnerability scans.

Sun Solaris Single User Patch Installations

For Sun Solaris patches requiring installation, when the client computer is in single user mode, apply the supplied shell script `S07radiapm` located in the Patch Agent Maintenance`\solaris\singleuser` folder on the CD-ROM to the appropriate Sun Solaris client directory.

- If your client computer is a *Solaris 9* based system install the script in the /etc/rc2.d directory. Change the permissions of the shell script to ensure it is executable by 'root'. You can install this file on a Sun Solaris client using a post installation task during the installation of the Application Manager client. For additional information on UNIX client post-installation tasks, see the *Installation and Configuration Guide for the HP OpenView Radia Application Manager*.
- If your client computer is a *Solaris 10* based system install the script in the `/etc/init.d` directory. Change the permissions of the shell script to ensure it is executable by 'root'. You can install this file on a Sun Solaris client using a post installation task during the installation of the Application Manager client. You must also install the supplied text file `radia-single.xml` located in Patch Agent Maintenance `\solaris\singleuser` on your Sun Solaris 10 client computer. The introduction of the Service Management Facility (SMF) in Solaris 10 requires this system modification on a Solaris 10 based client computer for the Radia Patch Manager single user patch installation facility to function properly. Verify that `radia-single.xml` is placed in the Sun Solaris 10 client 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 client post-installation tasks, see the *Installation and Configuration Guide for the HP OpenView Radia Application Manager*.

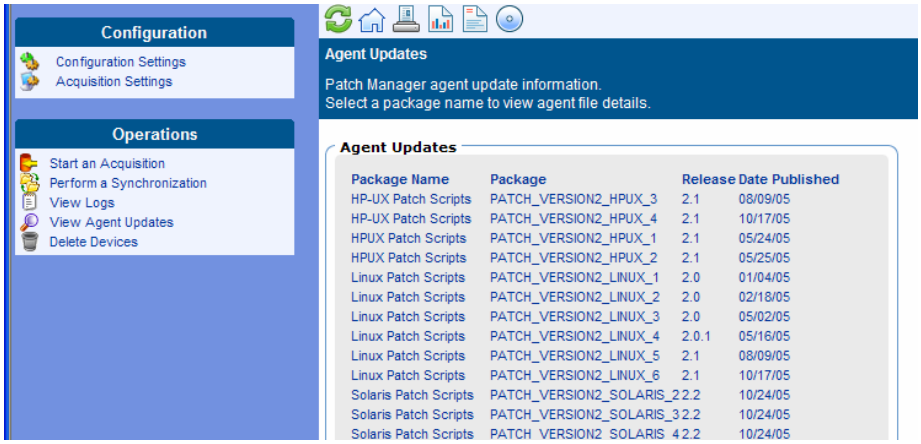
Updating the Patch Manager Client Agent

When you run a patch acquisition, you can also download updated product discovery 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. The AGENT_UPDATES parameter, specified during an acquisition session, controls script update processing.

As of Patch Manager, Version 2.0, the auto packaging feature will reapply Patch Manager agent maintenance files if a user deleted them between Radia connects.

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



Client agent files are distributed when the Discover Patch Service is processed on the Patch Manager client computer. 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 client agent maintenance packages created when you selected Publish or Publish, 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 System Explorer to do this. An example is shown below.

Figure 13 Create connections to the published package

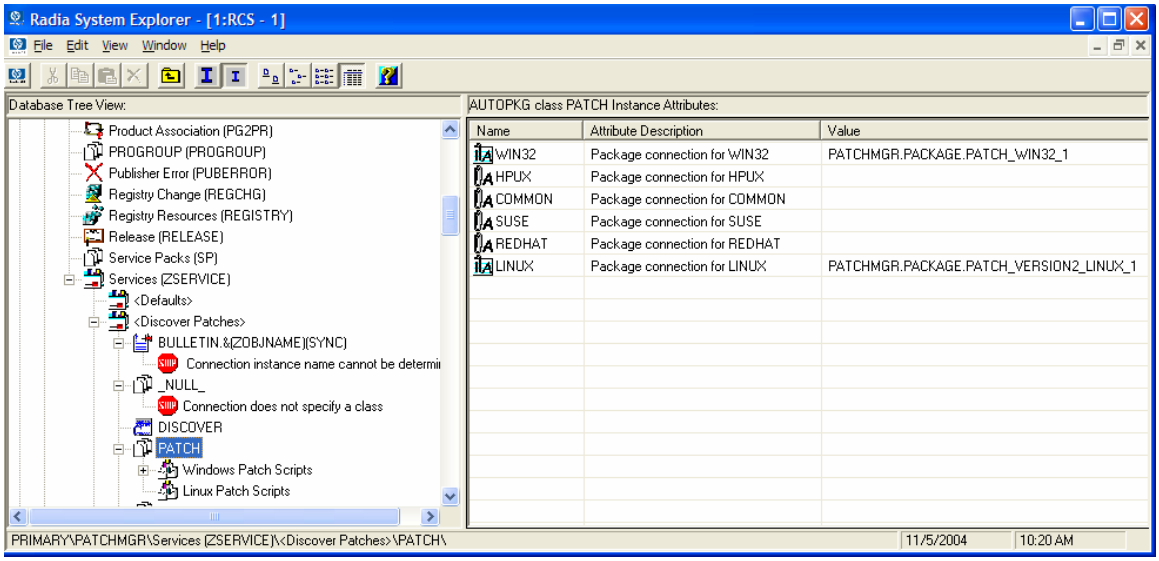


Table 6 AGENT_UPDATES Values

Value	Description
"" or blank	The agent updates will not be published to the Radia Database's 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 client computers.
Publish	The updates will be published to the PATCHMGR domain, but will not be connected for distribution to Patch Manager client computers. You will need to create these connections.

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

- Agent_os
  Use –agent_os to specify which operating systems to acquire the agent updates for. The default is to download all operating systems. Valid values are win32, linux, suse, and hpux. Note that RedHat, SuSE, Solaris, and HP-UX agent update are only available starting with version 2.0.
- Agent_version
  Use –agent_version to select which 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.
  - To update for version 2, specify –agent_version version2.
  - To update for version 1.2, specify –agent_version version1_2. (This is the default setting for backward compatibility.)

Product Discovery and Analysis

Before you can manage vulnerabilities, the Patch Manager client must discover which products are on the client computer. Patch Manager objects are cached locally on the client device to optimize bandwidth. Objects are downloaded only if they are different. In addition, the Patch Manager client needs to detect which patches are installed for each discovered product. To do this, assign the Patch Manager Discover Patch Service to the client computers.

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

To perform patch discovery

1 Connect your client computer (e.g. POLICY.USER.&(ZUSERID)) directly to the PATCHMGR.ZSERVICE.DISCOVER_PATCH service.

During a Solaris Patch Manager connect, applicable Solaris patches are downloaded and queued for management by a Patch Manager Service called FINALIZE_PATCH. This service must be specified in the client computer's policy. This service is prioritized to run as the last service on Patch Manager client agents. If you do not include this service in the client computer's policy, the client agent will fail to successfully apply Sun Alerts.

2 Create a radskman command line to make a regular client connect. At a minimum, the command line should look like:

```
radskman ip=<RadiaConfigurationServerIPaddress>,
   port=<RadiaConfigurationServerport>,dname=patch
```

For additional information on creating a radskman command line, see the *Application Manager Guide*.

Detecting and Managing Microsoft Office Security Bulletins

Patch Manager can detect Microsoft Office security vulnerabilities. It has the capability to manage Microsoft Office vulnerabilities for locally installed Microsoft Office applications. Locally installed means that the installation was performed from a CD-ROM in its native format, specifically not an administrative control point.

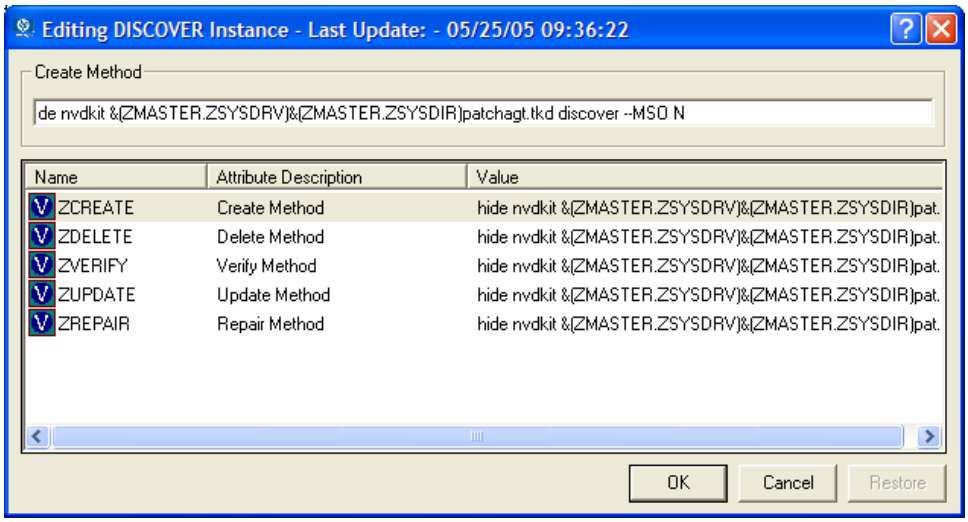
You may want to update Microsoft Windows Installer to versions 3.0 or 3.1. These versions contain considerable enhancements to the efficiency of managing patches for Windows Installer applications. Also, please note that some patches will require access to the original installation media. Be sure to test detection and deployment of vulnerabilities before deploying to a production environment.

Patch Manager does not support patch management for Office 95 and Office 97. Currently supported products include Office 2000, Office XP, Office 2003, as well as stand alone products such as Project 2002. For Microsoft Office applications that are either managed by HP OpenView using Radia or an ACP Install Source, the Patch Manager client Agent will *only* detect and report on the vulnerabilities.

Application Manager administrators are urged to use the MSI ACP patching technology built into the recent Radia offerings

Microsoft Office vulnerability detection is turned on by default. you may turn this feature off by modifying the PATCHMGR.CMETHOD.DISCOVER instance. If you want to turn off Microsoft Office detection, set the MSO parameter to N in all attributes of the instance as shown in the figure below.

Figure 14 Microsoft Office detection is turned off.



Patch Manager supports deployment and acquisition of Microsoft Office Service Packs. In some cases, Microsoft will determine that a particular Office patch is dependent on a specific Service Pack. In those cases, it will be necessary to distribute the Office Service Pack prior to installing the patch. 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 client 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 client 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 client computer will *still* be out of compliance because MS05-005 has not been installed. In other words, for this client 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 client computer has not been entitled to it in policy.

If you are using either Radia or an ACP (Administrative Control Point), you will see a comment in the Compliance reports, specifying that Patch Manager does not manage these types of Microsoft Office installations.

About ZOBJSTAT

The ZOBJSTAT object is created during patch resolution. This object contains information about what products and patches are installed on the client computer. During the resolution process, ZOBJSTAT is sent to the Configuration Server. Instead of storing the information in the Radia Database, the object's content is copied to a directory that is monitored by the Radia Messaging Service. The default location of this directory is *System Drive*:\Novadigm\ConfigurationServer\data\patch. The Radia Messaging Service exports this information to the Patch ODBC Database for storage and analysis. Only the most recent ZOBJSTAT for each client computer is kept. Furthermore, all client device information is stored in the ODBC Database, not in the Radia Database as in previous releases.

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 15 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 4.1.1 provides web-based reports for Patch Manager. For installation and configuration instructions for the Reporting Server, see the *Reporting Server Guide*. The installation media is on the Radia Infrastructure CD-ROM. To view the reports, first access your Reporting Server. Then, under Reporting Views, click **Software Patch Reports** to expand the list of reports.

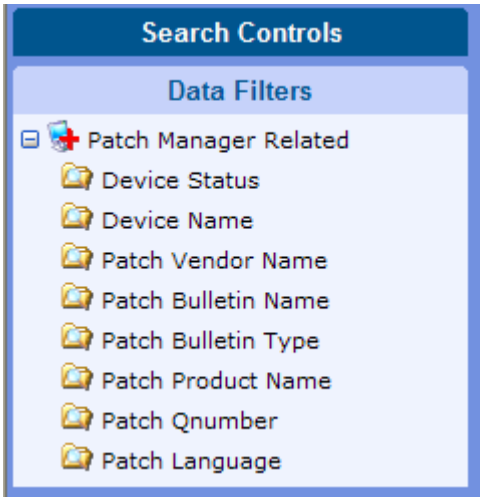
Figure 16 View the list of Patch Manager reports

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

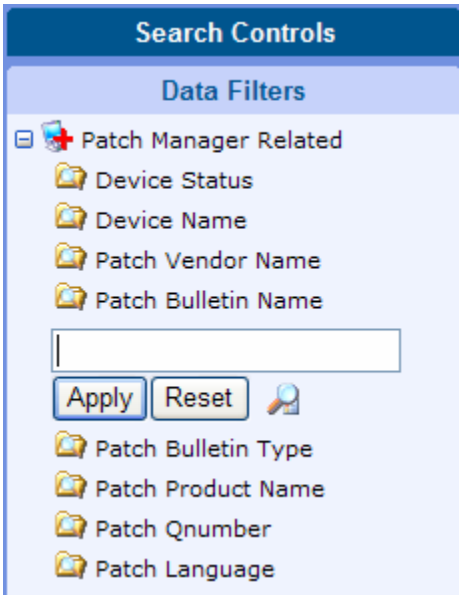
Reporting Server also provides filtering capabilities. To access the filters, expand Patch Manager Related in the Search Controls section of the Reporting Server page.

Figure 17 View the Patch Manager Related Data Filters



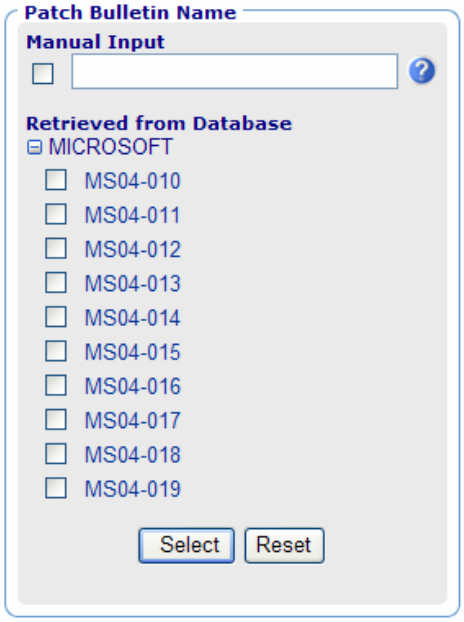
Some filters only allow a text entry. Others have a Show available options button or magnifying glass to open a filter lookup window.

Figure 18 Expand a filter



Click the magnifying glass to open the filter lookup window.

Figure 19 Select the filter.



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 see the *Reporting Server Guide*.

Compliance Reports

When a device in your enterprise runs the Patch Manager client, product and patch information is sent to 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 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.

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 bulleting.

— 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 Products column to see the products for the 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 client device is rebooted.
- Click the number in the Total column to see all patches that are relevant to this bulletin.

- **Compliance by Device**
  Use this report to see the vulnerabilities for devices under Radia 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.

Status	Name	CVE	Product / Release	Applicable Products	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pending	Total
	KB840987	CAN-2004-0200	Windows Server 2003, Enterprise Edition / Windows Server 2003 Gold	1	1	0	0	1	0	0	1
	KB841533	CAN-2004-0200	Windows 2000 Professional / Windows 2000 Service Pack 3	1	1	0	0	1	0	0	1
	KB841533	CAN-2004-0200	Windows 2000 Professional / Windows 2000 Service Pack 4	1	1	0	0	1	0	0	1

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.

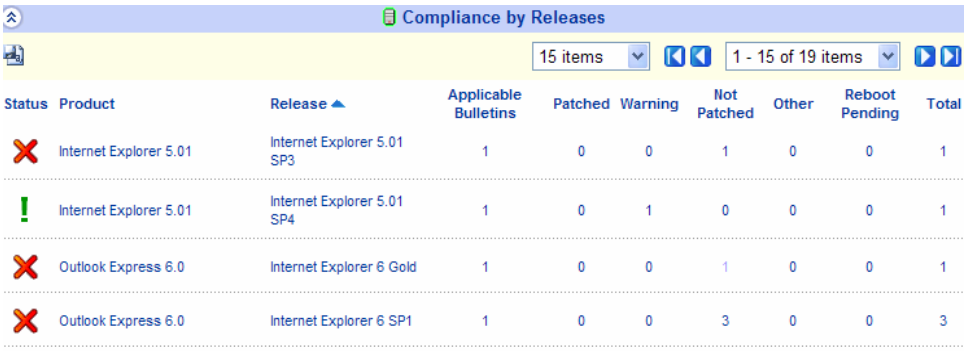
Another example may be that a file version on the device is newer than the one delivered by the patch. Again, in this case, Patch Manager cannot report the vulnerability as being patched so it reports a warning.

- 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 client 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.

- **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.

Status	Product	Applicable Devices	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗	Internet Explorer 5.01	2	1	0	1	1	0	0	2
✗	Internet Explorer 6	3	5	0	0	10	0	0	10
✓	Internet Explorer 6.0 for Windows Server 2003	1	1	1	0	0	0	0	1
✗	Internet Information Services 5.0	1	1	0	0	1	0	0	1

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



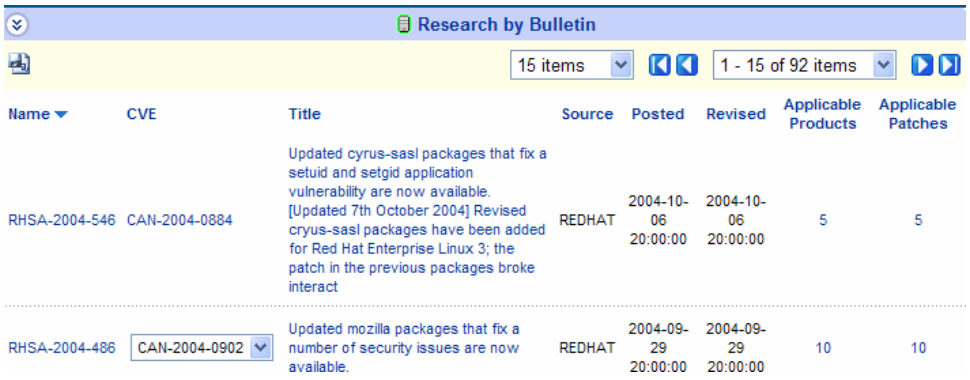
- **Compliance by Patches**
  This report lists products by patch. There is one row for each patch. Click to see Applicable Products and Applicable Devices.

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.

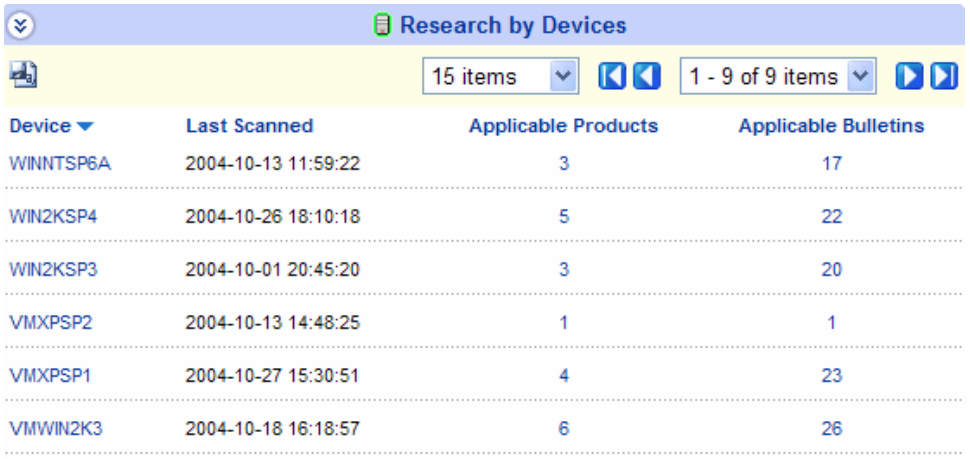
- **Research by Bulletin**
  Use this report to drill down to all bulletins. Click on the bulletin's number in the Name column to go to the vendor's web site for more information. Click on the number in the CVE column to go to the Common Vulnerability Exposures web site. Click the number in the Title 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

superceded by another patch. Click the number in the Applicable Products column to see which products are influenced by this bulletin.



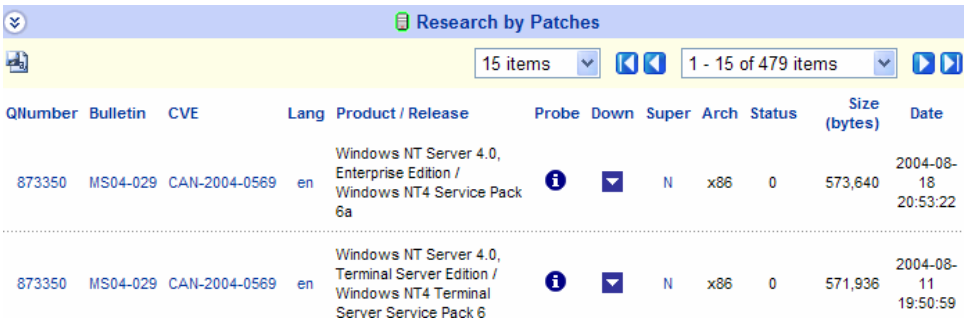
Name	CVE	Title	Source	Posted	Revised	Applicable Products	Applicable Patches
RHSA-2004-546	CAN-2004-0884	Updated cyrus-sasl packages that fix a setuid and setgid application vulnerability are now available. [Updated 7th October 2004] Revised cryus-sasl packages have been added for Red Hat Enterprise Linux 3; the patch in the previous packages broke interact	REDHAT	2004-10-06 20:00:00	2004-10-06 20:00:00	5	5
RHSA-2004-486	CAN-2004-0902	Updated mozilla packages that fix a number of security issues are now available.	REDHAT	2004-09-29 20:00:00	2004-09-29 20:00:00	10	10

- **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.

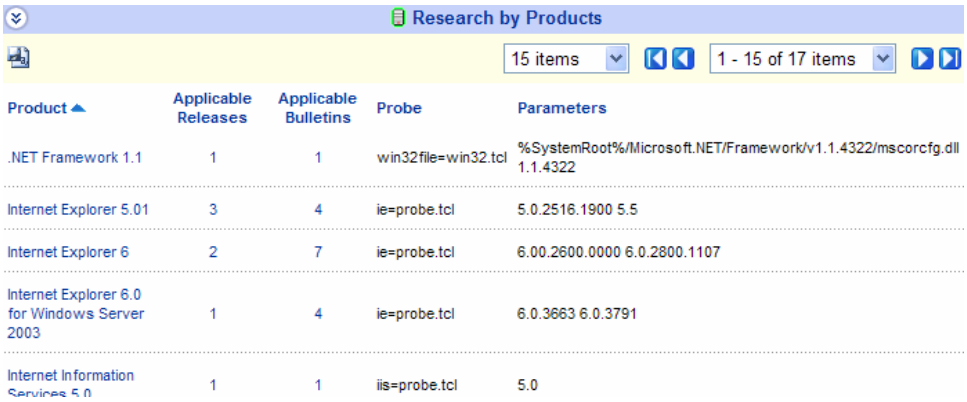


Device	Last Scanned	Applicable Products	Applicable Bulletins
WINNTSP6A	2004-10-13 11:59:22	3	17
WIN2KSP4	2004-10-26 18:10:18	5	22
WIN2KSP3	2004-10-01 20:45:20	3	20
VMXPSP2	2004-10-13 14:48:25	1	1
VMXPSP1	2004-10-27 15:30:51	4	23
VMWIN2K3	2004-10-18 16:18:57	6	26

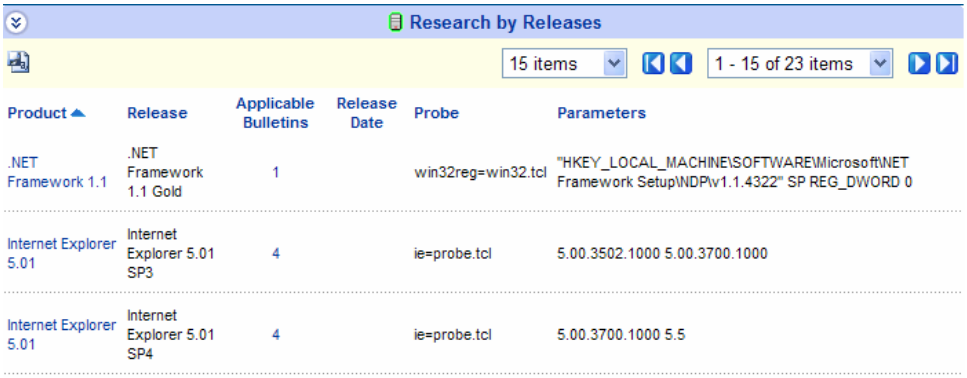
- **Research by Patches**
  Use this report to view information on patch files including on acquisition status. Click the number in the CVE column to go to the Common Vulnerability Exposures web site. Click the icon in the Down column to download the patch file.



- **Research by Products**
  Use this report to drill down to all bulletins filtered by product.



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



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:

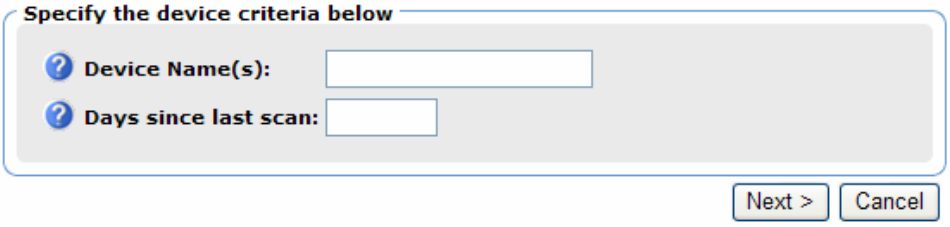
- connection errors during patch discovery
- an acquisition performed with force and replace options that caused a disconnect with the client's status information
- an inoperable Patch Client Agent

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 Client 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 20 Delete devices.

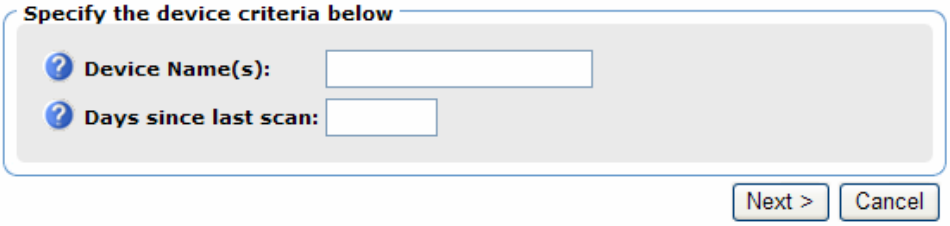


Enter device selection criteria for the devices to remove. You may:

- 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 to client 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. See the *Application 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 OpenView web site for details.

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

Notes on Solaris Patch Management

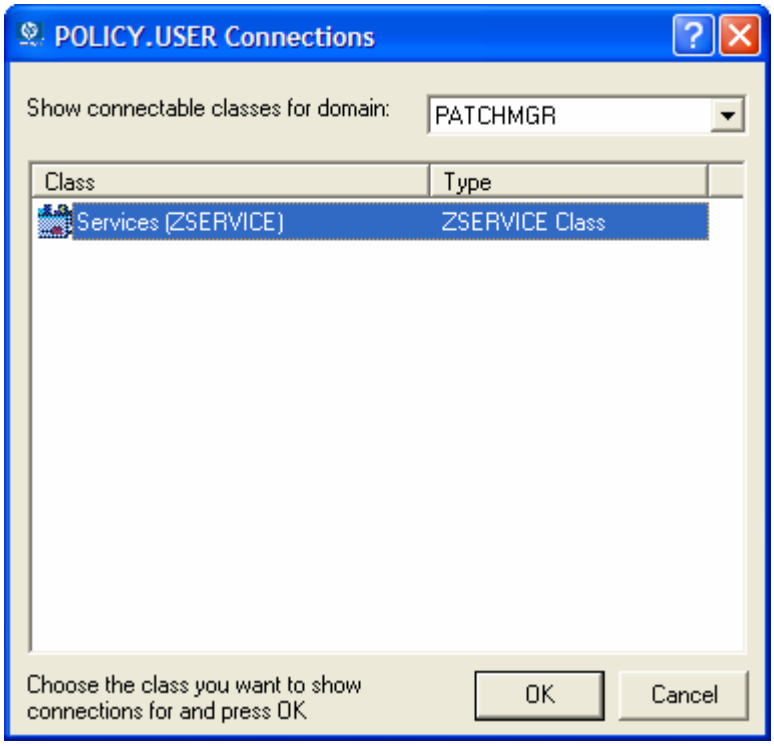
During a Solaris Patch Manager connect, applicable Solaris patches are downloaded and queued for management by a Patch Manager Service called FINALIZE_PATCH. This service must be specified in the client computer's policy. This service is prioritized to run as the last service on Patch Manager client agents. If you do not include this service in the client computer's policy, the client agent will fail to successfully apply Sun Alerts.

The Patch Manager client 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.

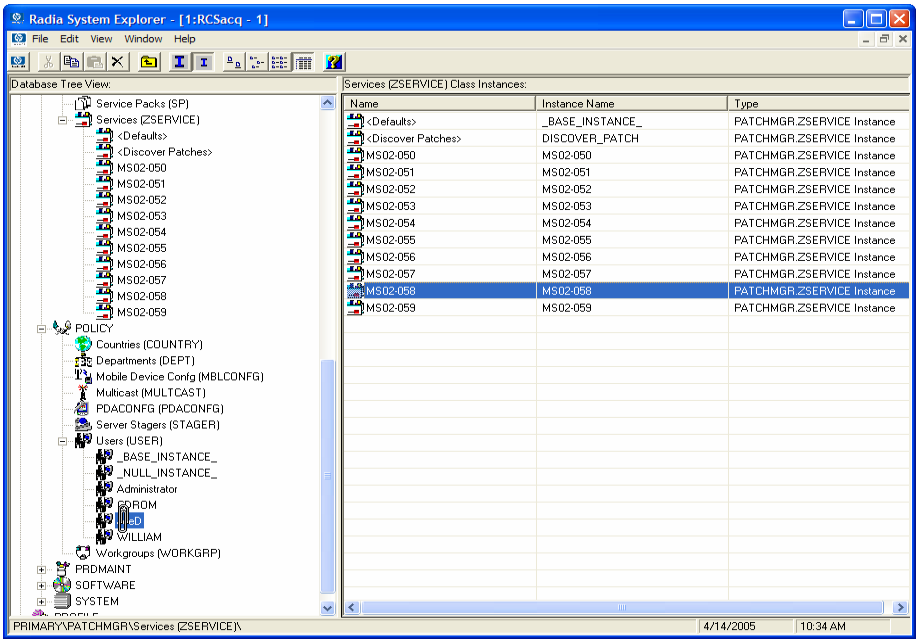
To manage a vulnerability

1. Right-click a user instance and select **Show Connections**.
2. Select the **PATCHMGR** domain from the drop-down box as shown in the figure below.



3 Click **OK**.

4 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.



5 Click **Copy**.

6 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.

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 client 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 client connect.

For more information on radskman, see the *Application 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 !) 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. 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 from Table 7 on page 118 with a return code from Table 8 on page 118. Separate multiple conditions with commas.

Table 7 DesiredState Tag (DSTATE) and Descriptions

State	Description
E	Exists Use this if your only criterion for status is if the file or registry key exists.
!E	Does not exist Use this if your only criterion for status is if the file or registry key does *not* exist.
EQ	Equal If the file or registry key meets the exact criteria.
!EQ	Not equal If the file or registry key does not meets at least one of the criteria.
LT	Less than If the file or registry key is less than at least one of the criteria.
GT	Greater than If the file or registry key is greater than at least one of the criteria.

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.

Table 8 Return Code Values

Return Code	Description
0	OK
4	Warning
8	Error

The sample code below shows 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.

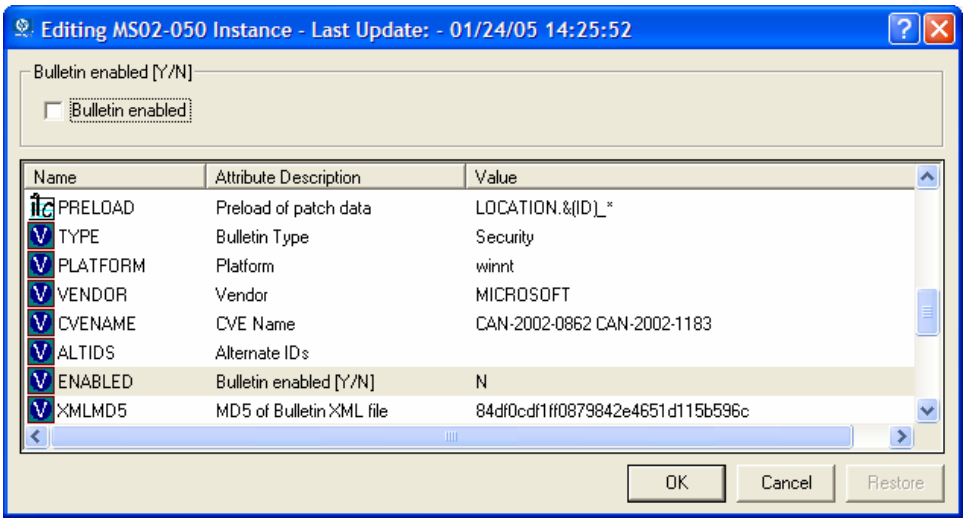
3 Set a REPORT threshold. The properties of the file or registry key will be sent to the Patch Manager based on this value. If the return code is greater than or equal to the value of the REPORT attribute, the file and registry information will be sent to the Patch Manager and will be available in Patch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

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 System Explorer to set the ENABLED attribute to N in the Bulletin or Patch instance in the PATCHMGR domain.

Figure 21 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.

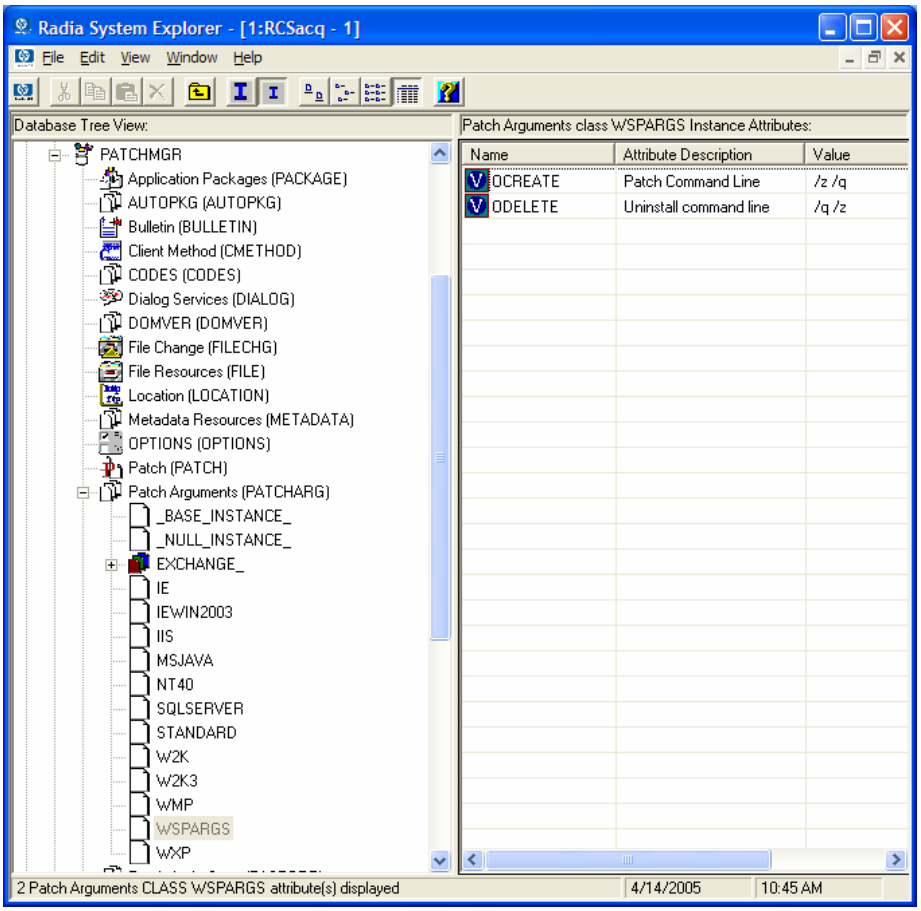
Controlling Patch Deployment (PATCHARG)

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.

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.

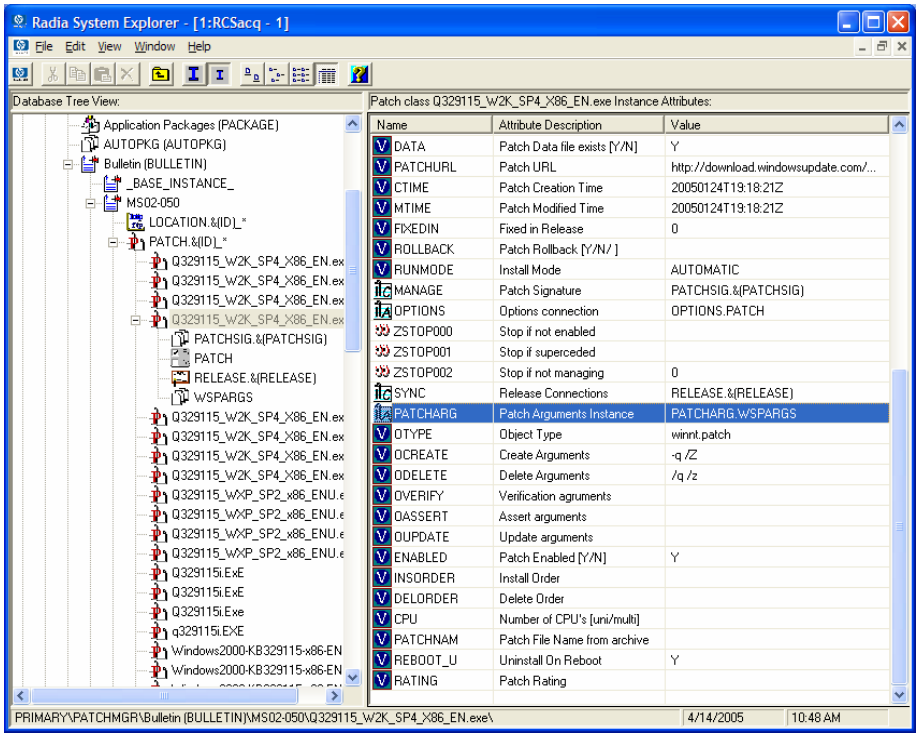
To create alternate command line parameters using PATCHARG

1. Use the System Explorer 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 Proxy Server and Staging Servers

If you are using a Proxy Server or Staging 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 or Staging Server will load the compressed data files from the PATCHMGR domain. For more

information on preloading, see the *Proxy Server Guide* or the *Staging 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 client computer 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 123 for additional information.

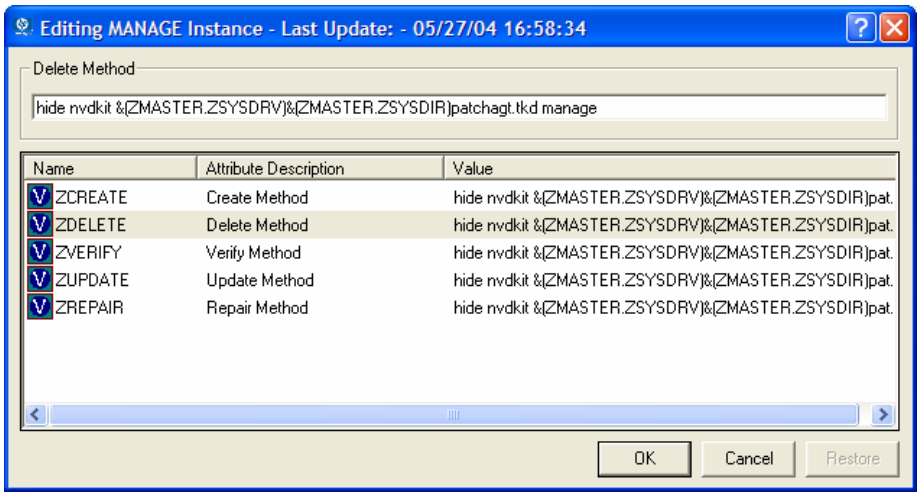
To remove a patch when a user is no longer assigned the service

1 Use the System Explorer to navigate to the MANAGE instance of the Client Method (CMETHOD) class in the PATCHMGR domain.

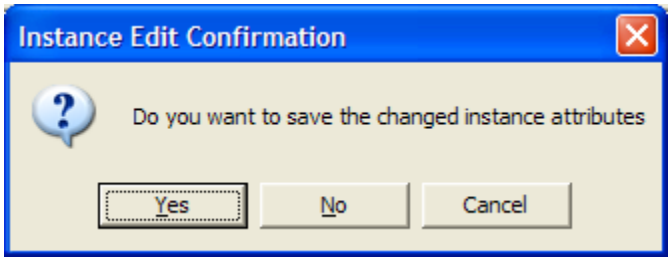
2 Double-click the ZDELETE attribute in the tree view.

3 In the text box, type:

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



4 Click **OK** to change the instance.



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

6 The Patch Manager client must make a connect for the client 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

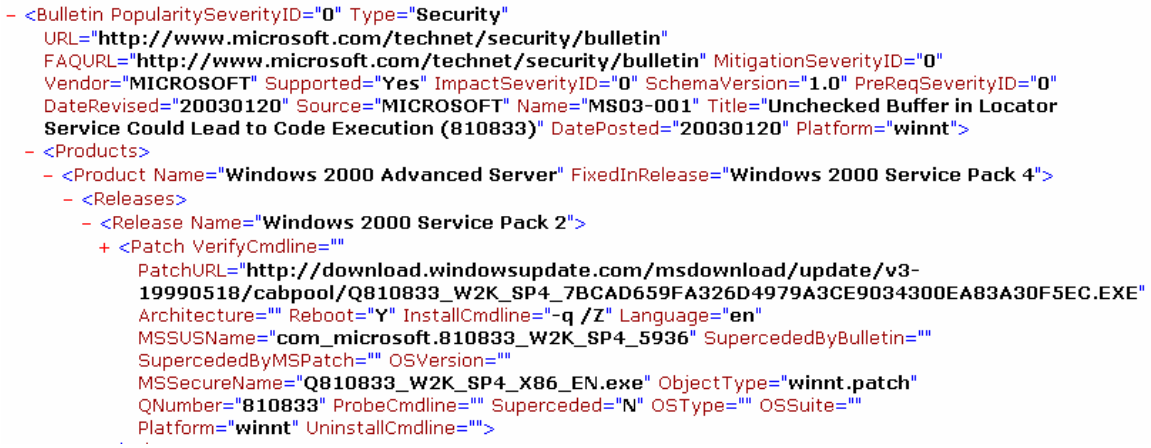
- Install the Patch Manager client on devices that you want to manage.
- Patch Manager supplies you with research, patch acquisition, and vulnerability reports.
- Use the reports to identify vulnerabilities in your enterprise.
- Manage vulnerabilities by assigning the patch's service to your client computers.

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 the figure.

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 22 View a sample patch descriptor file.



Bulletin Node

Node name: Bulletin

Parent node: None

Children: Products

Table 9 XML Tags in the BULLETIN class

XML Tag	Radia 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`

XML Tag	Radia Attribute	Description
Supported	SUPPORT	Supported [Y/N] Source: MSSECURE.XML
ImpactSeverityID	IMPACT	ImpactID Source: MSSECURE.XML
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
Source	SOURCE	Source [MICROSOFT/NOVADIGM /CUSTOM] Directory from which the patch descriptor file was published.
Vendor	VENDOR	MICROSOFT/REDHAT/HPUX
Type	TYPE	Type of Bulletin Security/ServicePack/Other
Platform	PLATFORM	Winnt/linux
Name	NAME	External ID Source: MSSECURE.XML
Title	TITLE	Title Bulletin title. Source: MSSECURE.XML
DatePosted	POSTED	Bulletin Posted On Date the bulletin was posted in YYYYMMDD format. Source: MSSECURE.XML

XML Tag	Radia Attribute	Description
Schema Version		The patch schema version currently 1.0
	MTIME	Time the instance was modified in the Radia Database.
	CTIME	Time the instance was created in the Radia Database.
	ID	Internal instance ID.
HPPosted	HPPOSTED	Date the bulletin was initially posted by HP.
HPRevised	HPREVISD	Date the bulletin was revised by HP.
Deployment	RUNMODE	Specifies whether the patch can be installed automatically (AUTOMATIC) or needs user interaction (INTERACTIVE).

Products Node

Node name: Products

Parent node: Bulletin

Children: Product

Attributes: None

Product Node

Node name: Product

Parent node: Products

Children: Releases

Table 10 XML Tags in the PRODUCT class

XML Tag	Radia Attribute	Description
Name	NAME	Source: `MSSECURE.XML`
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 11 XML Tags in the RELEASE class

XML Tag	Radia Attribute	Description
Name	NAME	Source: `MSSECURE.XML`

Patch Node

Node name: Patch

Parent node: Release

Children: Package

Table 12 XML Tags in the PATCH class

XML Tag	Radia Attribute	Description
PatchURL	PATCHURL	A URL that points to an .EXE or .MSI file. Source: `MSSECURE.XML/SUS`
Reboot	REBOOT	Specified if the client device should be rebooted, after the patch is installed. Source: `MSSECURE.XML/SUS`
Architecture	ARCH	x86|i64 Source: `MSSECURE.XML/SUS`
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 supercedes this patch. Source: `MSSECURE.XML`
SupercededByMSPatch	SUPERMSS	The MSSECURE patch name that supercedes this patch. Source: `MSSECURE.XML`
Superceded	SUPERCED	Specifies if the patch has been superceded. Valid values are Y or N. Source: `MSSECURE.XML`

XML Tag	Radia Attribute	Description
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,win9x,hpux,solaris,linux.
InstallCmdline	OCREATE	This is the arguments that are passed to the create procedure. Source: SUS
VerifyCmdline	OVERIFY	The Verify Arguments.
UninstallCmdline	ODELETE	The Uninstall Arguments.

XML Tag	Radia Attribute	Description
ObjectType	OTYPE	Format: namespace=script filename Default: winnt.patch This specifies the type of the object and the name of the script file that would have the following procedures defined verify create delete assert The procedures should have the namespace as part of the name, e.g., winnt.patch::create. If the script filename is not specified then the filename is {namespace}.tcl. Source: Novadigm
ProbeCmdline	OVERIFY	The probe command line. Source: Novadigm
	ID	The unique ID created in the RCS database for this patch.
	PATCHSIG	The name of the Patch Signature instance. Source: Novadigm
	LOCATION	The name of the LOCATION instance that contains the patch data.
	BULLETIN	The bulletin name set during publishing. Source: MSSECURE.XML

XML Tag	Radia 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

Chidren: None

Table 13 XML Tags in the FILECHG class

XML Tag	Radia 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`

XML Tag	Radia Attribute	Description
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 RCS database. Source: Novadigm
	REPORT	The report threshold. If on evaluation of this file change instance the RC is greater than the threshold then we will create a ZOBJSTAT for that instance. Source: Novadigm
	USE	The variables to use during comparison, e.g., Version,Checksum,Gmtdate. Source: Novadigm

RegChg Node

Node name: RegChg

Parent node: PatchSignature

Children: None

Table 14 XML Tags in the REGCHG class

XML Tag	Radia Attribute	Description
Name	NAME	Value Name. Source: MSSECURE.XML

XML Tag	Radia Attribute	Description
Path	PATH	The fully qualified Registry Key Name. Source: MSSECURE.XML
Value	VALUE	The Data value stored in the registry. Source: MSSECURE.XML
Type	TYPE	Registry data type should be one of the following: sz = Simple Registry String multi_sz = Registry Multi String expand_sz = Registry string with environment variables dword = Registry dword binary = Binary data Source: MSSECURE.XML
	DSTATE	The desired state of the FILECHG instance, this is usually classed in from another instance in the RCS database. Source: Novadigm
	REPORT	The report threshold. If on evaluation of this file change instance the RC is greater than the threshold then we will create a ZOBJSTAT for that instance. Source: Novadigm
	USE	Not used. Source: Novadigm

HPFileset Node

Node name: HPFileset

Parent node: PatchSignature

Children: None

Table 15 XML Tags in the HPFSET class

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

B Restarting the Client Computer

You may need to restart a client computer 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.

First, specify the application event that needs the reboot. Table 16 below lists the codes for all possible application events. 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 radksman command line, the parameter defaults to Y to handle service reboot requests. If you set hreboot to p, the client computer 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.

Table 16 Reboot Events and Codes

Application Events	Code	Description
Install	AI	Use AI to specify a reboot behavior for application installations. The default is no reboot.
Deinstall	AD	Use AD to specify a reboot behavior for application removals. The default is no reboot.
Locked File	AL	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).
Update	AU	Use AU to specify a reboot behavior for application updates. The default is no reboot.
Repair	AR	Use AR to specify a reboot behavior for application repairs. The default is no reboot.
Version Activation	VA	Use AI 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. Radia 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 client computer 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 Radia Software Manager and for Application Manager used with the Radia System Tray. If you do not want to show a warning message, specify ask=N in a radskman command line.

Radia Clients for Linux do not display reboot panels.

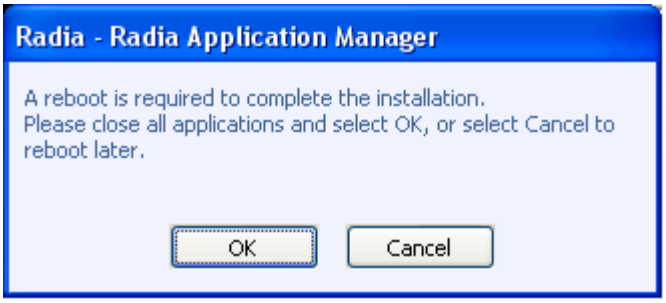
- **Quiet (Q)**
  No reboot panel will be displayed.

- **OK Button (A)**
  A warning message will display with an OK button only. Clicking the OK button will initiate the reboot. The user will not be able to cancel the restart.
- **OK and Cancel Button (Y)**
  Clicking the OK button will initiate 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 Radia Client to wait before continuing with the reboot process.

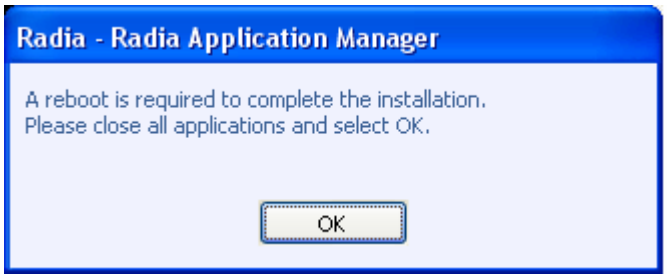
For example, the default Reboot panel displays both an OK and Cancel as shown in the figure below.

Figure 23 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 24 Change the reboot panel to show only the OK button.



Reboot Modifier: Machine and User Options

The Radia Client 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 client 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. Radia 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 Client 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 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 will want to 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 a Patch Manager client, 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 3.2.1.

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 { * }`.

Index

A

acquire command, 80
Acquire Microsoft Patches acquisition setting, 69
Acquire RedHat Patches acquisition setting, 69
acquisition settings, 67
agent_os parameter, 41, 97
agent_updates parameter, 41
agent_version parameter, 41, 97
Applicable Bulletins column, 108, 109, 112
Applicable Devices column, 107, 109
Applicable Patches column, 110
Applicable Products column, 107, 108, 111
ARCH attribute, 134
arch parameter, 72
Architecture acquisition setting, 70
Architecture tag, 134
AutoImport directories, 18, 55
automated import server, 55
automatic patch, definition, 117
AUTOPKG class, 95
AUTOPKG.PATCH instance, 96

B

bandwidth optimization, 97
Browse by Bulletin, 110
Browse by Device, 111
Browse by Patch, 111
Browse by Product, 112
Browse by Release, 112
BULLETIN attribute, 136
Bulletin column, 106
Bulletin node, 130
bulletin, definition, 16
Bulletins acquistion setting, 67
bulletins parameter, 72, 85

C

catexp parameter, 118
CHECKSUM attribute, 139
Checksum tag, 139
class parameter, 53
commit parameter, 53
Compliance and Research Exception Reports, 113
compliance assessment, 14
Compliance by Bulletin, 105
Compliance by Device, 107
Compliance by Patch, 110
Compliance by Product, 109
Compliance by Release, 109
compliance data
  removing, 113
compliance reports, 105
config parameter, 74
CRC32 attribute, 138
CRC32 tag, 138
CTIME attribute, 132
custom xml file, creating, 118
customer support, 3
CVE column, 106, 111

D

DATA attribute, 137
data_dir parameter, 42, 43, 74
databases
  synchronizing, 61
  synchronizing manually, 52
DatePosted tag, 131
DateRevised tag, 131
Deinstallapplication event, 144
deployment, 14

Deployment tag, 132, 137
descriptor file, creating, 80
DesiredState attribute, 118
DesiredState tag, 120
Discover Patch instance, 41
Discover Patch Service, 95
dsn parameter, 34, 43, 53
dsn_pass parameter, 34, 43, 53
dsn_user parameter, 34, 43, 53
DSTATE, 120
  valid values, 120
DSTATE attribute, 118, 137, 139, 140

E

exclamation point, 108

F

FAQURL attribute, 130
FAQURL tag, 130
FILECHG class, 118
FILECHG instance, 119
FileChg node, 138
filter bar, 110
filtering patch reports, 102
FINALIZE_PATCH, 98, 115
FIXEDIN attribute, 133
FixedInRelease tag, 133
Force acquisition setting, 68
force parameter, 74
ftp_proxy_pass parameter, 43, 75
ftp_proxy_url parameter, 43, 75
ftp_proxy_user parameter, 43, 75

G

GMTDATE attribute, 138
Gmtdate tag, 138
GMTTIME attribute, 138
Gmttime tag, 138

H

hard reboot, 145
history parameter, 40, 44, 75
host parameter, 53
HPFileset node, 140
HPPOSTED attribute, 132
HPPosted tag, 132
HPREVISD attribute, 132
HPRevised tag, 132
HPUX Security bulletins, 67
http_proxy_pass parameter, 39, 44, 75
http_proxy_url parameter, 39, 44, 75
http_proxy_user parameter, 39, 44, 75
http_timeout parameter, 39, 45, 76

I

ID attribute, 132, 136
impact analysis, 14
IMPACT attribute, 131
ImpactSeverityID tag, 131
Install application event, 144
Install Client task, 91
install.ini file, 92
InstallCmdline tag, 135
interactive patch, definition, 117

K

Knowledge Base Manager, 55

L

LANG attribute, 134
lang parameter, 42, 45, 76
Language tag, 134
Languages acquisition setting, 69
LDAP directory, 17
LOCATION attribute, 136
Locked File application event, 144

M

magnifying glass, 108
Microsoft feed settings, 35
Microsoft MSDE, 107, 108
Microsoft Security bulletins, 67
Microsoft SQL server, 22, 107, 108
microsoft_sus_url parameter, 35, 45

microsoft_url parameter, 35, 45
MITIGATE attribute, 131
MitigateSeverityID tag, 131
Mode acquisition setting, 68
mode parameter, 76
MSSECURE.XML file, 35
MSSecureName tag, 135
MSSNAME attribute, 135
MSSUSName tag, 134
MTIME attribute, 132
multiple reboot events, 148

N

NAME attribute, 131, 133, 138, 139, 141
Name tag, 131, 133, 138, 139, 141
no reboot, 145
Not Patched column, 107, 109
not-patched status, 108
nvd_attributename attribute, 52
nvd_classname table, 52
nvdm_url parameter, 34, 46

O

O/S Filter acquisition setting, 36
ObjectType tag, 136
OCREATE attribute, 122, 135
ODELETE attribute, 122, 135
OPTIONS class, 118
OPTIONS instance, 119
OSSUITE attribute, 135
OSSuite tag, 135
OSTYPE attribute, 135
OSType tag, 135
OSVER attribute, 135
OSVersion tag, 135
Other column, 107, 109
OTYPE attribute, 136
OVERIFY attribute, 135, 136

P

patch
  definition, 16
  removing, 125
patch acquisition
  parameters, 72
Patch Acquisition Reports, 82
  summary by bulletin, 83
  summary by session, 82
  summary of errors, 83
patch analysis, 101
patch collection, 61
patch descriptor file, 61
patch discovery, performing, 97
Patch node, 134
patch reports, 101
Patch signature node, 138
patch.cfg file, 25
patch.tkd
  synchronization parameters, 53
patch.tkd file, 61
PATCHARGS class, 122
patchdata, 23
Patched column, 107, 108
PATCHMGR domain, 52, 61
PATCHSIG attribute, 136
patchtemp, 24
PATCHURL attribute, 134
PatchURL tag, 134
PATH attribute, 138, 140
Path tag, 138, 140
pending reboot status, 108
pilot testing, 14
PLATFORM attribute, 131, 135
Platform tag, 131, 135
POPULAR attribute, 130
PopularitySeverityID tag, 130
POSTED attribute, 131
PREREQ attribute, 131
PreReqSeverityID tag, 131
probe, definition, 80
ProbeCmdline tag, 136
Product node, 132
product parameter, 77
Products node, 132

Proxy Server, preloading, 124
PUBERROR instance, 77
Publish Package Dependencies acquisition setting, 69
purge_errors parameter, 40, 46, 77

Q

QNUMBER attribute, 135
QNumber tag, 135
qnumber, definition, 16
question mark, 108

R

Radia Administrator Workstation, 17
Radia Configuration Analyzer
  description, 17
  installing, 55
Radia Database Updates, 28
Radia Database, synchronizing, 52
Radia Integration Server, 17
Radia Inventory Manager, 17
Radia Knowledge Base Manager, description, 18
Radia Management Portal, description, 17
Radia Patch Manager, 17
  components, 16
    Radia Configuration Analyzer, 18
    Radia Patch Manager Client, 17
    Radia Patch Manager Server, 17
    Radia System Explorer, 17
  features
    compliance assessment, 14
    deployment, 14
    impact analysis, 14
    pilot testing, 14
    vulnerability assessment, 14
  reports
    compliance, 105, 114
    Compliance
      by Bulletin, 105
      by Device, 107
    Patch Acquisition
      Summary, 82
    Research, 110
      Browse by Bulletin, 110
      Browse by Device, 111
      Browse by Patch, 111
      Browse by Product, 112
      Browse by Release, 112
    Vulnerability Assessment
      by Product, 109
      Compliance
        by Patch, 110
        by Release, 109
Radia Patch Manager Client
  description, 17
  installing from CD-ROM, 91, 92
  installing from RMP, 91
  updating, 7, 40, 95
Radia Patch Manager Server, 17
  description, 17
  installing, 25
Radia Patch Manager settings file, 32
Radia Reporting Server
  filtering patch reports, 102
  overview, 17
Radia SQL database, 17
Radia Staging Server, preloading, 124
Radia System Explorer, description, 17
Radia Usage Manager, 17
RadKBMgr, 55
radskman, 98
radskman command line, 118
rcs_pass parameter, 33, 46, 54, 85
rcs_url parameter, 33, 46, 85
rcs_user parameter, 33, 46, 54, 85
reboot
  events, 144
  modifiers, 143, 145
  multiple events, 148
  types, 143, 145
REBOOT attribute, 134
Reboot Pending column, 107, 109
Reboot tag, 134
Red Hat Security advisories, 67
Red Hat systemid file, creating, 64
red X, 108
RedHat acquisition settings, 69

REGCHG class, 118
REGCHG instance, 119
RegChg node, 139
Release node, 133
Releases node, 133
Repair application event, 144
Replace acquisition setting, 68
replace parameter, 78
report acquisition status, 71
REPORT attribute, 118, 137, 139, 140
REPORT threshold, 121
reporting options, customizing, 119
reporting_url parameter, 41, 46
ReportThreshold attribute, 118
Research Reports, 110
  Browse by Bulletin, 110
  Browse by Device, 111
  Browse by Patch, 111
  Browse by Product, 112
  Browse by Release, 112
retire parameter, 42, 47, 78
REVISED attribute, 131
rh_depends parameter, 36, 48
rhn_register tool, 64
rhn_url parameter, 36, 49
RUNMODE attribute, 132, 137

S

Schema Version tag, 132
security advisory, definition, 16
SIZE attribute, 138
Size tag, 138
soft reboot, 145
Solaris patches, 66
Solaris_patch_url parameter, 79
Solaris_patchpro_base_url parameter, 79
Solaris_patchpro_db_url parameter, 79
Solaris_patchpro_jar_url parameter, 79
Solaris_pdiag_url parameter, 79
Solaris_sunalerts_url parameter, 79
SOURCE attribute, 131
Source tag, 131
SQL Patch database, creating, 23
state files, 18
state_dir parameter, 86
Sun Alert, 115
Sun Solaris 10, 94
Sun Solaris 9, 93
Sun Solaris Sun Alerts, 67
SUPERBU attribute, 134
SUPERCED attribute, 134
Superceded tag, 134
superceded_patches parameter, 79
SupercededByBulletin tag, 134
SupercededByMSPatch tag, 134
SUPERMSS attribute, 134
SUPPORT attribute, 131
Supported, 81, 131
Supported tag, 131
SuSE security patch acquisition, 65
SuSE Security patches, 67
SUSNAME attribute, 134
sync parameter, 49
synchronization parameters for patch.cfg, 53
systemid file, 64

T

tablespace, creating, 23
technical support, 3
TITLE attribute, 131
Title column, 106
Title tag, 131
Total column, 109
Total link, 107
TYPE attribute, 131, 140
Type tag, 131, 140

U

UninstallCmdline tag, 135
Update application event, 144
URL attribute, 130
URL tag, 130
USE attribute, 119, 137, 139, 140, 141

V

VALUE attribute, 140
Value tag, 140
VENDOR attribute, 131
Vendor tag, 131
vendor_os_filter parameter, 80
vendors parameter, 80
VerifyCmdline tag, 135
Version Activation application event, 144
VERSION attribute, 139
Version tag, 139
vulnerabilities
  assessing, 14
  managing, 114

W

Warning column, 107, 108

X

XML tags
  BULLETIN class, 130
  FILECHG class, 138
  PATCH class, 134
  PRODUCT class, 133
  REGCHG class, 139, 141
  RELEASE class, 133

Z

ZDELETE attribute, 125
ZOBJSTAT object, description, 100
ZSERVICE.REBOOT attribute, 143