HP OpenView Patch Manager Using Radia

for the Windows and Linux operating systems

Software Version: 2.0

Installation and Configuration Guide

Manufacturing Part Number: T3424-90080

February 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

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

Support

Please visit the HP OpenView web site at:

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

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

You can also go directly to the support web site at:

http://support.openview.hp.com/

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 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://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

https://passport.hp.com/hpp2/newuser.do

Revisions

The version number on the title page of this document indicates the software version. The print date on the title page changes each time this document is updated.

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

The sections below show new features that have been added to the Radia Patch Manager after release 1.2.

Chapter 2: Creating the Radia Patch Manager Environment

2.0 Page 27, To install the Radia Patch Manager Components: For version 2.0, the Radia Patch Manager no longer includes an option for the installation of the Radia Messaging Server.

2.0 Page 33, Configuring the Radia Patch Manager Server: The Radia Patch Administrator provides an interface to modify Radia Patch Manager settings.

1.2.1 Page 34, To use the Radia Patch Manager Administrator: The Radia Patch Manager setup page has been updated to reflect new configuration parameters.

2.0 Page 35, 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.

2.0 Page 37, Red Hat Feeds Settings: Specify the URL for the Red Hat Network data feed using the Radia Patch Manager Administrator. This URL is the value for the rhn_url parameter in `patch.cfg`.

2.0 Page 40, Reporting Settings: Specify the location of the Radia Reporting Server in the Radia Patch Manager Administrator. Click the Reporting icon in the Radia Patch Manager Administrator to view Patch Reports. This URL is the value for the reporting_url parameter in `patch.cfg`.

Chapter 3: Patch Acquisition

2.0 Page 58, See the figure The vendor's patch repository is contacted: Shows that security patches can now be acquired from the Red Hat Network data feed.

2.0 Page 70, See the table Patch Acquisition Parameters: Use ARCH to specify for which machine architectures you want to acquire patches.

1.2.1 Page 72, See the table Patch Acquisition Parameters: A new variable called HISTORY controls how long to keep the Patch Auth Store (PASTORE) instances.

1.2.1 Page 73, See the table Patch Acquisition Parameters: A LANG filter, specified in `patch.cfg` or on your acquisition command line, has been added that provides a single comma-delimited list of the language filters to include or exclude from publishing.

1.2.1 Page 75, See the table Patch Acquisition Parameters: A PRODUCT filter, specified in `patch.cfg` or on your acquisition command line, has been added that provides a single comma-delimited list of the product filters to include and exclude from publishing.

1.2.1 Page 75, See the table Patch Acquisition Parameters: A new variable in called PURGE_ERRORS controls how long to keep Publisher Error (PUBERROR) instances.

1.2.3 Page 77, See the table Patch Acquisition Parameters: A RETIRE option, specified in `patch.cfg` or on the acquisition command line has been added. Use the -retire parameter to delete specified bulletins if they exist in the Radia Database during the current publishing session, or to prevent publishing 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. HP recommends the use of the retire parameter in the `patch.cfg` file.

2.0 Page 78, See the table Patch Acquisition Parameters: For the rh_depends parameter in `patch.cfg`, specify yes if you want to publish additional Red Hat packages that downloaded security advisories may depend on in Acquisition Settings.

2.0 Page 78, See the table Patch Acquisition Parameters: Use SUPERCEDED_PATCHES to specify if you want to download the data for superceded patches.

2.0 Page 78, See the table Patch Acquisition Parameters: Use VENDORS to specify for which vendors you want to acquire patches.

2.0 Page 79, See the table Patch Acquisition Parameters: 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.

1.2.1 Page 79, To acquire patches from a command line: The patch publisher now logs the build and version number of the `patch.tkd`.

2.0 Page 80, Patch Acquisition Reports: Radia Patch Manager uses the Radia Reporting Server for patch acquisition reports.

Chapter 4: Patch Assessment and Analysis

2.0 Page 90, Installing the Radia Patch Manager Client: Radia Patch Manager Client Agent for Linux now supports deployment to Red Hat Enterprise Server 2.1 and 3.

1.2.1 Page 92, Updating the Radia Patch Manager Client Agent: A new class AUTOPKG has been added to the PATCHMGR domain for automated acquisition and distribution of product probes (both patch descriptor files and the scripts associated with a product probe).

2.0 Page 92, Updating the Radia Patch Manager Client Agent: Use AGENT_OS to specify for which operating systems you want to get Radia Patch Manager Client agents updates.

2.0 Page 92, Updating the Radia Patch Manager Client Agent: Use AGENT_VERSION to specify for which Radia Patch Manager Client version you want to get updates.

1.2.2 Page 92, Product Discovery and Analysis: Bandwidth optimization has been added to the Radia Patch Manager Client. Radia Patch Manager objects are cached locally on the client device.

2.0 Page 94, Patch Analysis and Reports: Radia Patch Manager now uses the Radia Reporting Server for patch compliance and research reports. To see the reports for Radia Patch Manager prior to version 2.0. see Appendix D.

2.0 Page 107, Deploying Automatic and Interactive Patches: Radia 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.

1.2.1 Page 108, Customizing Reporting Options: Customize the reporting status of a patch file or registry key using three new supported xml tags in the patch descriptor file for a bulletin. The new tags are DesiredState, ReportThreshold, and Use.

1.2.1 Page 111, Disabling Vulnerability Detection and Deployment: Disable a BULLETIN or PATCH instance for detecting patch vulnerability and patch deployment.

Contents

3 Patch Acquisition 57

4 Patch Assessment and Analysis....87

1 Introduction

At the end of this chapter, you will:

- Know the capabilities of Radia Patch Manager.

Radia Patch Manager

Radia Patch Manager provides value for business continuity and security initiatives. Radia 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 and Red Hat web-based depositories. For Microsoft, this includes both `mssecure.xml` and the Microsoft Software Update Service (SUS) data feed. For Red Hat the RedHat Network data feed is used.

- **Impact Analysis and Pilot Testing**:
  identification of affected applications, devices, and users to determine configuration impact before security patches are deployed. Radia 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.

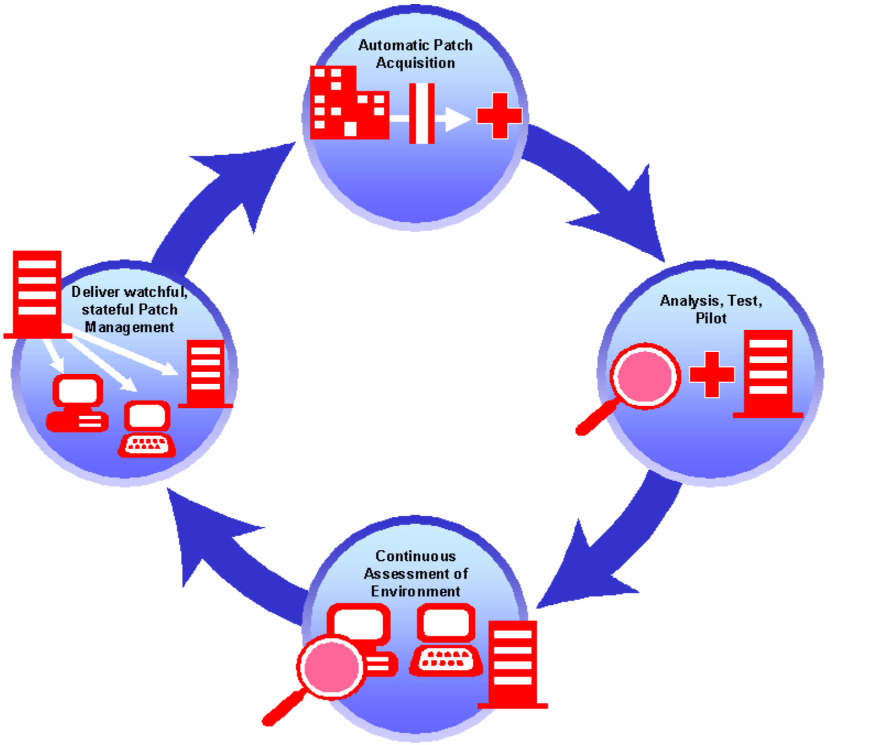

Automatic Patch Acquisition
Analysis, Test, Pilot
Continuous Assessment of Environment
Deliver watchful, stateful Patch Management

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 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

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

- **Radia Configuration Server**
  Applications and information about the subscribers and client computers are stored in the Radia Database on the Radia Configuration Server. The PATCHMGR domain in the Radia Database contains instances for patch management. The Radia Configuration Server processes information received from the Radia Patch Manager Client. The Radia Configuration Server manages vulnerabilities based on policies established by the Radia administrator using the Radia System Explorer. For more information, see the *Radia Configuration Server Guide*.
- **Radia Management Portal**
  Use the Radia Management Portal to configure the Radia Patch Manager Server and deploy the Radia Patch Manager Client. The Radia Management Portal is a module of the Radia Integration Server, and runs under the Radia Integration Server service. See the *Radia Management Portal Guide* for more information.
- **Radia Patch Manager Server**
  The Radia 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 Radia Patch Manager reports. Radia Patch Manager is a module of the Radia Integration Server, and runs under the Radia Integration Server service.

- **Radia Patch Manager Client**
  Install the Radia Patch Manager Client on devices for which you want to manage vulnerabilities. The client discovers products and patches on managed devices.

- **Radia Reporting Server**
  As part of the Radia extended infrastructure, the web-based Radia Reporting Server allows you to query the combined data in existing Radia Inventory Manager, Radia 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 Radia Reporting Server interface provides a dynamic and intuitive way to use Radia SQL data for reporting and overall environmental assessment.

- **Radia System Explorer**
  The Radia administrator uses the Radia System Explorer to view and manage vulnerabilities stored in the Radia Database. For more information, see the *Radia System Explorer Guide*.

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

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

- **Radia Knowledge Base Manager**
  The Radia Knowledge Base Manager performs automated import processing of Radia state files into a database allowing you to compare state files. See the *Radia Knowledge Base Manager Guide* for more information.

Summary

- Use the Radia 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 Radia Patch Manager version 2.0 or above.

2 Creating the Radia Patch Manager Environment

At the end of this chapter, you will:

- Be familiar with the tasks needed to set up the Radia Patch Manager environment.
- Know how to modify the Radia Database and Radia Configuration Server.
- Be able to install the Radia Patch Manager.

Radia Patch Manager Implementation Tasks

Before setting up your environment for the Radia Patch Manager, you must have already installed the latest version of the Radia 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 Radia Patch Manager main CD-ROM. To use the Radia Patch Manager, you will need to complete the following tasks:

- ❑ Create the SQL or Oracle Patch Database and an ODBC DSN.
- ❑ Install the Radia Configuration Server. See the *Radia Getting Started Guide.*
- ❑ Install the Radia Messaging Server. See the *Radia Messaging Server Guide*.
- ❑ Install the Radia Administrator. See the *Radia Application Manager Guide.*
- ❑ Run the Radia Patch Manager installation. This installation includes:
  - Modifying the Radia Database.
  - Modifying the Radia Configuration Server executables.
  - Installing the Radia Patch Manager Server.
  - Configuring Radia Patch Manager to use your DSN.
  - Synchronizing the Radia Database with the SQL or Oracle Database.
- ❑ Add a Method Connection to your Radia Database.
- ❑ Modify the Radia Messaging Server.
- ❑ Install the Radia Management Portal.
- ❑ Install the Radia Reporting Server.
- ❑ Optional: Install and configure the Radia Configuration Analyzer.
- ❑ Optional: Install and configure the Radia Knowledge Base Manager.

> 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 the Microsoft-supplied ones.

Creating the ODBC Patch Database

Before installing Radia 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 Radia 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 Radia 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 Radia 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 Radia Administrator Workstation

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

Installing the Radia Patch Manager Server

Identify a computer to act as your Radia Patch Manager Server. It must be able to communicate with your Radia Configuration Server, your ODBC Server, and the Internet. Radia Patch Manager may be installed on Windows 2000, Windows XP, or Windows 2003 Server. See the operating system's documentation for system requirements.

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

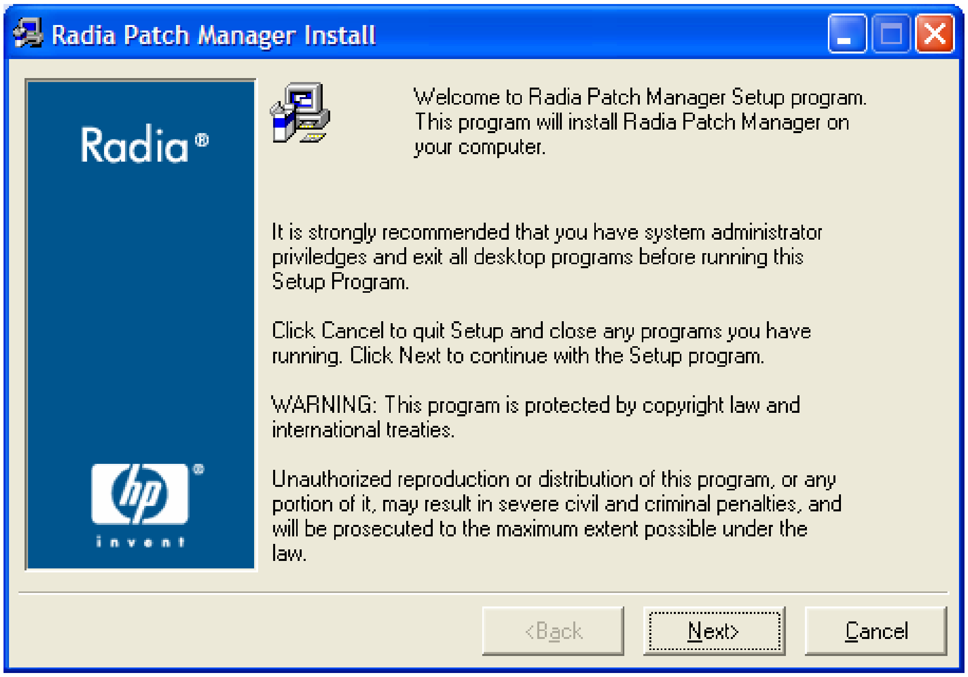
The minimum version of Microsoft Data Access Components (MDAC) required is 2.8 on the Radia Patch Manager Server. If you are using Oracle for your Patch Database, you must use the Oracle Corporation's ODBC drivers, minimum version 9.2.0.3, not those supplied by Microsoft.

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

To install the Radia Patch Manager Components

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

  The minimum build of nvdkit required for Radia Patch Manager Version 2.0 is 145. This is included with the installation materials.



Welcome to Radia Patch Manager Setup program. This program will install Radia Patch Manager on your computer.

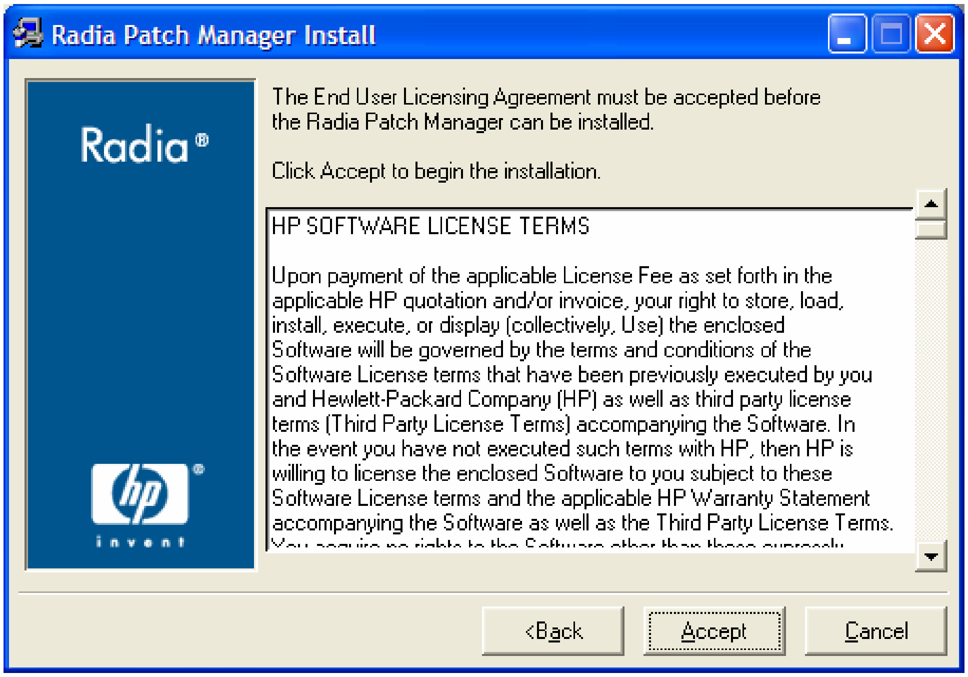
It is strongly recommended that you have system administrator priviledges and exit all desktop programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2 Click **Next**.



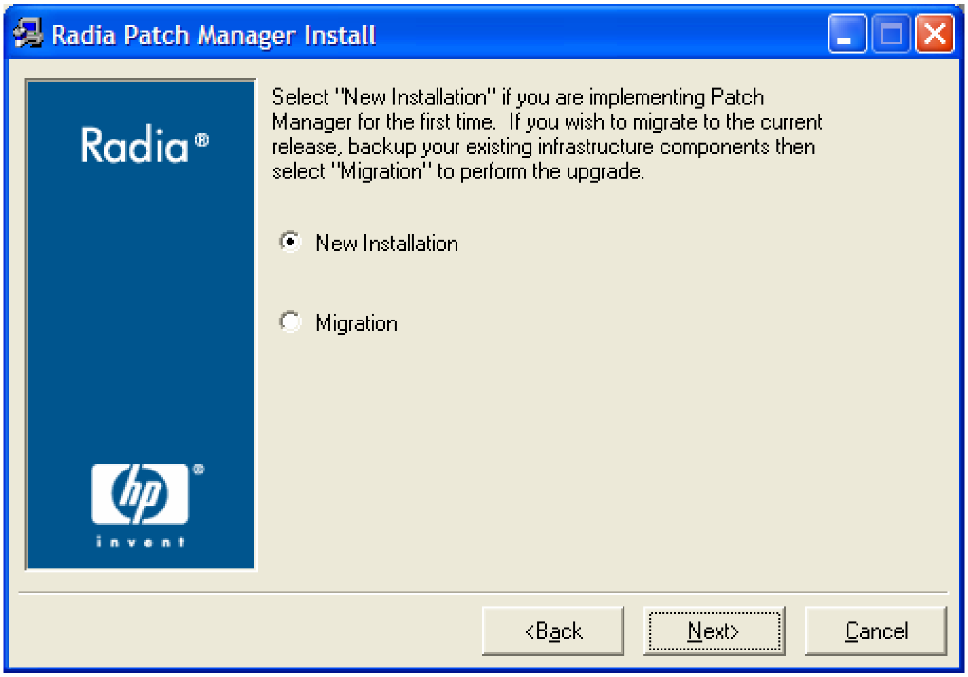
The End User Licensing Agreement must be accepted before the Radia Patch Manager can be installed.

Click Accept to begin the installation.

HP SOFTWARE LICENSE TERMS

Upon payment of the applicable License Fee as set forth in the applicable HP quotation and/or invoice, your right to store, load, install, execute, or display (collectively, Use) the enclosed Software will be governed by the terms and conditions of the Software License terms that have been previously executed by you and Hewlett-Packard Company (HP) as well as third party license terms (Third Party License Terms) accompanying the Software. In the event you have not executed such terms with HP, then HP is willing to license the enclosed Software to you subject to these Software License terms and the applicable HP Warranty Statement accompanying the Software as well as the Third Party License Terms.

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



Radia Patch Manager Install

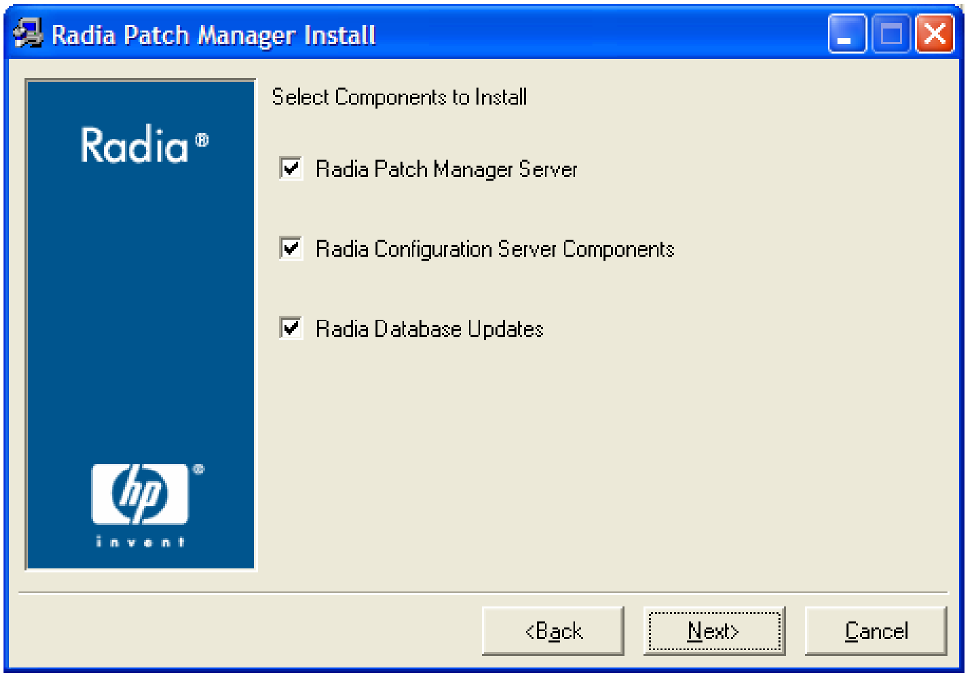
Select "New Installation" if you are implementing Patch Manager for the first time. If you wish to migrate to the current release, backup your existing infrastructure components then select "Migration" to perform the upgrade.

● New Installation

○ Migration

4 Select **New Installation** if this is a new installation of the Radia Patch Manager. If you want to migrate from Radia Patch Manager Version 1.2, Release 1.2.2 to Radia Patch Manager Version 2.0, select **Migration.** Migration instructions can be found in the Radia Patch Manager media's Migration directory.

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



Select Components to Install

☑ Radia Patch Manager Server

☑ Radia Configuration Server Components

☑ Radia Database Updates

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

— **Radia Patch Manager Server**
Installs the Radia Patch Manager Server including the Radia Integration Server.

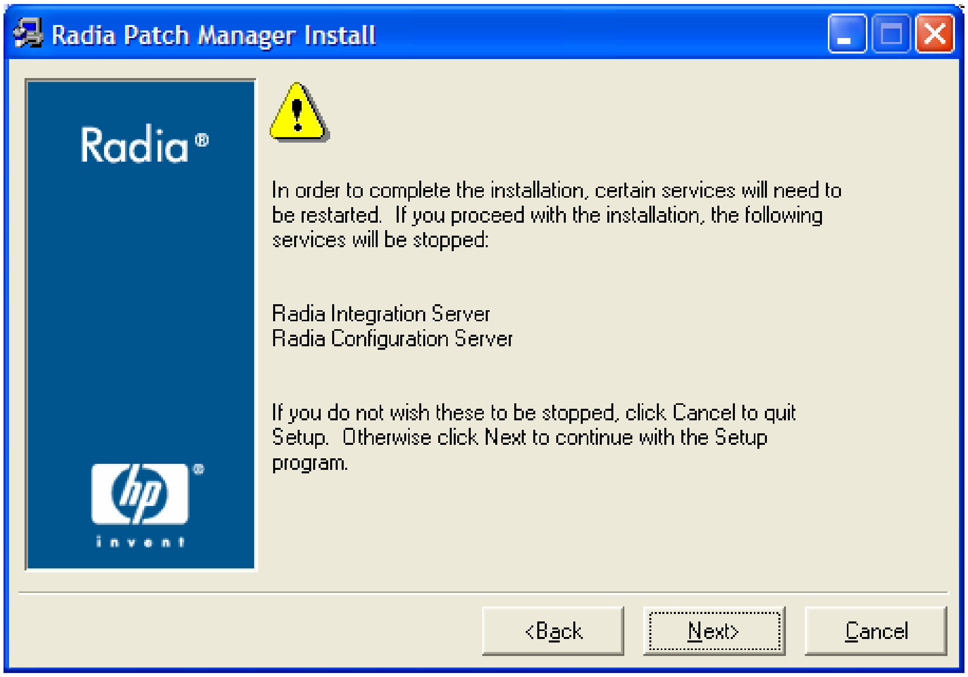
— **Radia Configuration Server Components**
Installs updated executables and scripts for the Radia Configuration Server to work with Radia Patch Manager.

> To use the features of Radia 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 Radia Configuration Server Components and Radia Database Updates portions of the Radia Patch Manager installation can only be run on the Radia Configuration Server computer. These pieces cannot be installed over a network connection.

After making your selections, click **Next**.

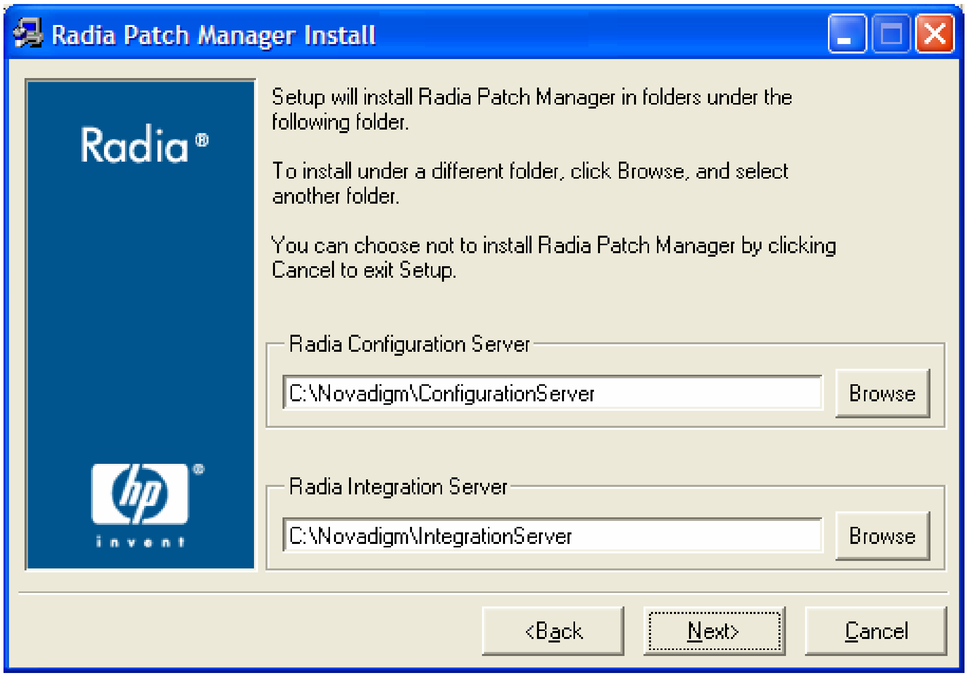


In order to complete the installation, certain services will need to be restarted. If you proceed with the installation, the following services will be stopped:

Radia Integration Server
Radia Configuration Server

If you do not wish these to be stopped, click Cancel to quit Setup. Otherwise click Next to continue with the Setup program.

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



Setup will install Radia Patch Manager in folders under the following folder.

To install under a different folder, click Browse, and select another folder.

You can choose not to install Radia Patch Manager by clicking Cancel to exit Setup.

Radia Configuration Server: C:\Novadigm\ConfigurationServer

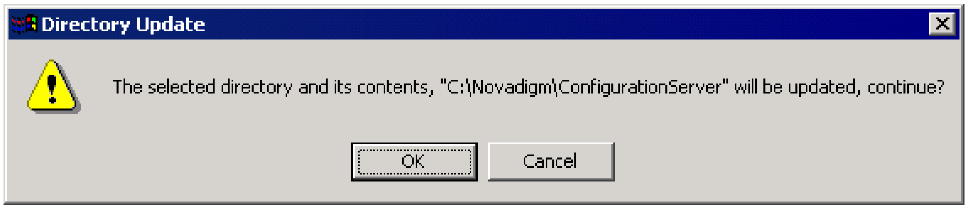
Radia Integration Server: C:\Novadigm\IntegrationServer

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

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

Where possible, accept the defaults for these directories.

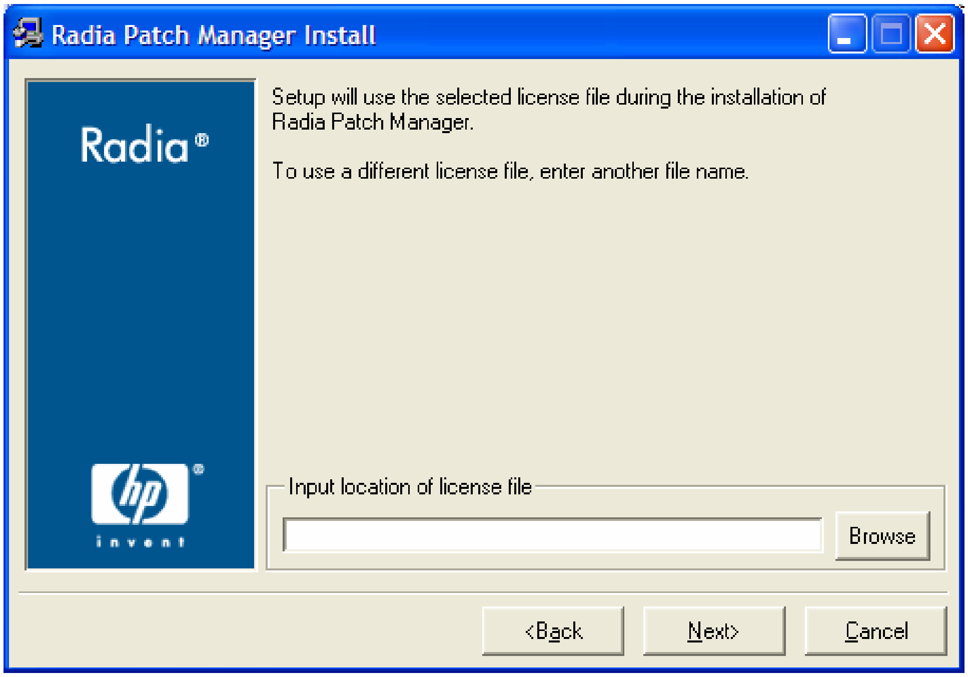
8 Click **Next**.



Directory Update

The selected directory and its contents, "C:\Novadigm\ConfigurationServer" will be updated, continue?

9 Click **OK** if you would like to continue.



Radia Patch Manager Install

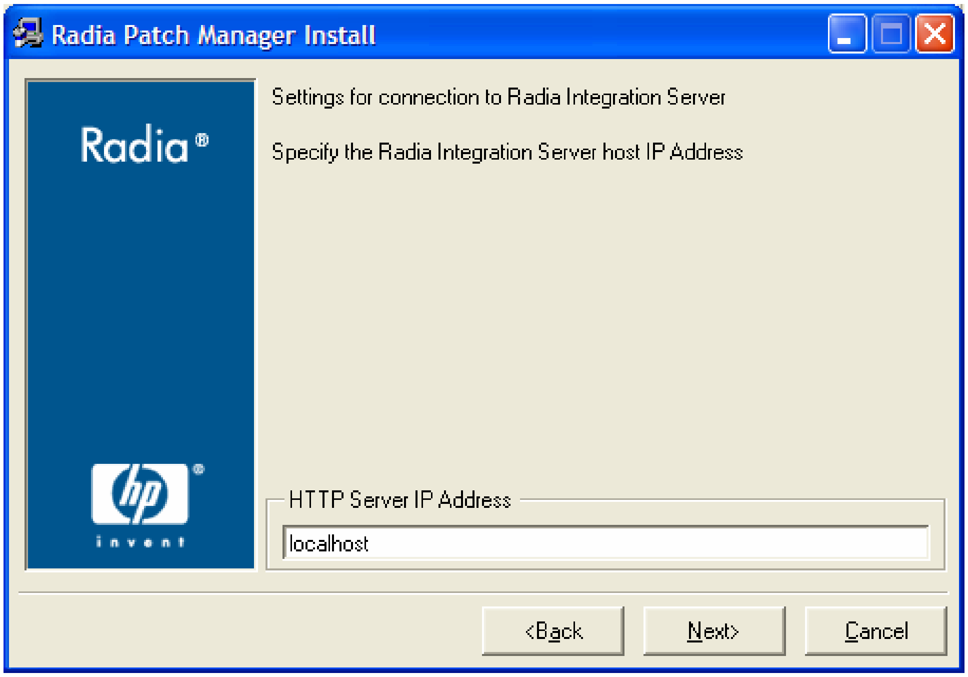
Setup will use the selected license file during the installation of Radia Patch Manager.

To use a different license file, enter another file name.

Input location of license file

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

11 Click **Next**.

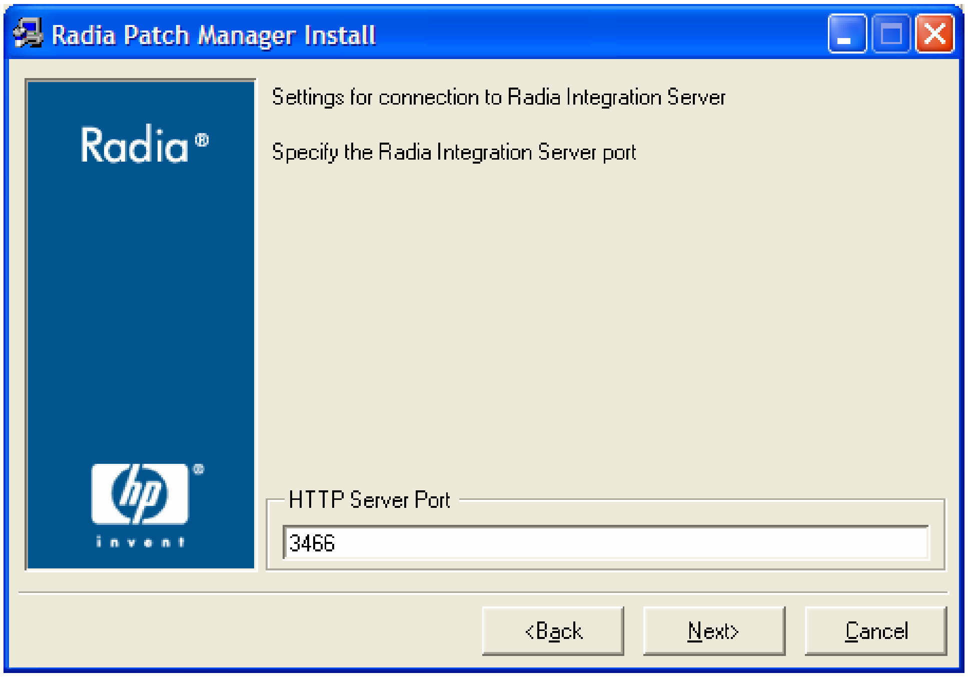


Settings for connection to Radia Integration Server

Specify the Radia Integration Server host IP Address

HTTP Server IP Address: localhost

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



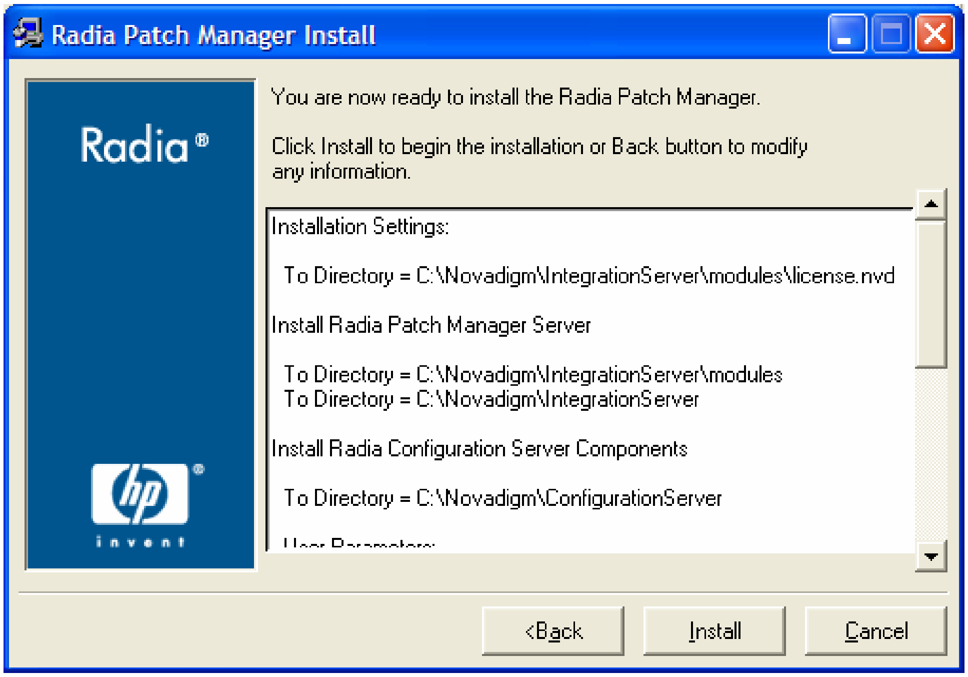
Radia Patch Manager Install

Settings for connection to Radia Integration Server

Specify the Radia Integration Server port

HTTP Server Port: 3466

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



Radia Patch Manager Install

You are now ready to install the Radia Patch Manager.

Click Install to begin the installation or Back button to modify any information.

```
Installation Settings:

  To Directory = C:\Novadigm\IntegrationServer\modules\license.nvd

Install Radia Patch Manager Server

  To Directory = C:\Novadigm\IntegrationServer\modules
  To Directory = C:\Novadigm\IntegrationServer

Install Radia Configuration Server Components

  To Directory = C:\Novadigm\ConfigurationServer

  User Parameters:
```

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

You should be directed to 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 Radia Patch Manager Server

The Radia Patch Administrator page provides an interface to the Radia Patch Manager settings file, `patch.cfg`. `Patch.cfg` includes settings such as passwords, server locations, and DSN information. Use the Radia Patch Administrator to modify these settings or you can edit this file manually.

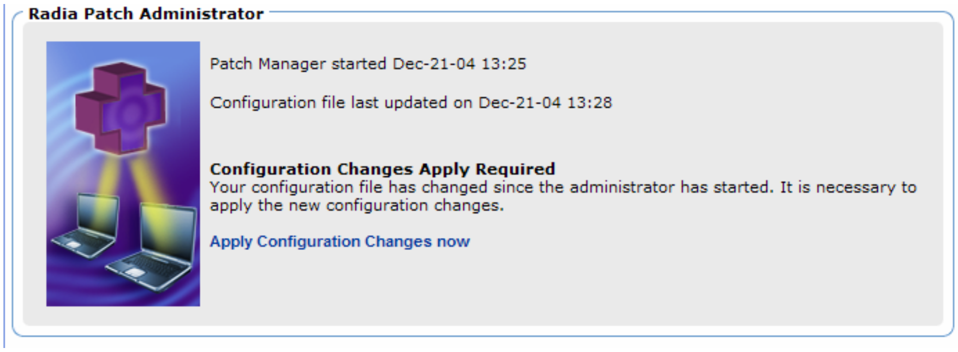
The Radia Patch Manager Administrator is divided into eleven areas described below: Configuration Server, Patch Manager, ODBC DSN, Microsoft Feeds, RedHat Feeds, HTTP, Acquisition History, Patch Agent, Reporting, Default, and Patch Configuration.

To use the Radia 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 the table *Patch Acquisition Parameters* on page 70.

3 Click **Save** to apply changes. You will be prompted to restart for the changes to take effect.



Radia Patch Administrator

Patch Manager started Dec-21-04 13:25

Configuration file last updated on Dec-21-04 13:28

Configuration Changes Apply Required
Your configuration file has changed since the administrator has started. It is necessary to apply the new configuration changes.

Apply Configuration Changes now

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

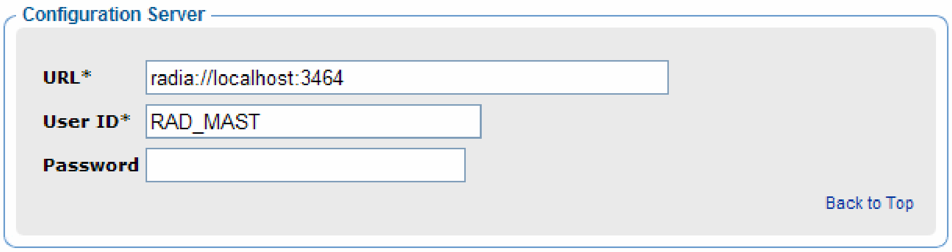
Configuration Server Settings

The following settings are configured in the Configuration Server section:

URL Specify the location of your Radia 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 Radia 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 Radia Configuration Server, specify the password for the rcs_user. This is the same as the rcs_pass parameter in `patch.cfg`.



Configuration Server

URL* radia://localhost:3464

User ID* RAD_MAST

Password

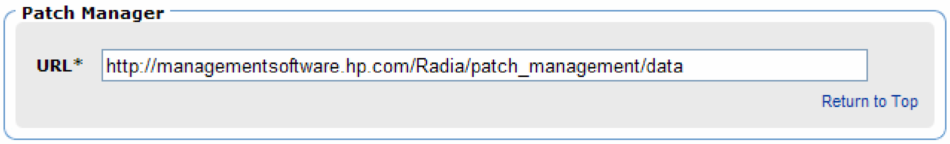
Patch Manager Settings

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`.

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.



Patch Manager

URL* http://managementsoftware.hp.com/Radia/patch_management/data

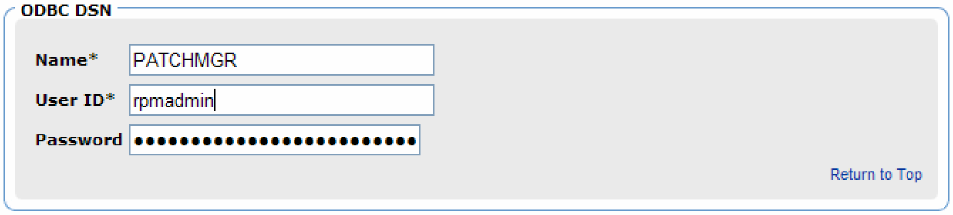
ODBC DSN Settings

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`.



ODBC DSN

Name* PATCHMGR

User ID* rpmadmin

Password ●●●●●●●●●●●●●●●●●●●●●●●●●

Microsoft Feeds Settings

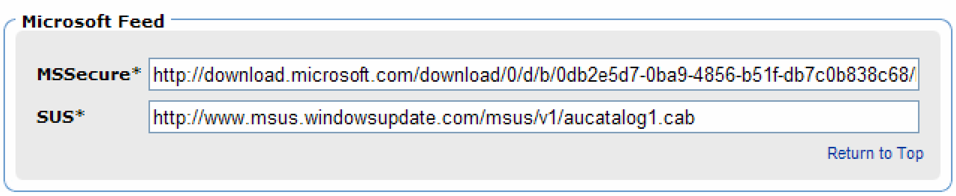
The following settings are configured in the Vendor Feeds section:

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**



Microsoft Feed

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

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

Red Hat Feeds Settings

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

RedHat

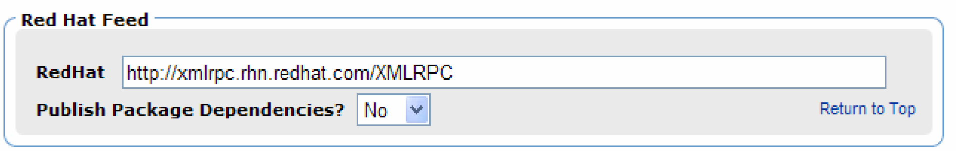
Specify the URL for the Red Hat Network data feed. This is the same as the rhn_url parameter in `patch.cfg`.

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



Red Hat Feed

RedHat http://xmlrpc.rhn.redhat.com/XMLRPC

Publish Package Dependencies? No

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

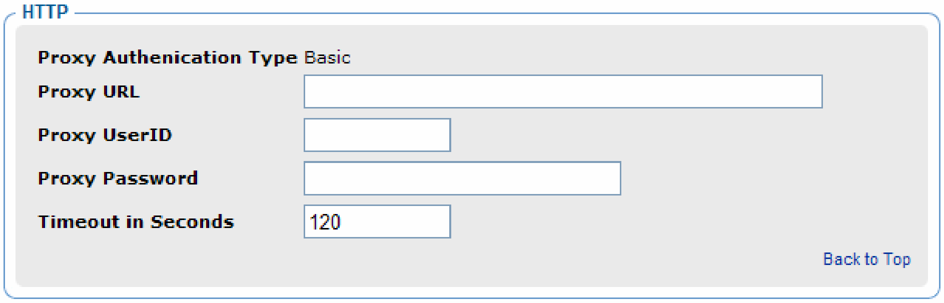
If you use a proxy server for http traffic, specify your user ID. This is the same as the http_proxy_user parameter in `patch.cfg`.

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`.



HTTP

Proxy Authenication Type Basic

Proxy URL

Proxy UserID

Proxy Password

Timeout in Seconds 120

Acquisition History Settings

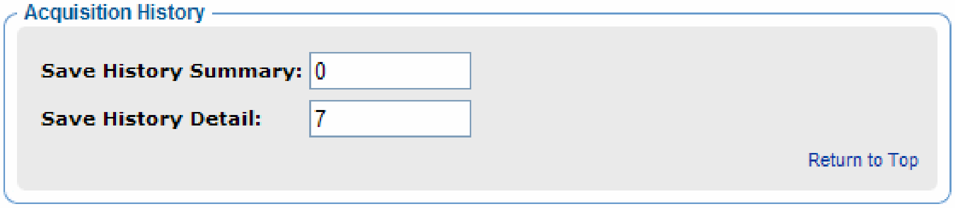
The following settings are configured in the Acquisition History section:

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`.



Save History Summary: 0

Save History Detail: 7

Patch Agent Settings

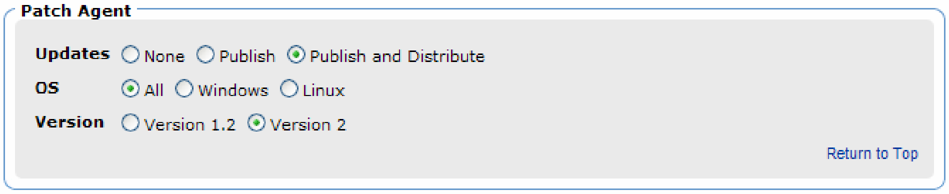
These settings are for the maintenance of the Radia Patch Manager Client agent files. For more information on this, see *Updating the Radia Patch Manager Client Agent* on page 90. The following settings are configured in the Patch Agent section:

Updates

If you select Publish, the updates will be published to the PATCHMGR domain, but will not be connected for distribution (deployment) to Radia 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 Radia 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 Radia Patch Manager version you would like to acquire the agent updates for. You can only publish one version to one Radia Configuration Server. This is the same as the agent_version parameter in `patch.cfg`.



Patch Agent

Updates ○ None ○ Publish ● Publish and Distribute

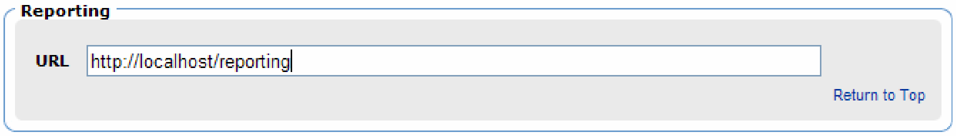
OS ● All ○ Windows ○ Linux

Version ○ Version 1.2 ● Version 2

Reporting Settings

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

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



Reporting

URL http://localhost/reporting

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`.

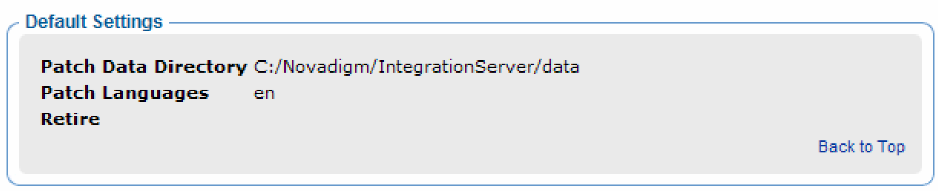
Patch Data Directory — The directory where patches are downloaded to before they are sent to the Radia Configuration Server. This is the same as the data_dir parameter in `patch.cfg`.

Language — Radia 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.



Default Settings

Patch Data Directory C:/Novadigm/IntegrationServer/data
Patch Languages en
Retire

Patch Configuration Settings File

If you are unable to use the Radia Patch 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 Radia Patch Manager Server are listed below. There are additional parameters that are only used for patch acquisition. See the chapter Patch Acquisition starting on page 57 for more information.

Table 1: 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 Radia 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 the directory from which you are running the command).
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, Radia 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.

Table 1: **Patch Manager Server Configuration Parameters**

Parameter	Description
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, Radia Patch Manager supports basic authentication only.
http_proxy_user	If you use a proxy server for http traffic, specify your user ID.
http_timeout	Set the total amount of time to wait for the file to be completely downloaded. If the acquisition session is unable to download the file in this time, then the acquisition will abort the current http location, and will continue the acquisition with the next http location. Increase the http_timeout if you need to allow additional time for a bulletin to download. Http_timeout is displayed in the `setup.tsp` page in seconds. Specify http_timeout in either the `patch.cfg` file or on the command line in milliseconds. 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	Radia 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_pass	Specify the password for Microsoft_user.
microsoft_sus_url	Specify the URL for the Microsoft SUS feed. Default: **http://www.msus.windowsupdate.com /msus/v1/aucatalog.cab**.

Table 1: Patch Manager Server Configuration Parameters

Parameter	Description
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 Radia Patch Manager previous to 1.2.2, you must specify this path on the acquisition command line. This path is hard coded into Radia Patch Manager 1.2.2.
microsoft_user	Specify the user for the Microsoft web site.
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 Radia Configuration Server, specify the password for the rcs_user.

Table 1: Patch Manager Server Configuration Parameters

Parameter	Description
rcs_url	Specify the location of your Radia Configuration Server in URL format. Use the format: `radia://`*`ipaddress`*`:`*`port`* where: • `radia` indicates the session type to be opened to the Radia Configuration Server • *`ipaddress`* is the hostname or IP address of the computer hosting the Radia Configuration Server • *`port`* is the port number of the Radia Configuration Server. Note: This parameter is required.
rcs_user	If authentication has been enabled on your Radia Configuration Server, specify the rcs_user.
reporting_url	Specify the URL of your Radia Reporting Server.

Table 1: Patch Manager Server Configuration Parameters

Parameter	Description
retire	Specify the bulletins to retire separated by commas. Use the -retire parameter to: • Delete specified bulletins if they exist in the Radia Configuration Server database during the current publishing session. • Not publish the bulletins specified in the retire parameter to the Radia 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 Radia 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 which are currently under management in your enterprise, the retired security patches may be removed from your Radia Patch Manager Client devices. Example: -retire MS00-001,MS00-029

Table 1: Patch Manager Server Configuration Parameters

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, Radia 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**.
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 the chapter Patch Acquisition starting on page 57 in this guide for more information on running an acquisition command line.

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

```
patch::init {
        AGENT_OS *
        AGENT_UPDATES PUBLISH,DISTRIBUTE
        AGENT_VERSION VERSION2
        ALERT_DAYS 14
        BUILD 254
        BULLETINS *
        COMMIT_INTERVAL 5000
        CVENAME Y
        DATA_DIR C:/Novadigm/IntegrationServer/data
        DL_DATEFMT {%Y-%m-%d %T}
        DSN rpm20
        DSN_ATTEMPTS 3
        DSN_DATEFMT {%Y-%m-%d %H:%M:%S}
        DSN_DELAY 10
        DSN_PASS {}
        DSN_PING 60
        DSN_TRACE 0
        DSN_USER rpmadmin
        ETC C:/Novadigm/IntegrationServer/etc/patch
        FORCE no
        FTP_PASS {{DES}sSSDIkipqXYjIWXELBpFLw==:16}
        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
        HTTP_PROXY_AUTHENTICATION basic
        HTTP_PROXY_PASS {}
        HTTP_PROXY_SCRIPT {}
        HTTP_PROXY_TIMEOUT 120
        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}
        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
        STATUS_INTERVAL 600
        STATUS_RESET {12:00 am}
        SUPERCEDED_PATCHES N
        TITLE {Radia Patch Manager Reporting}
        URL /patch
        VENDORS microsoft
        VERSION 2.0.0
        WORKER_RETRY 3
        WORKER_TIMEOUT 180}
#
# END OF CONFIG
#
```

Database Synchronization

The patch information that has been sent to the Radia Database on the Radia 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.

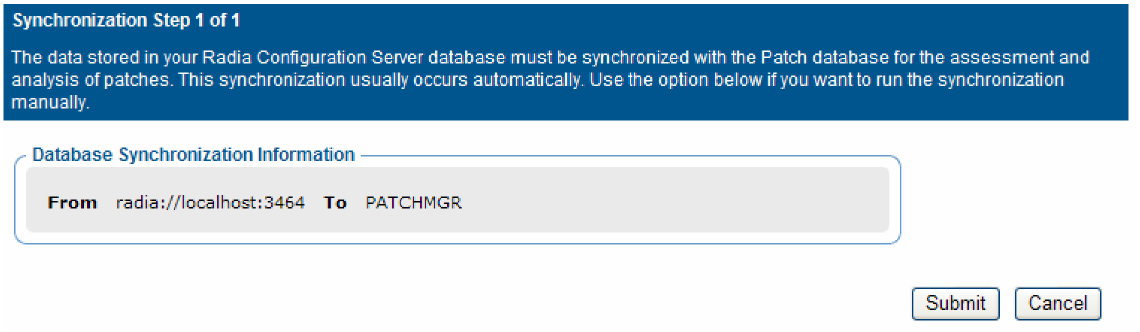
- Each class in the PATCHMGR domain becomes a class in the ODBC database. The corresponding table is named nvd_*classname*.
- Each attribute in each class becomes a column in its table. The corresponding column name is nvd_*attributename*. Expressions and connection variables are *not* replicated.

- 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**.



Synchronization Step 1 of 1

The data stored in your Radia Configuration Server database must be synchronized with the Patch database for the assessment and analysis of patches. This synchronization usually occurs automatically. Use the option below if you want to run the synchronization manually.

Database Synchronization Information

From radia://localhost:3464 **To** PATCHMGR

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 Radia Configuration Server is the local machine.

See the table Patch.tkd Synchronization Parameters below.

Table 2: Patch.tkd Synchronization Parameters

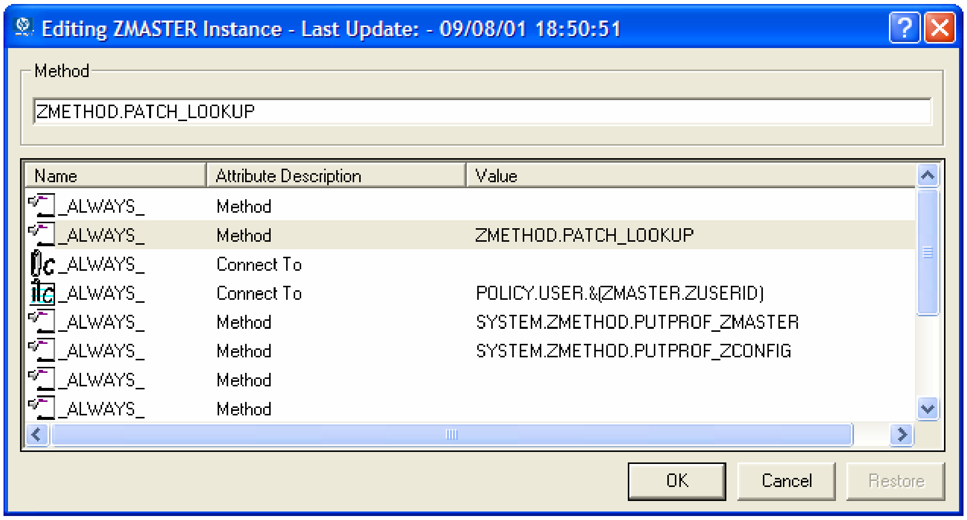
Parameter	Description
dsn	Specify the Data Source Name (DSN) the Patch ODBC database. Note: This parameter is required.
dsn_user	Specify the user for the dsn for the Patch ODBC database.
dsn_pass	Specify the password for the user of the Patch ODBC database.
host	Specify the location of your Radia Configuration Server in URL format. Use the format: *radia*://*ipaddress*:*port* where: • *radia* indicates the session type to be opened to the Radia Configuration Server. • *ipaddress* is the hostname or IP address of the computer hosting the Radia Configuration Server. • *port* is the port number of the Radia Configuration Server. Note: This parameter is required.
class	Specify the classes you wish to synchronize between the Radia 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 Radia 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.

Table 2: `Patch.tkd` **Synchronization Parameters**

Parameter	Description
rcs_pass	If authentication has been enabled on your Radia Configuration Server, specify the password for the rcs_user.
rcs_user	If authentication has been enabled on your Radia Configuration Server, specify the rcs_user.

Adding a Method Connection

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



Method: ZMETHOD.PATCH_LOOKUP

Name	Attribute Description	Value
ALWAYS	Method	
ALWAYS	Method	ZMETHOD.PATCH_LOOKUP
ALWAYS	Connect To	
ALWAYS	Connect To	POLICY.USER.&(ZMASTER.ZUSERID)
ALWAYS	Method	SYSTEM.ZMETHOD.PUTPROF_ZMASTER
ALWAYS	Method	SYSTEM.ZMETHOD.PUTPROF_ZCONFIG
ALWAYS	Method	
ALWAYS	Method	

Figure 2 Edit the ZMASTER instance.

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

Modifying the Radia Messaging Server

Install the Radia Messaging Server from the Radia V4 Infrastructure CD-ROM. If you already have the Radia Messaging Server installed, you will need to edit its configuration file to work with Radia Patch Manager.

To edit the `rms.cfg` file

1 Use a text editor to open the `rms.cfg` file. By default, its location is `<System Drive>:\Novadigm\MessagingServer\etc`.

2 Find the section starting with msg::register router.

> The Radia Messaging Server expects the DIR parameter to be `../ConfigurationServer/data/default`. If you change the directory of your Radia Configuration Server, be sure to change the DIR parameter in the `rms.cfg` file found in the Radia Messaging Server's etc subdirectory.

3 Add the lines in the rectangle in the sample code below.

```
msg::register router {
    TYPE        ROUTER

    ROUTE       {
        TO      CORE.RIM
        USE     rim
    }
    ROUTE       {
        TO      CORE.RMP
        USE     /dev/null
    }
    ROUTE       {
        TO      INVENTORY
        USE     rim
    }
    ROUTE       {
        TO      INVENTORY.WBEM
        USE     rim
    }
    ROUTE       {
        TO      PATCH
        USE     patch
    }
```

Add these lines.

4 Add the lines shown below to the end of the file.

```
msg::register patch {
  TYPE          ODBC

  DSN           "put your dsn here"
  USER          "user"
  PASS          "password"
}
```

5 Save and close `rms.cfg`.

6 Restart the Radia Messaging Service.

Radia Reporting Server

The Radia Reporting Server version 4.1 is required to view enhanced reports for Radia Patch Manger. Please obtain the Radia Reporting Server from the HP Support web site, and review the Release Notes prior to installing. The Radia Reporting Server Guide also includes instructions on how to use the Radia Reporting Server.

Radia Configuration Analyzer Installation Tasks (Optional)

The Radia Configuration Analyzer provides a powerful console for viewing, storing, and comparing application data. Backed by an SQL database, the Radia 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 Radia 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 Radia Configuration Analyzer and Radia 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 Radia Configuration Analyzer, see the *Radia Configuration Analyzer Guide*.

Installing and Configuring the Radia Knowledge Base Manager (Optional)

The Radia KB Manager performs automated import processing of Radia state files into the Radia Application Knowledge Base allowing you to compare state files. The Radia KB Manager automated import server runs independent of the Radia Configuration Server to import files found in the AutoImport directories that you specify. The Radia KB 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 Radia Knowledge Base Manager, see the *Radia Knowledge Base Manager Guide* available on the HP OpenView web site.

➤ If you are using Oracle with the Radia 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 Radia Configuration Analyzer and Radia 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 Radia Configuration Server and the Radia Database.
- Radia Patch Manager requires an SQL or Oracle database.
- Install the Radia Patch Manager on a computer that can access the Radia Configuration Server and your ODBC Data Source.
- Install the Radia Configuration Analyzer and the Radia 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

Radia 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.

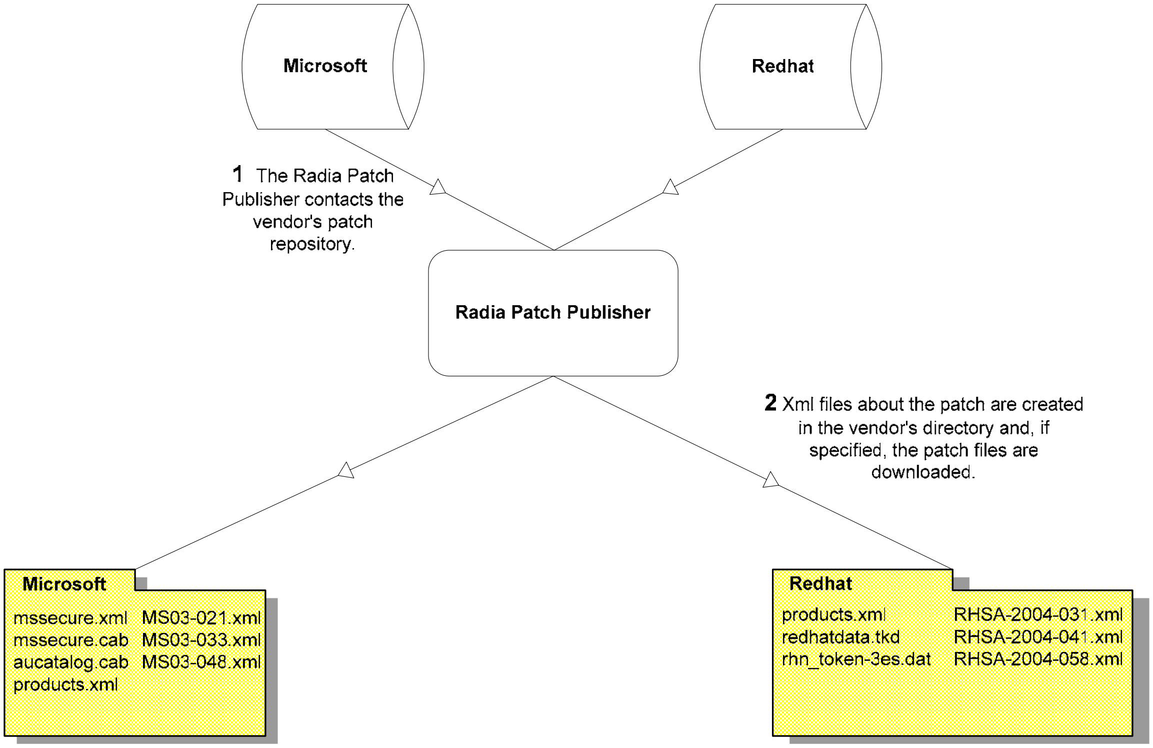


Figure 3 The vendor's patch repository is contacted.

Patch Acquisition Overview

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

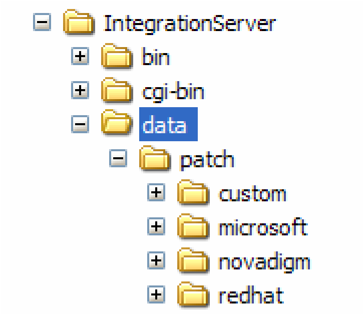
During the acquisition, the following things occur:

- 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.
- 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 Radia 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.



IntegrationServer
bin
cgi-bin
data
patch
custom
microsoft
novadigm
redhat

Figure 4 View the 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 Microsoft or Redhat directory. You can also create or modify your own patch descriptors that will override files in the Novadigm, Microsoft, 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.

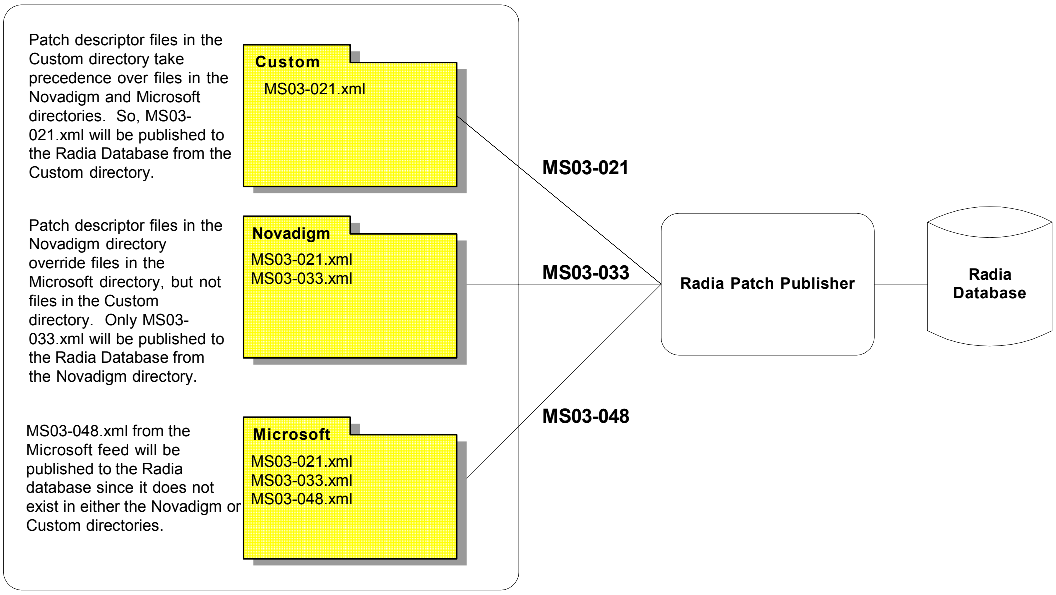

Patch descriptor files in the Custom directory take precedence over files in the Novadigm and Microsoft directories. So, MS03-021.xml will be published to the Radia Database from the Custom directory.
Custom
MS03-021.xml
Patch descriptor files in the Novadigm directory override files in the Microsoft directory, but not files in the Custom directory. Only MS03-033.xml will be published to the Radia Database from the Novadigm directory.
Novadigm
MS03-021.xml
MS03-033.xml
MS03-048.xml from the Microsoft feed will be published to the Radia database since it does not exist in either the Novadigm or Custom directories.
Microsoft
MS03-021.xml
MS03-033.xml
MS03-048.xml
MS03-021
MS03-033
MS03-048
Radia Patch Publisher
Radia Database

Figure 5 Patch descriptor files in Custom override those in Novadigm and Microsoft.

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 both Red Hat Enterprise Server Version 2.1 and Red Hat Enterprise Server Version 3, you will need a Red Hat Network account with at least two Red Hat Network system entitlements, one for each Enterprise Server version, 2.1 and 3.

- 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, Radia 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 Radia 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 Radia Configuration Server and ODBC parameters are configured in `patch.cfg`.

Performing a Patch Acquisition

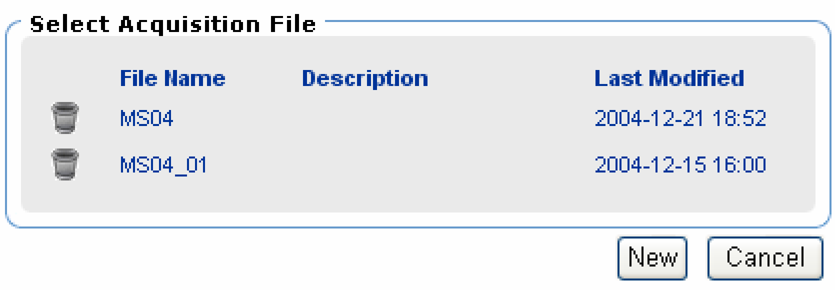
You can acquire patches either using the Radia Patch Administrator or using a command line. The Radia Patch Administrator provides a user friendly interface that allows you to create acquisition profiles that can be saved and used repeatedly. You will need to first create the acquisition file, and then 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 file. See Configuring the Radia Patch Manager Server on page 33 for more information.

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.**

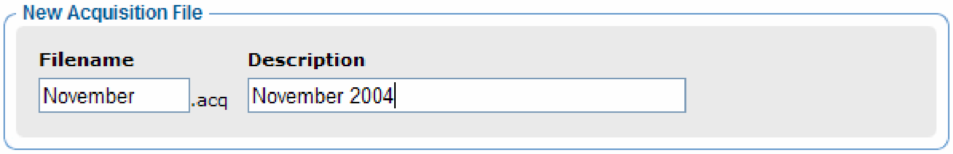
2 From Configuration, click **Acquisition Settings**.



Select Acquisition File

File Name	Description	Last Modified
MS04		2004-12-21 18:52
MS04_01		2004-12-15 16:00

3 Either select an existing file to edit, or click **New** to create a new file. Click the trashcan icon to delete an acquisition file. In this example, we click **New**.

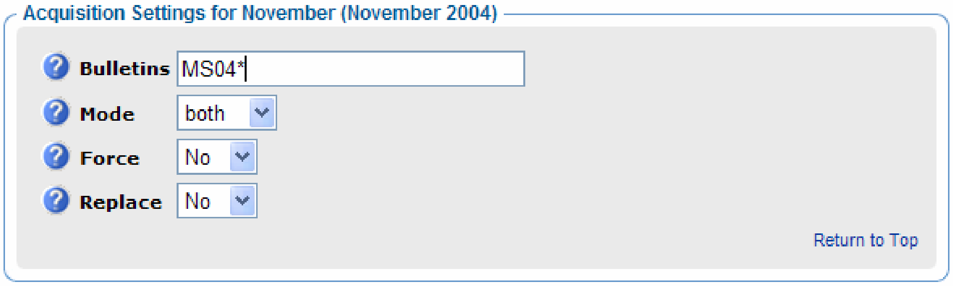


New Acquisition File

Filename	Description
November.acq	November 2004

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

5 You will be taken to Step 2, where you can set Acquisition Settings, Microsoft Settings, and RedHat Settings.



Acquisition Settings for November (November 2004)

Bulletins	MS04*
Mode	both
Force	No
Replace	No

Acquisition Settings

Bulletins

Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. Microsoft service packs are listed in the format MSSP_<*operatingsystem*>_<*spnumber*>.

To acquire Microsoft service packs, specify MSSP*. This will download sample service packs using information in the Novadigm or Custom folders.

This the same as the bulletins parameter in `patch.cfg`. For Red Hat Security advisories, use a hyphen (-) in place of an asterisk (*) for filtering.

Example: -bulletins MS00-001,MS00-029,RHSA-2004-*

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

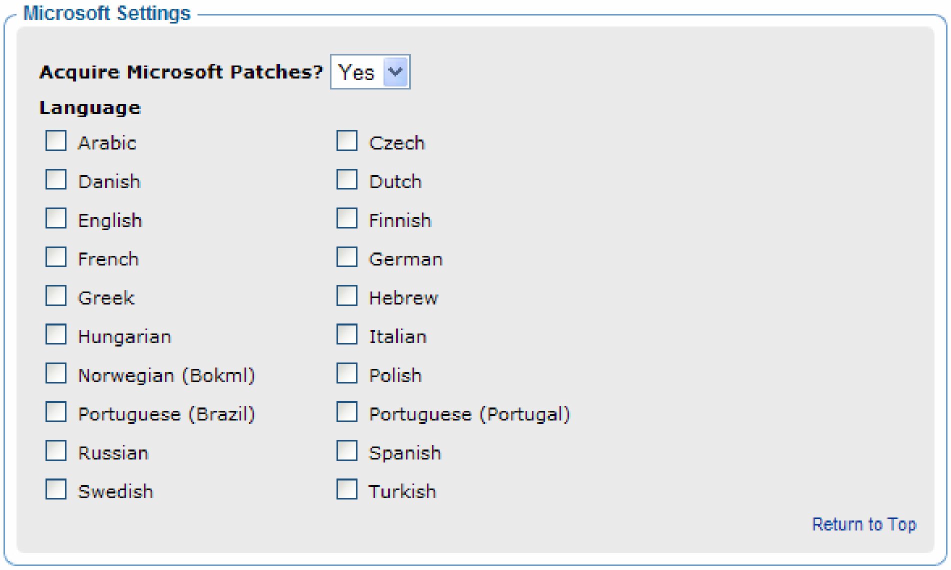
Use force when:

- 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.

Note: 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`.



Acquire Microsoft Patches? Yes

Language

□ Arabic

□ Danish

□ English

□ French

□ Greek

□ Hungarian

□ Norwegian (Bokml)

□ Portuguese (Brazil)

□ Russian

□ Swedish

□ Czech

□ Dutch

□ Finnish

□ German

□ Hebrew

□ Italian

□ Polish

□ Portuguese (Portugal)

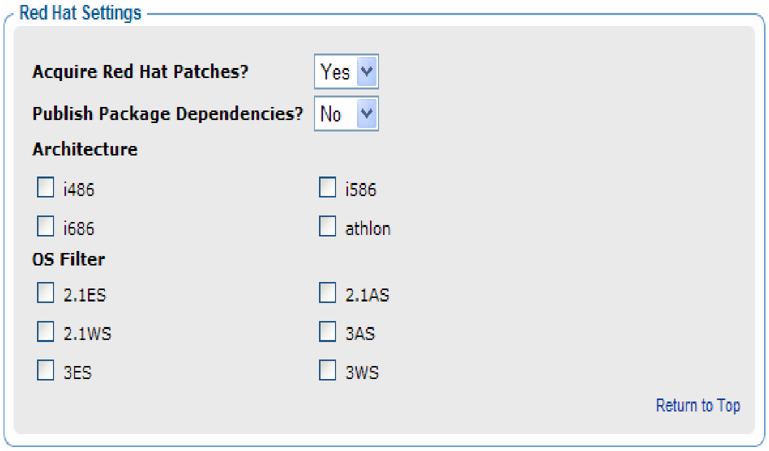
□ Spanish

□ Turkish

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`.



Red Hat Settings

Acquire Red Hat Patches? Yes

Publish Package Dependencies? No

Architecture

□ i486 □ i586

□ i686 □ athlon

OS Filter

□ 2.1ES □ 2.1AS

□ 2.1WS □ 3AS

□ 3ES □ 3WS

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, Radia 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`.

O/S Filter — Select operating systems for the acquisition of Red Hat patches. This is the same as 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.

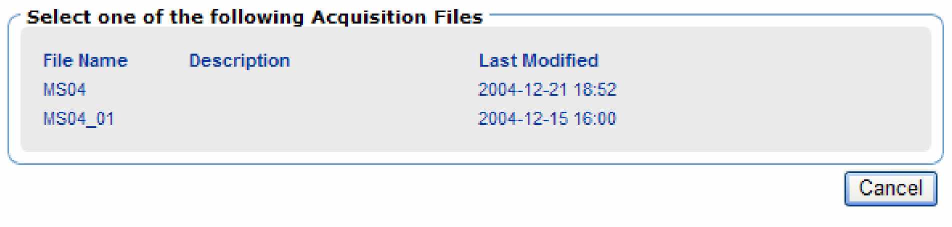
Now, you can use the Radia Patch Administrator to run the acquisition using your saved settings.

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**.

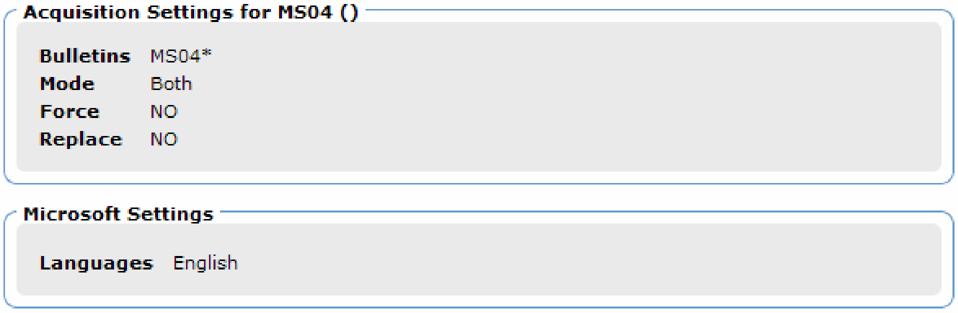
3 Select a file by clicking on its name.



Select one of the following Acquisition Files

File Name	Description	Last Modified
MS04		2004-12-21 18:52
MS04_01		2004-12-15 16:00

4 Confirm the settings for this acquisition.



Acquisition Settings for MS04 ()

Bulletins	MS04*
Mode	Both
Force	NO
Replace	NO

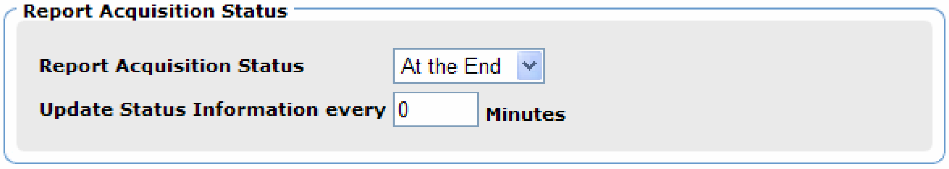
Microsoft Settings

Languages English

Report Acquisition Status

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



Report Acquisition Status

Report Acquisition Status At the End

Update Status Information every 0 **Minutes**

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 Radia 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 the table Patch Acquisition Parameters 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 3: 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 '*" wildcard character is recognized. If no bulletins are specified, then all new or updated bulletins will be acquired. Microsoft service packs are listed in the format MSSP_<operatingsystem>_<spnumber>. To acquire all service packs, specify MSSP*. For Red Hat Security advisories, use a hyphen (-) in place of a colon (:) for filtering. Example: -bulletins MS00-001,MS00-029,RHSA-2004-* Note: If you do not want to download any bulletins, use –bulletins NONE.
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`.

Table 3: Patch Acquisition Parameters

Parameter	Description
data_dir	Specify the directory where you want the patches downloaded to before they are sent to your Radia 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).
dsn	Specify the Data Source Name (DSN) the Patch ODBC database. Note: This parameter is required.
dsn_user	Specify the user for the ODBC DSN.
dsn_pass	Specify the password for the user for the ODBC DSN.
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.

Table 3: **Patch Acquisition Parameters**

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, Radia 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, Radia Patch Manager supports basic authentication only.
http_proxy_user	If you use a proxy server for http traffic, specify your user ID.

Table 3: Patch Acquisition Parameters

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	Radia 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_pass	Specify the password for Microsoft_user. (Reserved for future use.)
microsoft_sus_url	Specify the URL for the Microsoft SUS feed. Default: **http://www.msus.windowsupdate.com /msus/v1/aucatalog1.cab**.

Table 3: Patch Acquisition Parameters

Parameter	Description
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 Radia Patch Manager previous to 1.2.2, you must specify this path on the acquisition command line. This path is hard coded into Radia Patch Manager 1.2.2.
microsoft_user	Specify the user for the Microsoft web site. (Reserved for future use.)
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.
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.

Table 3: Patch Acquisition Parameters

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 are excluded since these platforms are not supported by Radia 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.
rcs_pass	If authentication has been enabled on your Radia Configuration Server, specify the password for the rcs_user.

Table 3: Patch Acquisition Parameters

Parameter	Description
rcs_url	Specify the location of your Radia Configuration Server in URL format. Use the format: *radia*://*ipaddress*:*port* where: • *radia* indicates the session type to be opened to the Radia Configuration Server • *ipaddress* is the hostname or IP address of the computer hosting the Radia Configuration Server • *port* is the port number of the Radia Configuration Server. Note: This parameter is required.
rcs_user	Specify a valid administrator id on your Radia Configuration Server.
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.

Table 3: Patch Acquisition Parameters

Parameter	Description
retire	Specify the bulletins to retire separated by commas. Use the retire parameter to: • Delete specified bulletins if they exist in the Radia Configuration Server database during the current publishing session. • Not publish the bulletins specified in the retire parameter to the Radia 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 Radia 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 which are currently under management in your enterprise, the retired security patches may be removed from your Radia Patch Manager Client devices. Example: -retire MS00-001,MS00-029

Table 3: **Patch Acquisition Parameters**

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. Prerequisite, or dependency, Red Hat packages can come 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, Radia Patch Manager will first look for the .rpm packages in the appropriate directory. For example, for Red Hat Enterprise Linux 3ES, the files should be placed in `data/patch/redhat/packages/3es`. If the dependency package 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 Network data feed. Default: **http://xmlrpc.rhn.redhat.com /XMLRPC**
superceded_patches	Set superceded_patches to Y if you want to publish the data even if a patch is marked as superceded. Default: N
sync	Specify the targets that need to be synchronized. Default: rcs.
vendors	Specify the vendors to acquire patches from. Example: -vendors Microsoft, Redhat Default: Microsoft.

Table 3: Patch Acquisition Parameters

Parameter	Description
vendor_os_filter	Specify a filter for the vendor's operating systems in the format <*vendor*>::<*operating system*>. Example: –vendor_os_filter Redhat::2.1es,Redhat::3es 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 sytems instead.

Look at the Patch Acquisition Reports on the Radia 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 Microsoft and Red Hat 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, 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
```

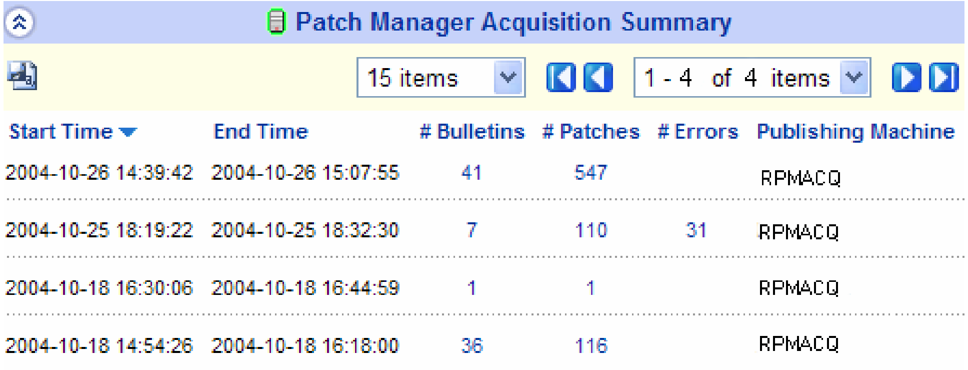
5 View the `patch-acquire.log` to see where the publishing process obtained the xml from:

```
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 Radia Reporting Server version 4.1 or above you installed. Installation and configuration information can be found in the Radia Reporting Server Guide. Under Reporting Views, click **Software Patch Reports** to expand the list of reports. If you are unable to use the Radia Reporting Server, see the appendix Radia Patch Manager Reports starting on page 139.

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.



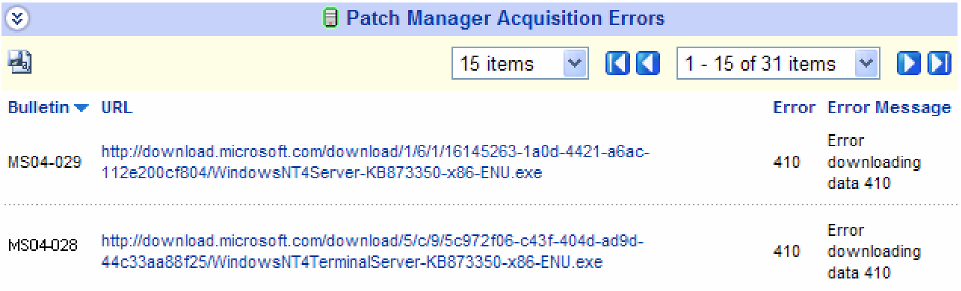
Patch Manager Acquisition Summary

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

Figure 6 View the Acquisition summary report.

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

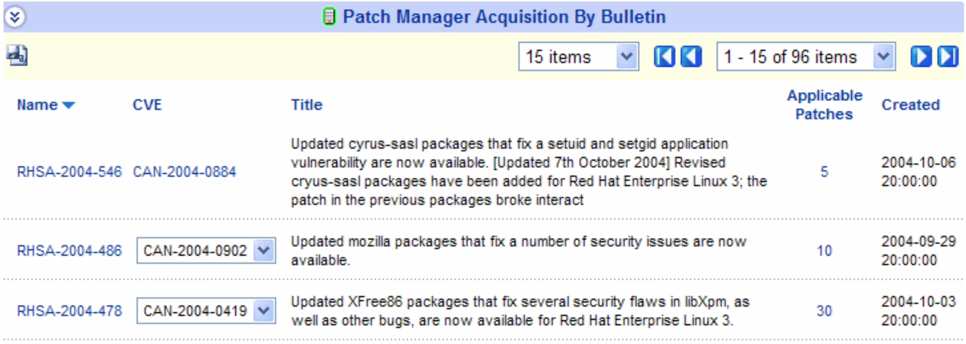
Click **# Errors** to see further explanations of why the acquisition failed. Numeric error codes displayed in the error reports are standard http status codes. For additional details on these codes, search for "HTTP Status Codes" on the World Wide Web.



Bulletin	URL	Error	Error Message
MS04-029	http://download.microsoft.com/download/1/6/1/16145263-1a0d-4421-a6ac-112e200cf804/WindowsNT4Server-KB873350-x86-ENU.exe	410	Error downloading data 410
MS04-028	http://download.microsoft.com/download/5/c/9/5c972f06-c43f-404d-ad9d-44c33aa88f25/WindowsNT4TerminalServer-KB873350-x86-ENU.exe	410	Error downloading data 410

Figure 7 View the acquisition error summary.

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

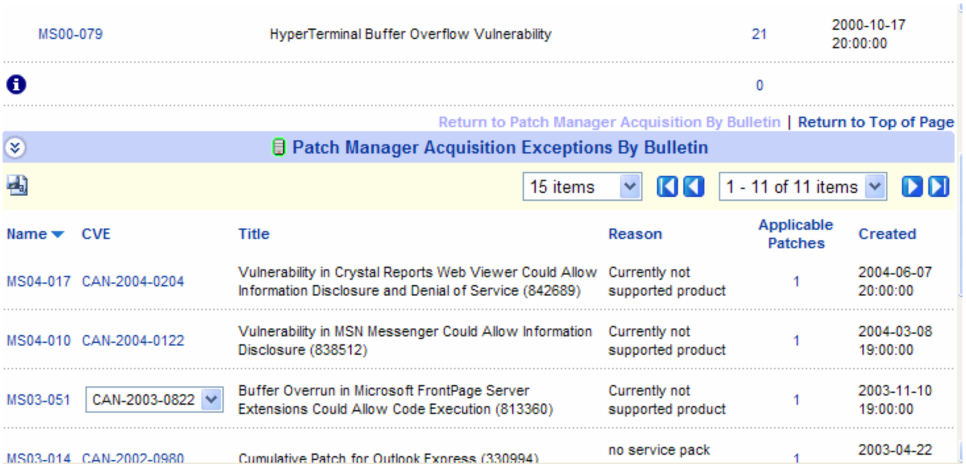


Name	CVE	Title	Applicable Patches	Created
RHSA-2004-546	CAN-2004-0884	Updated cyrus-sasl packages that fix a setuid and setgid application vulnerability are now available. [Updated 7th October 2004] Revised cryus-sasl packages have been added for Red Hat Enterprise Linux 3; the patch in the previous packages broke interact	5	2004-10-06 20:00:00
RHSA-2004-486	CAN-2004-0902	Updated mozilla packages that fix a number of security issues are now available.	10	2004-09-29 20:00:00
RHSA-2004-478	CAN-2004-0419	Updated XFree86 packages that fix several security flaws in libXpm, as well as other bugs, are now available for Red Hat Enterprise Linux 3.	30	2004-10-03 20:00:00

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 Radia Patch Manager does not support, an asterisk (*) will be displayed preceding the bulletin number. In the figure View the acquisition summary by bulletin above, one of the files associated with MS04-001 is not currently supported by Radia 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 Radia Patch Manager. These bulletins will not appear in the Research reports.



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

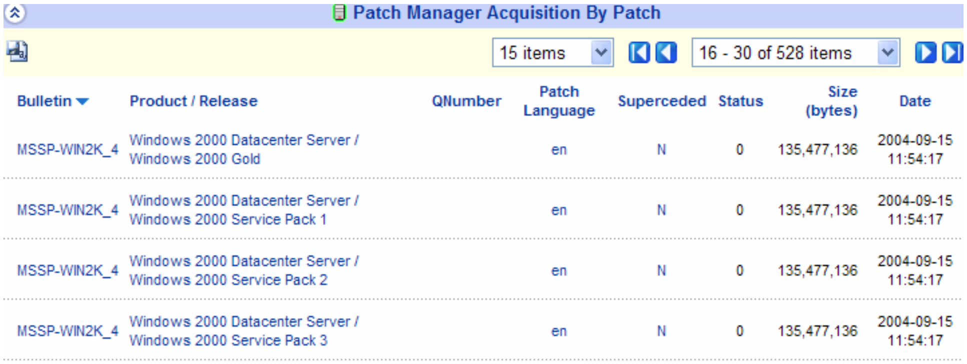
Return to Patch Manager Acquisition By Bulletin | Return to Top of Page

Patch Manager Acquisition Exceptions By Bulletin

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

Figure 9 View the acquisition exceptions by bulletin

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



Patch Manager Acquisition By Patch

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

Figure 10 View the acquisition summary by patch.

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 Radia 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. Radia 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 the table State File Creation Parameters below. Parameters set on the command line will override those from the `patch.cfg` file.

Table 4: 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 Radia Configuration Server, specify the password for the rcs_user.
rcs_url	Specify the location of your Radia Configuration Server in URL format. Use the format: *`radia`*`://`*`ipaddress`*`:`*`port`* where: • *`radia`* indicates the session type to be opened to the Radia Configuration Server. • *`ipaddress`* is the hostname or IP address of the computer hosting the Radia Configuration Server. • *`port`* is the port number of the Radia Configuration Server. Note: This parameter is required.
rcs_user	If authentication has been enabled on your Radia 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 Radia 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 the table State File Creation Parameters on page 84, 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 *Radia 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 Radia Patch Manager Client agent.
- Know how to manage patches on client devices.
- Be familiar with reports that you can generate for patch files.

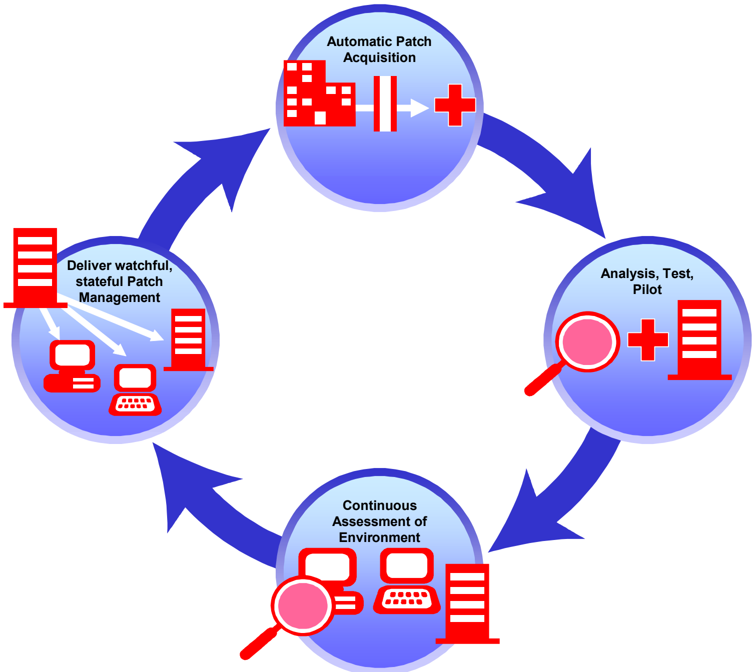

Automatic Patch Acquisition
Analysis, Test, Pilot
Continuous Assessment of Environment
Deliver watchful, stateful Patch Management

Figure 11 Product discovery and analysis.

Installing the Radia Patch Manager Client

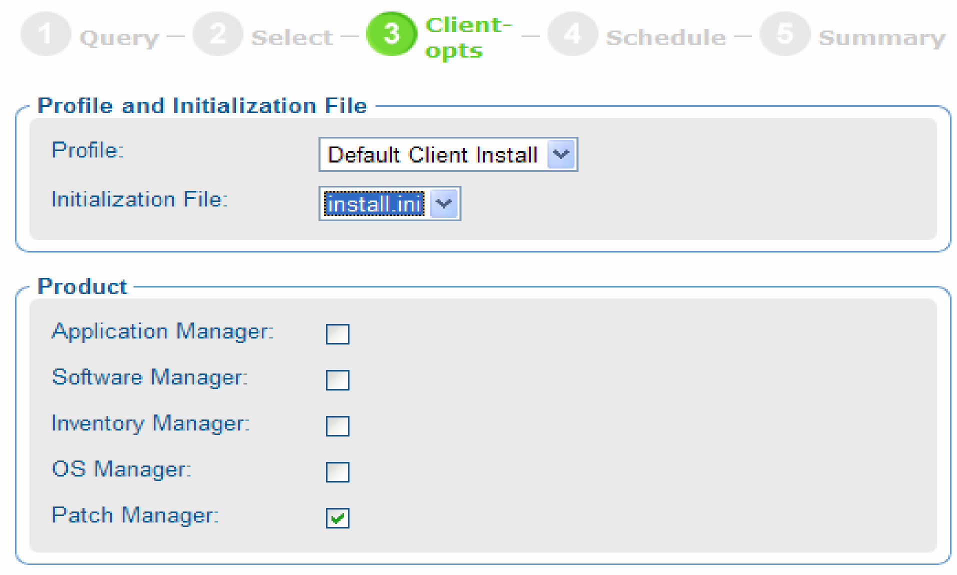
The Radia Patch Manager Client must be installed on any client computer that you want to manage vulnerabilities for. You can do this using the Radia Management Portal or using the installation from the CD-ROM provided. For detailed installation instructions, see the *Radia Management Portal Guide* or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

The minimum required version of nvdkit is 145 for the Radia 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 Radia Management Portal version 2.0. These screens and instructions may change in future versions. See the *Radia Management Portal Guide* for additional information.

To install the Radia Patch Manager Client from the Radia Management Portal

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



Profile and Initialization File

Profile: Default Client Install

Initialization File: install.ini

Product

Application Manager: □

Software Manager: □

Inventory Manager: □

OS Manager: □

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 Radia 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 Radia 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 the client agent for Linux

The minimum Radia client version supported for Linux is 3.1.2. This version includes nvdkit build version 145. The Radia Patch Manager Client Agent for Linux supports Red Hat Enterprise Server 2.1 and 3 for patch deployment.

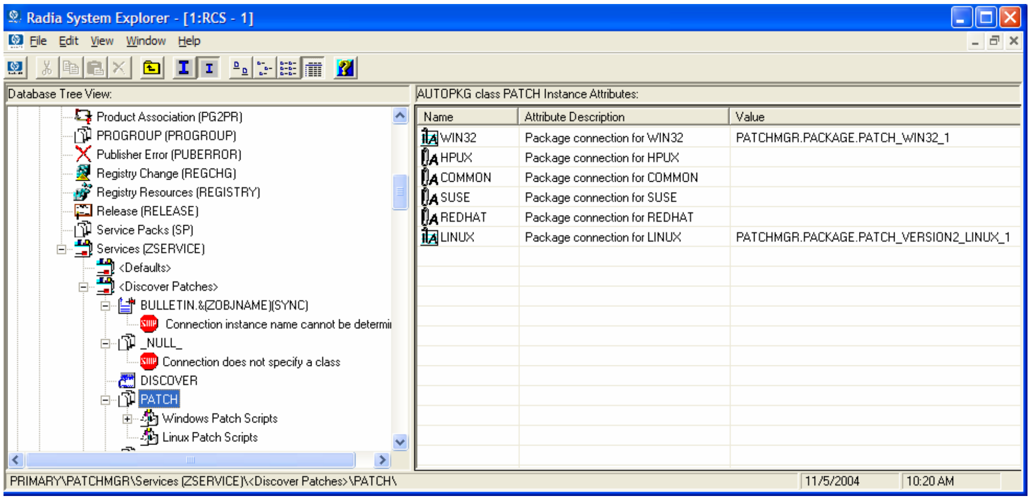
- HP will provide a file called maint31.tar located in the `Patch Agent Maintenance\redhat\ram` folder on the CD-ROM. Copy maint31.tar to the same directory as the client31.tar file. (For installations using Radia Management Portal, copy the file to `\integrationserver\media\client\default\linux\ram`.)

Updating the Radia Patch Manager Client Agent

When you run a patch acquisition, you can also download updated product discovery scripts. These files are received from the Novadigm 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.

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

Client agent files are distributed when the Discover Patch Service is processed on the Radia 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 Radia System Explorer to do this. An example is shown below.



Database Tree View:

- Product Association (PG2PR)
- PROGROUP (PROGROUP)
- Publisher Error (PUBERROR)
- Registry Change (REGCHG)
- Registry Resources (REGISTRY)
- Release (RELEASE)
- Service Packs (SP)
- Services (ZSERVICE)
  - <Defaults>
  - <Discover Patches>
    - BULLETIN.&(ZOBJNAME)(SYNC)
      - Connection instance name cannot be determi
    - _NULL_
      - Connection does not specify a class
    - DISCOVER
    - PATCH
      - Windows Patch Scripts
      - Linux Patch Scripts

AUTOPKG class PATCH Instance Attributes:

Name	Attribute Description	Value
WIN32	Package connection for WIN32	PATCHMGR.PACKAGE.PATCH_WIN32_1
HPUX	Package connection for HPUX	
COMMON	Package connection for COMMON	
SUSE	Package connection for SUSE	
REDHAT	Package connection for REDHAT	
LINUX	Package connection for LINUX	PATCHMGR.PACKAGE.PATCH_VERSION2_LINUX_1

PRIMARY\PATCHMGR\Services (ZSERVICE)\<Discover Patches>\PATCH\ 11/5/2004 10:20 AM

Figure 12 Create connections to the published package.

Table 5: AGENT_UPDATES values

Value	Description
"" or blank	The agent updates will not be published to the Radia Database's PATCHMGR domain.

Value	Description
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 Radia Patch Manager Client computers.
Publish	The updates will be published to the PATCHMGR domain, but will not be connected for distribution to Radia 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, and hpux.
- Agent_version
  Use –agent_version to select which Radia Patch Manager version for which you would like to acquire the agent updates. You can only publish one version to one Radia Configuration Server. One Radia Configuration Server cannot host multiple versions of the agent. If piloting, create a separate Radia 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 Radia Patch Manager Client must discover which products are on the client computer. Radia Patch Manager objects are cached locally on the client device to optimize bandwidth. Objects are downloaded only if they are different. In addition, the Radia Patch Manager Client needs to detect which patches are installed for each discovered product. To do this, assign the Radia Patch Manager Discover Patch Service to the client computers.

➤ Running the Radia Patch Manager Client connect *requires* that the dname parameter be set to PATCH. This will keep the resolution of services for the Radia Patch Manager Client separate from the resolution of services for the Radia Application Manager client. If you are using Radia Policy Server with Radia Patch Manager, see the appendix Radia Policy Server Integration starting on page 137.

To perform patch discovery

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

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 *Radia Application Manager Guide*.

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 Radia 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\default`. The Radia Messaging Service exports this information to the Patch SQL 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 SQL Database, not in the Radia Database as in previous releases.

Radia Patch Manager Administrator Icons

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

Figure 13 Click an icon.

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

Patch Analysis and Reports

Radia Reporting Server provides web-based reports for Radia Patch Manager. For installation and configuration instructions for the Radia Reporting Server, see the *Radia Reporting Server Guide*. The installation media is on the Radia Infrastructure CD-ROM. To view the reports, first access your Radia Reporting Server. Then, under Reporting Views, click **Software Patch Reports** to expand the list of reports. If you are unable to use the Radia Reporting Server, see the appendix Radia Patch Manager Reports starting on page 139.

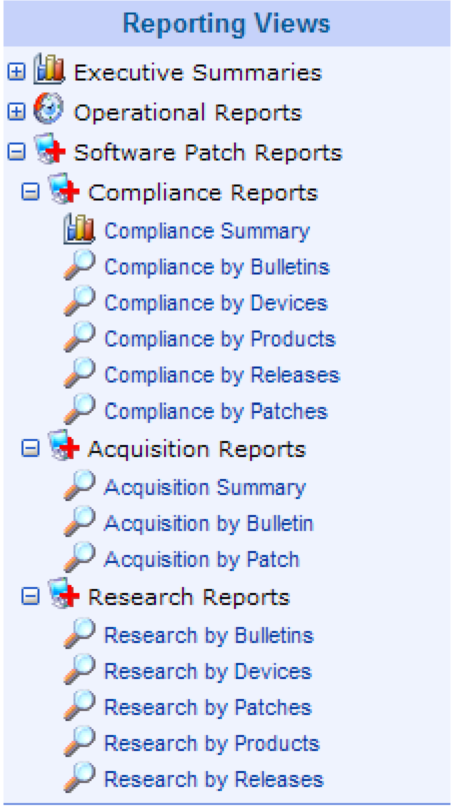


Figure 14 View the list of Radia Patch Manager Reports.

There are three types of Patch Manager Reports, Compliance, Acquisition, and Research. For information on the Acquisition Reports, see the chapter Patch Acquisition starting on page 57.

Filtering Patch Reports with Radia Reporting Server

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

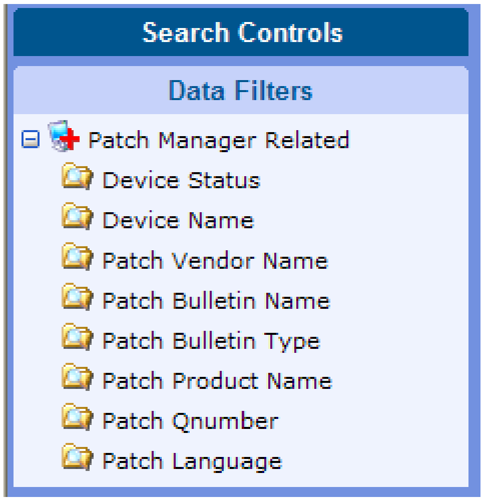


Figure 15 View the Patch Manager Related Data Filters.

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

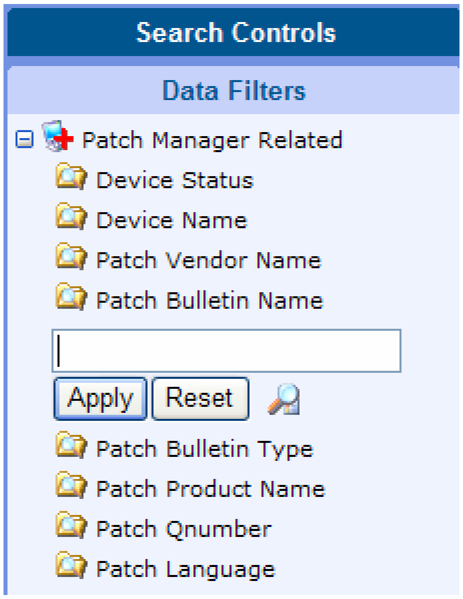


Figure 16 Expand a filter.

Click the magnifying glass to open the filter lookup window.

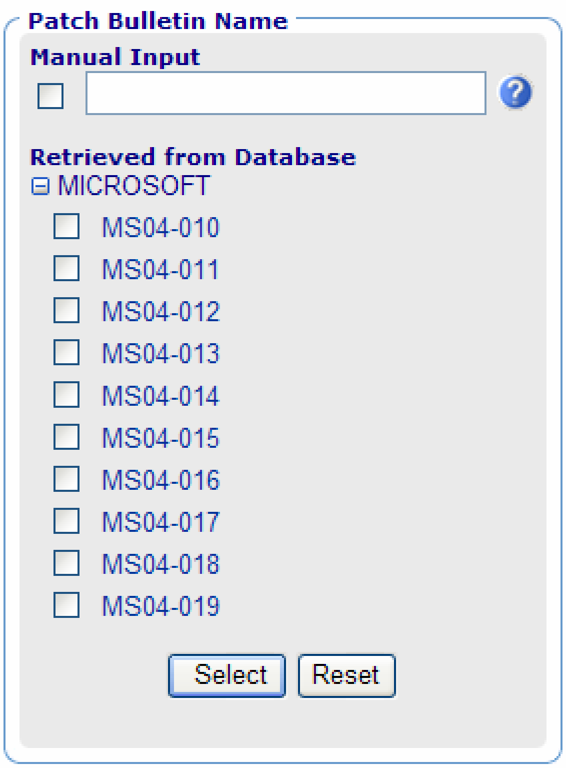


Figure 17 Select the filters.

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 *Radia Reporting Server Guide*.

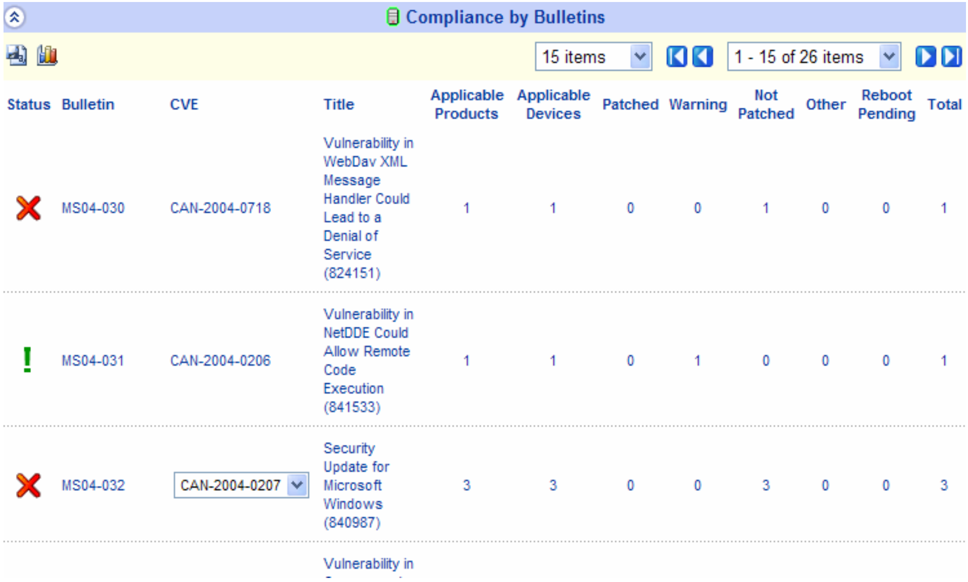
Compliance Reports

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



Compliance by Bulletins

15 items | 1 - 15 of 26 items

Status	Bulletin	CVE	Title	Applicable Products	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗	MS04-030	CAN-2004-0718	Vulnerability in WebDav XML Message Handler Could Lead to a Denial of Service (824151)	1	1	0	0	1	0	0	1
!	MS04-031	CAN-2004-0206	Vulnerability in NetDDE Could Allow Remote Code Execution (841533)	1	1	1	0	0	0	0	1
✗	MS04-032	CAN-2004-0207	Security Update for Microsoft Windows (840987)	3	3	0	0	3	0	0	3
			Vulnerability in								

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 Radia 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 Radia Patch Manager cannot report the vulnerability as being patched, this would be reported as a warning.

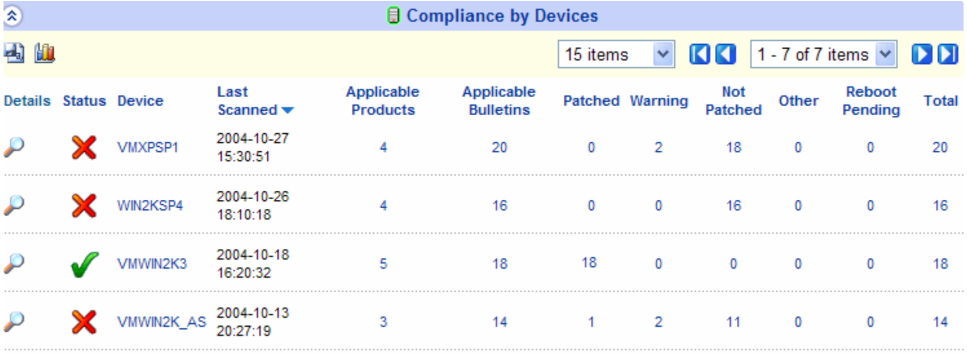
  Another example may be that a file version on the device is newer than the one delivered by the patch. Again, in this case, Radia Patch Manager cannot report the vulnerability as being patched so it reports a warning.
- Click the number in the Not Patched column to see what patches are available but have not been applied.
- Items in the Other column represent patches that Radia 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 mark indicates a warning.



Compliance by Devices

15 items | 1 - 7 of 7 items

Details	Status	Device	Last Scanned	Applicable Products	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending	Total
🔍	✗	VMXPSP1	2004-10-27 15:30:51	4	20	0	2	18	0	0	20
🔍	✗	WIN2KSP4	2004-10-26 18:10:18	4	16	0	0	16	0	0	16
🔍	✓	VMWIN2K3	2004-10-18 16:20:32	5	18	18	0	0	0	0	18
🔍	✗	VMWIN2K_AS	2004-10-13 20:27:19	3	14	1	2	11	0	0	14

For each device, you can

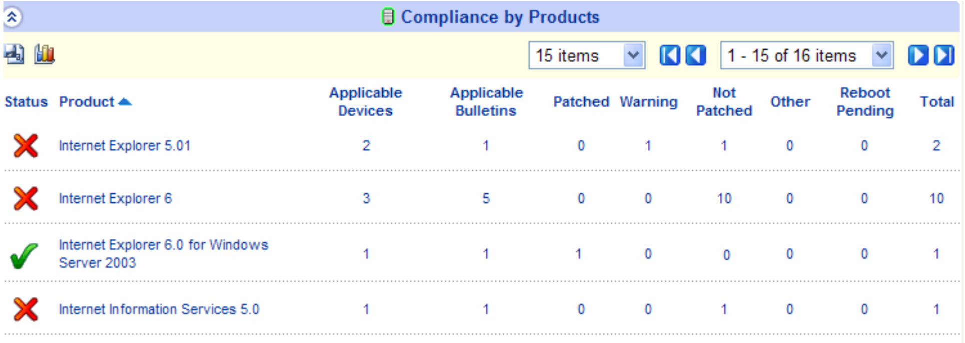
- Click the magnifying glass for additional detail.
- Click the number in the Applicable Products column to see the products discovered for that device.
- Click the number in the Applicable Bulletins column to see the applicable bulletins for that device.

  - 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 Radia 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 Radia 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, Radia 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 Radia 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.

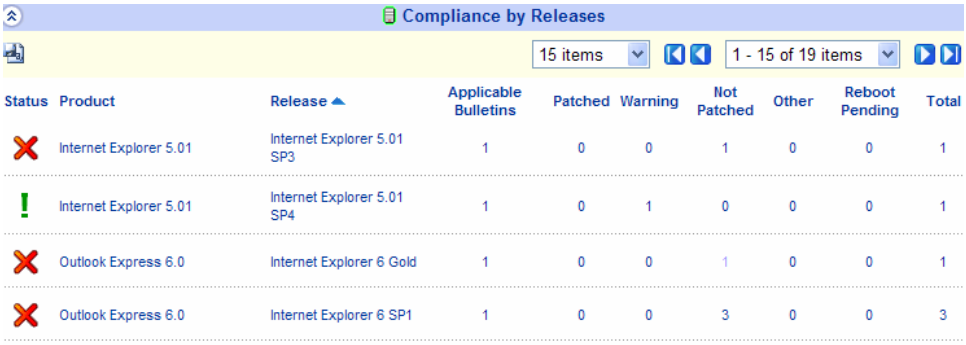
- **Compliance by Products**
  This report displays one row for each product. For each product, you can
  - Click the number in the Applicable Devices column to see the devices affected by the vulnerability.
  - Click the number in the Applicable Bulletins column to see bulletins for the product.
  - View detected vulnerabilities.



Compliance by Products

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

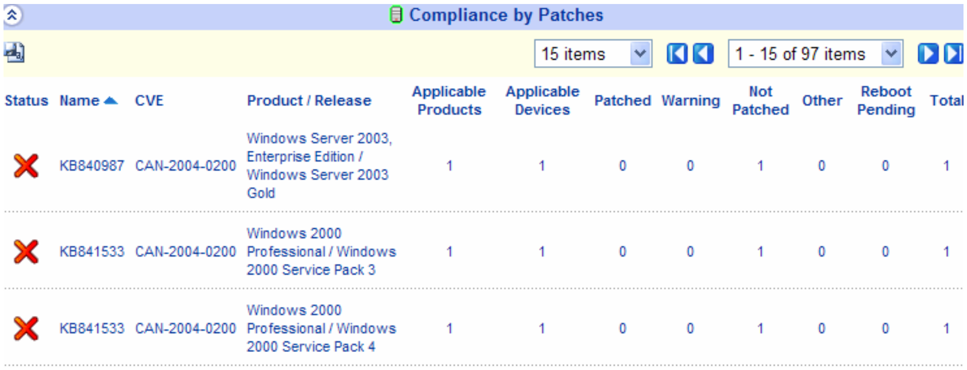
- **Compliance by Releases**
  This report lists products by release. There is one row for each release of each product. Click to see **Applicable Bulletins.**



Compliance by Releases

Status	Product	Release	Applicable Bulletins	Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗	Internet Explorer 5.01	Internet Explorer 5.01 SP3	1	0	0	1	0	0	1
!	Internet Explorer 5.01	Internet Explorer 5.01 SP4	1	0	1	0	0	0	1
✗	Outlook Express 6.0	Internet Explorer 6 Gold	1	0	0	1	0	0	1
✗	Outlook Express 6.0	Internet Explorer 6 SP1	1	0	0	3	0	0	3

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

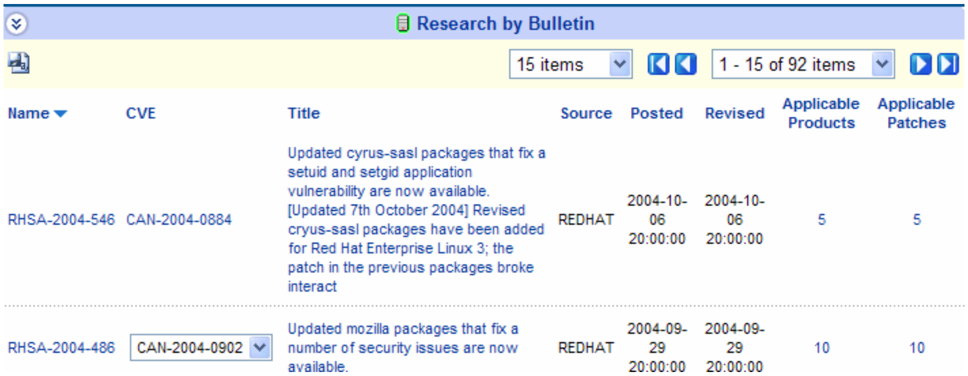


Status	Name ▲	CVE	Product / Release	Applicable Products	Applicable Devices	Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗	KB840987	CAN-2004-0200	Windows Server 2003, Enterprise Edition / Windows Server 2003 Gold	1	1	0	0	1	0	0	1
✗	KB841533	CAN-2004-0200	Windows 2000 Professional / Windows 2000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

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.

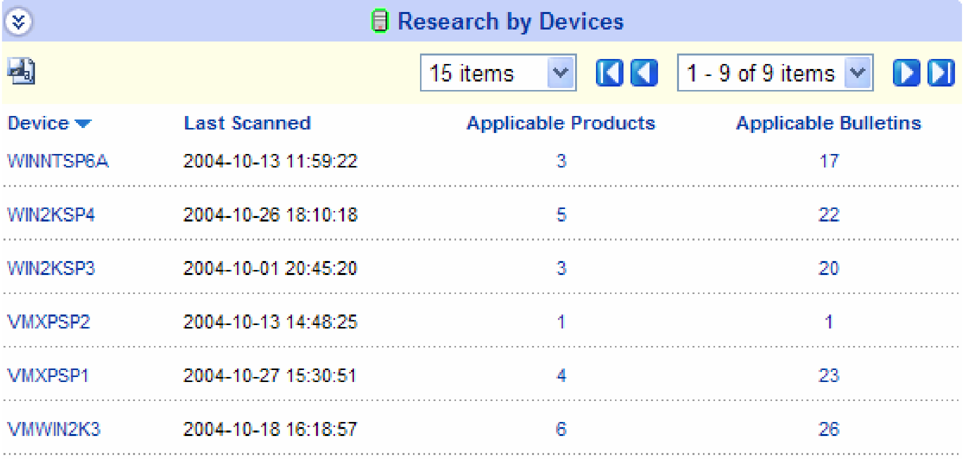
- **Research by Bulletin**
  Use this report to drill down to all bulletins. Click on the bulletin's number in the Name column to go to the vendor's web site for more information. Click on the number in the CVE column to go to the Common Vulnerability Exposures web site. Click the number in the Title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

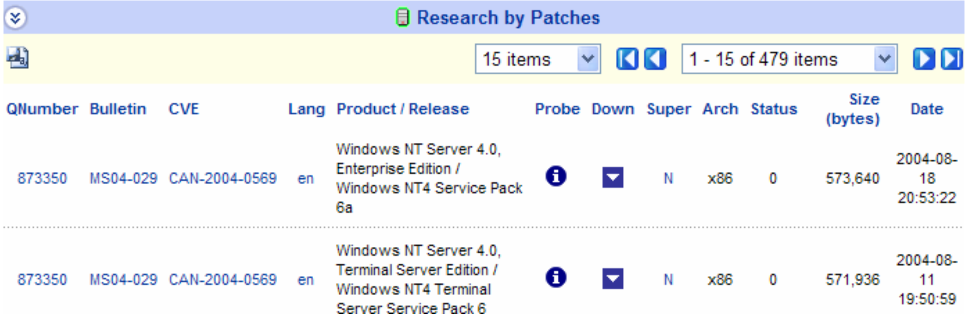


Research by Devices

15 items | 1 - 9 of 9 items

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.

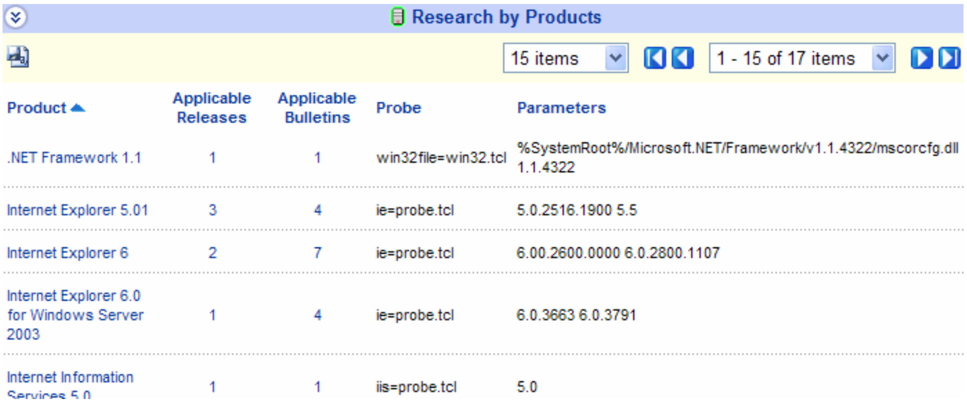


Research by Patches

15 items | 1 - 15 of 479 items

QNumber	Bulletin	CVE	Lang	Product / Release	Probe	Down	Super	Arch	Status	Size (bytes)	Date
873350	MS04-029	CAN-2004-0569	en	Windows NT Server 4.0, Enterprise Edition / Windows NT4 Service Pack 6a	ℹ	▼	N	x86	0	573,640	2004-08-18 20:53:22
873350	MS04-029	CAN-2004-0569	en	Windows NT Server 4.0, Terminal Server Edition / Windows NT4 Terminal Server Service Pack 6	ℹ	▼	N	x86	0	571,936	2004-08-11 19:50:59

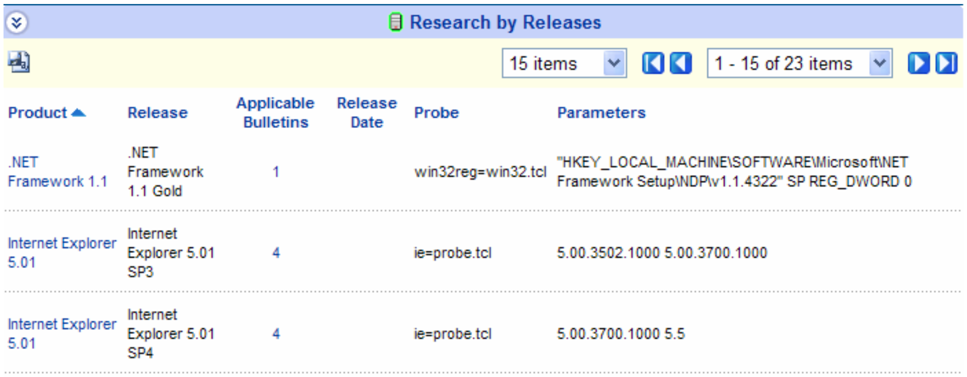
- **Research by Products**
  Use this report to drill down to all bulletins filtered by product.



Research by Products

Product	Applicable Releases	Applicable Bulletins	Probe	Parameters
.NET Framework 1.1	1	1	win32file=win32.tcl	%SystemRoot%/Microsoft.NET/Framework/v1.1.4322/mscorcfg.dll 1.1.4322
Internet Explorer 5.01	3	4	ie=probe.tcl	5.0.2516.1900 5.5
Internet Explorer 6	2	7	ie=probe.tcl	6.00.2600.0000 6.0.2800.1107
Internet Explorer 6.0 for Windows Server 2003	1	4	ie=probe.tcl	6.0.3663 6.0.3791
Internet Information Services 5.0	1	1	iis=probe.tcl	5.0

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



Research by Releases

Product	Release	Applicable Bulletins	Release Date	Probe	Parameters
.NET Framework 1.1	.NET Framework 1.1 Gold	1		win32reg=win32.tcl	"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v1.1.4322" SP REG_DWORD 0
Internet Explorer 5.01	Internet Explorer 5.01 SP3	4		ie=probe.tcl	5.00.3502.1000 5.00.3700.1000
Internet Explorer 5.01	Internet Explorer 5.01 SP4	4		ie=probe.tcl	5.00.3700.1000 5.5

Managing Vulnerabilities

After you have found where vulnerabilities may exist in your enterprise, use Radia 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 *Radia Application Manager Guide* for complete descriptions of the attributes available in the ZSERVICE instance in the

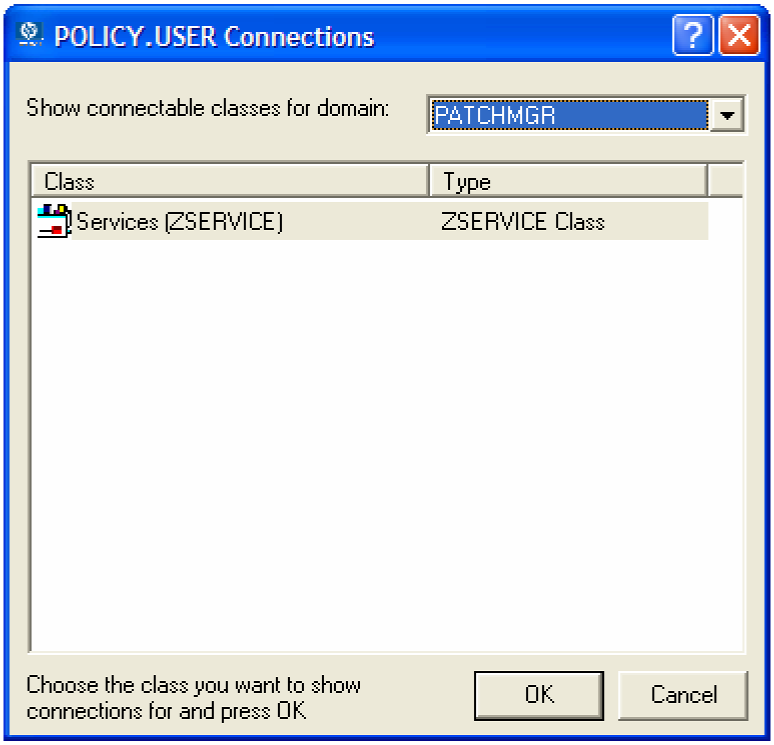
SOFTWARE domain. In addition, the PATCHMGR.ZSERVICE instance supports bandwidth throttling. See the HP OpenView web site for details.

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.

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.



POLICY.USER Connections

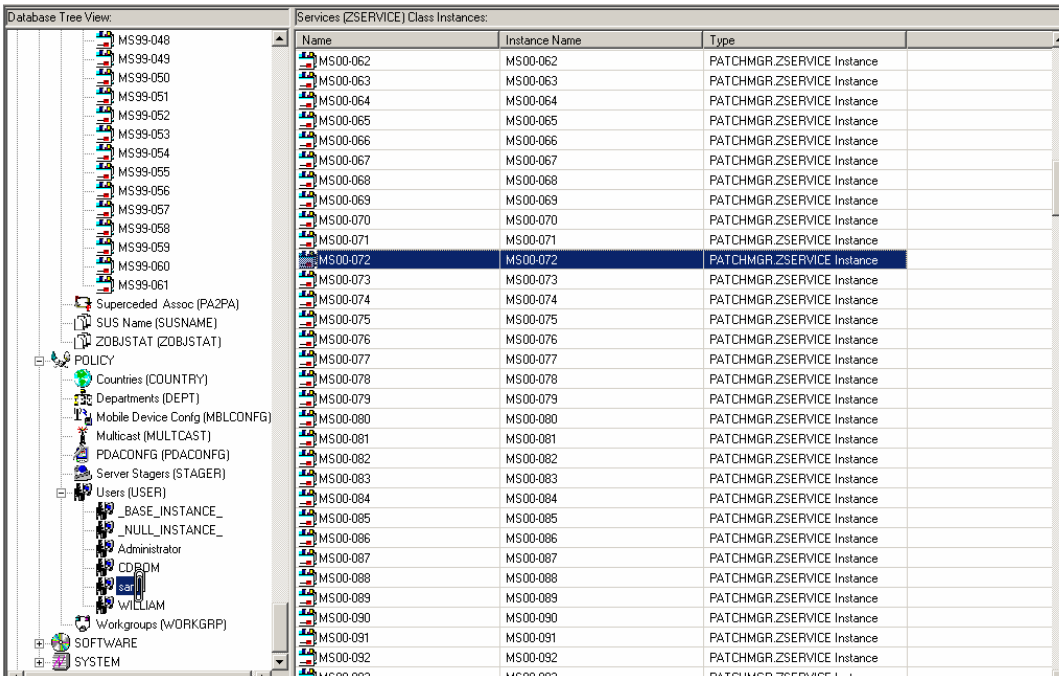
Show connectable classes for domain: PATCHMGR

Class	Type
Services (ZSERVICE)	ZSERVICE Class

Choose the class you want to show connections for and press OK

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. In this example, bulletin MS00-072 is connected to the Sam user instance.



Database Tree View:

- MS99-048
- MS99-049
- MS99-050
- MS99-051
- MS99-052
- MS99-053
- MS99-054
- MS99-055
- MS99-056
- MS99-057
- MS99-058
- MS99-059
- MS99-060
- MS99-061
- Superceded Assoc (PA2PA)
- SUS Name (SUSNAME)
- ZOBJSTAT (ZOBJSTAT)
- POLICY
  - Countries (COUNTRY)
  - Departments (DEPT)
  - Mobile Device Confg (MBLCONFG)
  - Multicast (MULTCAST)
  - PDACONFG (PDACONFG)
  - Server Stagers (STAGER)
  - Users (USER)
    - _BASE_INSTANCE_
    - _NULL_INSTANCE_
    - Administrator
    - CDROM
    - sam
    - WILLIAM
  - Workgroups (WORKGRP)
- SOFTWARE
- SYSTEM

Services (ZSERVICE) Class Instances:

Name	Instance Name	Type
MS00-062	MS00-062	PATCHMGR.ZSERVICE Instance
MS00-063	MS00-063	PATCHMGR.ZSERVICE Instance
MS00-064	MS00-064	PATCHMGR.ZSERVICE Instance
MS00-065	MS00-065	PATCHMGR.ZSERVICE Instance
MS00-066	MS00-066	PATCHMGR.ZSERVICE Instance
MS00-067	MS00-067	PATCHMGR.ZSERVICE Instance
MS00-068	MS00-068	PATCHMGR.ZSERVICE Instance
MS00-069	MS00-069	PATCHMGR.ZSERVICE Instance
MS00-070	MS00-070	PATCHMGR.ZSERVICE Instance
MS00-071	MS00-071	PATCHMGR.ZSERVICE Instance
MS00-072	MS00-072	PATCHMGR.ZSERVICE Instance
MS00-073	MS00-073	PATCHMGR.ZSERVICE Instance
MS00-074	MS00-074	PATCHMGR.ZSERVICE Instance
MS00-075	MS00-075	PATCHMGR.ZSERVICE Instance
MS00-076	MS00-076	PATCHMGR.ZSERVICE Instance
MS00-077	MS00-077	PATCHMGR.ZSERVICE Instance
MS00-078	MS00-078	PATCHMGR.ZSERVICE Instance
MS00-079	MS00-079	PATCHMGR.ZSERVICE Instance
MS00-080	MS00-080	PATCHMGR.ZSERVICE Instance
MS00-081	MS00-081	PATCHMGR.ZSERVICE Instance
MS00-082	MS00-082	PATCHMGR.ZSERVICE Instance
MS00-083	MS00-083	PATCHMGR.ZSERVICE Instance
MS00-084	MS00-084	PATCHMGR.ZSERVICE Instance
MS00-085	MS00-085	PATCHMGR.ZSERVICE Instance
MS00-086	MS00-086	PATCHMGR.ZSERVICE Instance
MS00-087	MS00-087	PATCHMGR.ZSERVICE Instance
MS00-088	MS00-088	PATCHMGR.ZSERVICE Instance
MS00-089	MS00-089	PATCHMGR.ZSERVICE Instance
MS00-090	MS00-090	PATCHMGR.ZSERVICE Instance
MS00-091	MS00-091	PATCHMGR.ZSERVICE Instance
MS00-092	MS00-092	PATCHMGR.ZSERVICE Instance

5. Click **Copy**.
6. Click **Yes** to Confirm the Connection.

The patch is added to the user's policy. The next time the Sam 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. Radia 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. Radia Patch Manager can detect vulnerabilities for both automatic and interactive patches. Radia 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 Radia 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 Radia 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
```

For more information on radskman, see the *Radia 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 a !) 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 Radia 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 Radia Patch Manager and will be available in Radia 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 Radia 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 the table DesiredState Tag (DSTATE) and Descriptions on page 110 with a return code from the table Return Code Values on page 110. Separate multiple conditions with commas.

Table 6: 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 7: 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" />
```

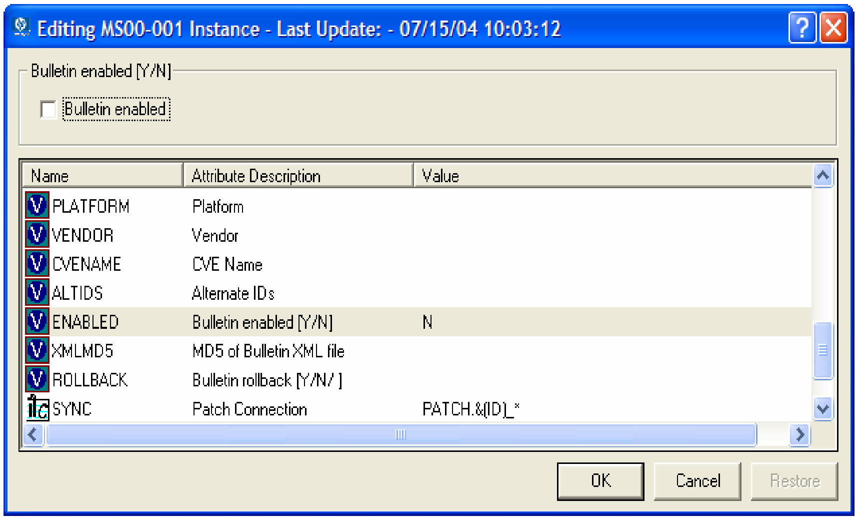
The values in the XML file are entirely surrounded by quotes.

3 Set a REPORT threshold. The properties of the file or registry key will be sent to the Radia 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 Radia Patch Manager and will be available in Radia 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 Radia System Explorer to set the ENABLED attribute to N in the Bulletin or Patch instance in the PATCHMGR domain.


Editing MS00-001 Instance - Last Update: - 07/15/04 10:03:12

Bulletin enabled [Y/N]

□ Bulletin enabled

Name	Attribute Description	Value
PLATFORM	Platform	
VENDOR	Vendor	
CVENAME	CVE Name	
ALTIDS	Alternate IDs	
ENABLED	Bulletin enabled [Y/N]	N
XMLMD5	MD5 of Bulletin XML file	
ROLLBACK	Bulletin rollback [Y/N/]	
SYNC	Patch Connection	PATCH.&(ID)_*

Figure 18 Disable detection of Bulletin MS00-001.

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

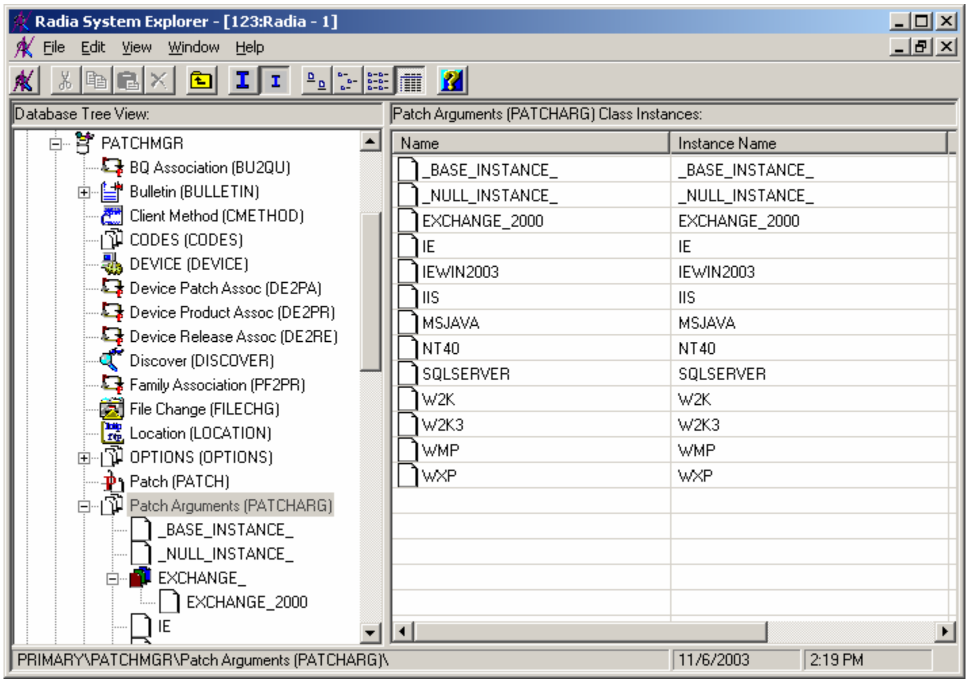
Controlling Patch Deployment (PATCHARG)

For each patch file, Radia 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 Radia System Explorer to navigate to the PATCHARG class in the PATCHMGR domain.

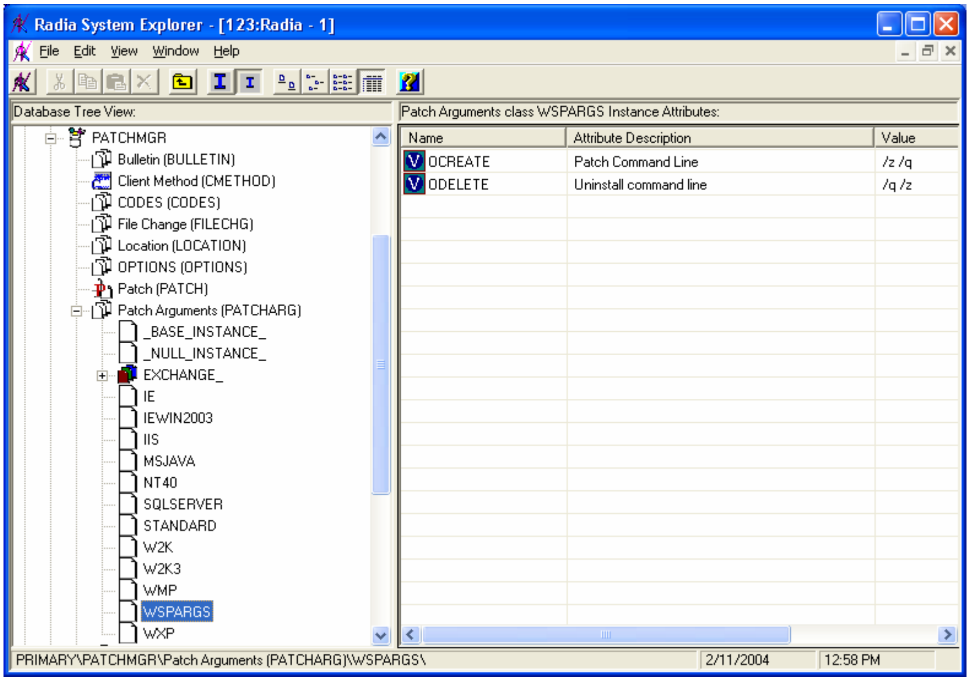


Patch Arguments (PATCHARG) Class Instances:

Name	Instance Name
_BASE_INSTANCE_	_BASE_INSTANCE_
_NULL_INSTANCE_	_NULL_INSTANCE_
EXCHANGE_2000	EXCHANGE_2000
IE	IE
IEWIN2003	IEWIN2003
IIS	IIS
MSJAVA	MSJAVA
NT40	NT40
SQLSERVER	SQLSERVER
W2K	W2K
W2K3	W2K3
WMP	WMP
WXP	WXP

PRIMARY\PATCHMGR\Patch Arguments (PATCHARG)\ 11/6/2003 2:19 PM

2 Right-click **PATCHARG** and create a new instance. A new instance called WSPARGS has been created in the figure below.



Database Tree View:

PATCHMGR
Bulletin (BULLETIN)
Client Method (CMETHOD)
CODES (CODES)
File Change (FILECHG)
Location (LOCATION)
OPTIONS (OPTIONS)
Patch (PATCH)
Patch Arguments (PATCHARG)
_BASE_INSTANCE_
_NULL_INSTANCE_
EXCHANGE_
IE
IEWIN2003
IIS
MSJAVA
NT40
SQLSERVER
STANDARD
W2K
W2K3
WMP
WSPARGS
WXP

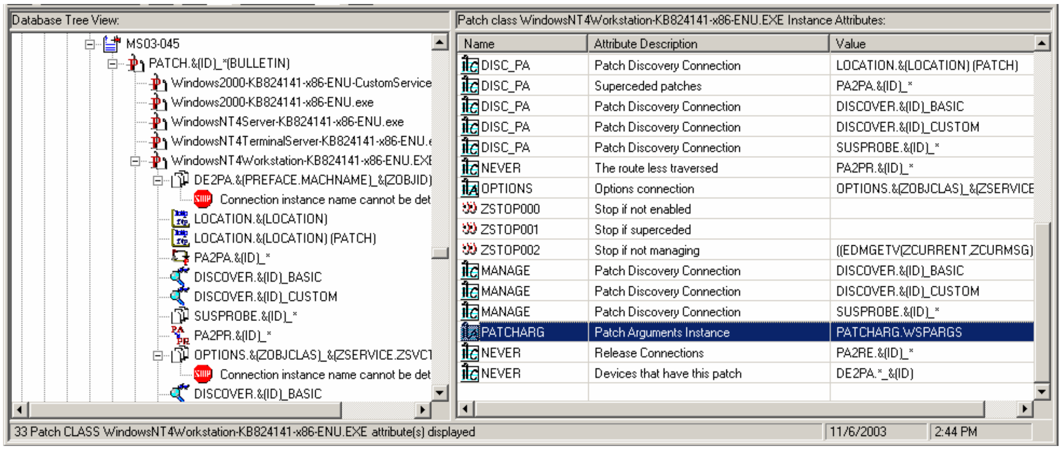
Patch Arguments class WSPARGS Instance Attributes:

Name	Attribute Description	Value
V OCREATE	Patch Command Line	/z /q
V ODELETE	Uninstall command line	/q /z

PRIMARY\PATCHMGR\Patch Arguments (PATCHARG)\WSPARGS\ 2/11/2004 12:58 PM

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.



Database Tree View:

MS03-045
PATCH.&(ID)_*(BULLETIN)
Windows2000-KB824141-x86-ENU-CustomService
Windows2000-KB824141-x86-ENU.exe
WindowsNT4Server-KB824141-x86-ENU.exe
WindowsNT4TerminalServer-KB824141-x86-ENU.e
WindowsNT4Workstation-KB824141-x86-ENU.EXE
DE2PA.&(PREFACE.MACHNAME)_&(ZOBJID)
Connection instance name cannot be det
LOCATION.&(LOCATION)
LOCATION.&(LOCATION) (PATCH)
PA2PA.&(ID)_*
DISCOVER.&(ID)_BASIC
DISCOVER.&(ID)_CUSTOM
SUSPROBE.&(ID)_*
PA2PR.&(ID)_*
OPTIONS.&(ZOBJCLAS)_&(ZSERVICE.ZSVCT
Connection instance name cannot be det
DISCOVER.&(ID)_BASIC

Patch class WindowsNT4Workstation-KB824141-x86-ENU.EXE Instance Attributes:

Name	Attribute Description	Value
DISC_PA	Patch Discovery Connection	LOCATION.&(LOCATION) (PATCH)
DISC_PA	Superceded patches	PA2PA.&(ID)_*
DISC_PA	Patch Discovery Connection	DISCOVER.&(ID)_BASIC
DISC_PA	Patch Discovery Connection	DISCOVER.&(ID)_CUSTOM
DISC_PA	Patch Discovery Connection	SUSPROBE.&(ID)_*
NEVER	The route less traversed	PA2PR.&(ID)_*
OPTIONS	Options connection	OPTIONS.&(ZOBJCLAS)_&(ZSERVICE
ZSTOP000	Stop if not enabled	
ZSTOP001	Stop if superceded	
ZSTOP002	Stop if not managing	((EDMGETV(ZCURRENT.ZCURMSG)
MANAGE	Patch Discovery Connection	DISCOVER.&(ID)_BASIC
MANAGE	Patch Discovery Connection	DISCOVER.&(ID)_CUSTOM
MANAGE	Patch Discovery Connection	SUSPROBE.&(ID)_*
PATCHARG	Patch Arguments Instance	PATCHARG.WSPARGS
NEVER	Release Connections	PA2RE.&(ID)_*
NEVER	Devices that have this patch	DE2PA.*_&(ID)

33 Patch CLASS WindowsNT4Workstation-KB824141-x86-ENU.EXE attribute(s) displayed 11/6/2003 2:44 PM

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

Preloading Radia Proxy Server and Radia Staging Servers

If you are using a Radia Proxy Server or Radia Staging Server you may want to preload the patch files. To do this, go to your preload user instance (the default for Radia 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, then type **`PATCHMGR.ZSERVICE .MS03-*(PRELOAD)`** in the connection instance.

The next time you run a preload, the Radia Proxy Server or Radia Staging Server will load the compressed data files from the PATCHMGR domain. For more information on preloading, see the *Radia Proxy Server Guide* or the *Radia 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.

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

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.

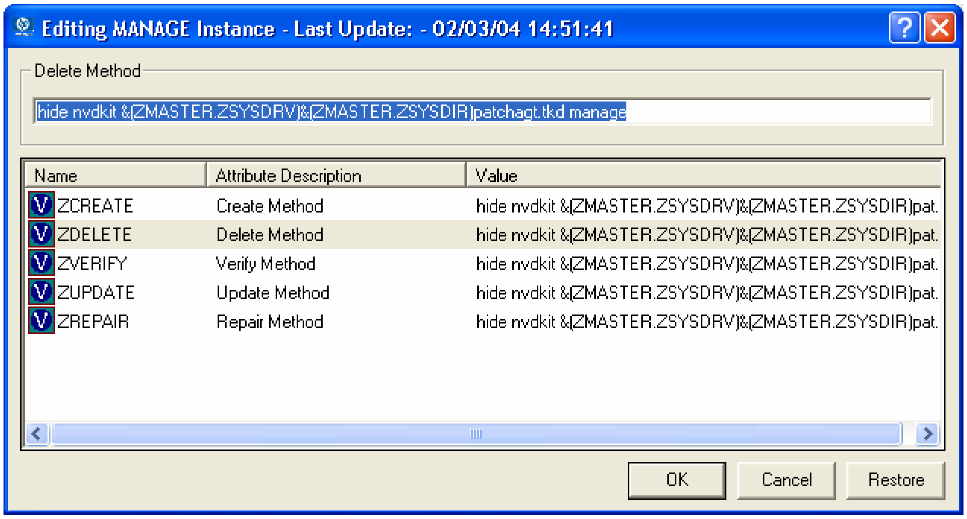
To remove a patch when a user is no longer assigned the service

1 Use Radia 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
```



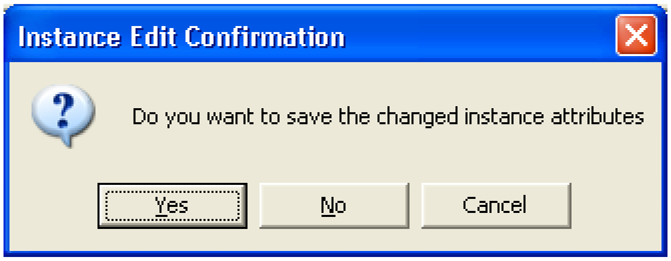
Editing MANAGE Instance - Last Update: - 02/03/04 14:51:41

Delete Method

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

Name	Attribute Description	Value
ZCREATE	Create Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)pat.
ZDELETE	Delete Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)pat.
ZVERIFY	Verify Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)pat.
ZUPDATE	Update Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)pat.
ZREPAIR	Repair Method	hide nvdkit &(ZMASTER.ZSYSDRV)&(ZMASTER.ZSYSDIR)pat.

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



Instance Edit Confirmation

Do you want to save the changed instance attributes

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

6 The Radia 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.

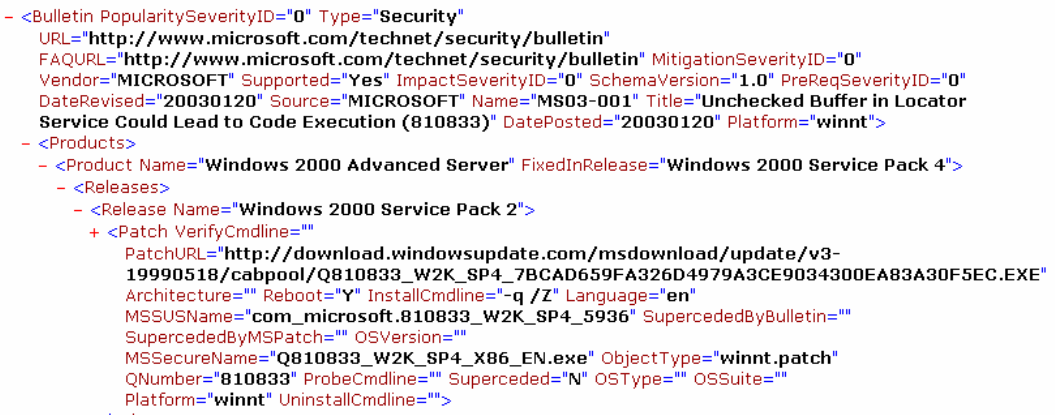
Summary

- Install the Radia Patch Manager Client on devices that you want to manage.
- Radia 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.



```
- <Bulletin PopularitySeverityID="0" Type="Security"
   URL="http://www.microsoft.com/technet/security/bulletin"
   FAQURL="http://www.microsoft.com/technet/security/bulletin" MitigationSeverityID="0"
   Vendor="MICROSOFT" Supported="Yes" ImpactSeverityID="0" SchemaVersion="1.0" PreReqSeverityID="0"
   DateRevised="20030120" Source="MICROSOFT" Name="MS03-001" Title="Unchecked Buffer in Locator
   Service Could Lead to Code Execution (810833)" DatePosted="20030120" Platform="winnt">
  - <Products>
    - <Product Name="Windows 2000 Advanced Server" FixedInRelease="Windows 2000 Service Pack 4">
      - <Releases>
        - <Release Name="Windows 2000 Service Pack 2">
          + <Patch VerifyCmdline=""
               PatchURL="http://download.windowsupdate.com/msdownload/update/v3-
               19990518/cabpool/Q810833_W2K_SP4_7BCAD659FA326D4979A3CE9034300EA83A30F5EC.EXE"
               Architecture="" Reboot="Y" InstallCmdline="-q /Z" Language="en"
               MSSUSName="com_microsoft.810833_W2K_SP4_5936" SupercededByBulletin=""
               SupercededByMSPatch="" OSVersion=""
               MSSecureName="Q810833_W2K_SP4_X86_EN.exe" ObjectType="winnt.patch"
               QNumber="810833" ProbeCmdline="" Superceded="N" OSType="" OSSuite=""
               Platform="winnt" UninstallCmdline="">
```

Figure 19 View a sample patch descriptor file.

Bulletin Node

Node name: Bulletin

Parent node: None

Children: Products

Table 8: 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`

Table 8: XML Tags in the BULLETIN class

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`

Table 8: XML Tags in the BULLETIN class

XML Tag	Radia Attribute	Description
DatePosted	POSTED	Bulletin Posted On Date the bulletin was posted in YYYYMMDD format. Source: `MSSECURE.XML`
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 9: 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 10: 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 11: 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`

Table 11: XML Tags in the PATCH class

XML Tag	Radia Attribute	Description
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`
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,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.

Table 11: XML Tags in the PATCH class

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`

Table 11: XML Tags in the PATCH class

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 12: 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`

Table 12: XML Tags in the FILECHG class

XML Tag	Radia Attribute	Description
Size	SIZE	The size of the file. Source: `MSSECURE.XML`
Checksum	CHECKSUM	The checksum of the file. Source: `MSSECURE.XML`
Version	VERSION	The version of the file. Source: `MSSECURE.XML`
	DSTATE	The desired state of the FILECHG instance, this is usually classed in from another instance in the 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 13: XML Tags in the REGCHG class

XML Tag	Radia Attribute	Description
Name	NAME	Value Name. Source: `MSSECURE.XML`
Path	PATH	The fully qualified Registry Key Name. Source: `MSSECURE.XML`
Value	VALUE	The Data value stored in the registry. Source: `MSSECURE.XML`

Type	TYPE	Registry data type should be one of the following:
		sz = Simple Registry String
		multi_sz = Registry Multi String
		expand_sz = Registry string with environment variables
		dword = Registry dword
		binary = Binary data
		Source: `MSSECURE.XML`

	DSTATE	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

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. The table Reboot Events and Codes 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 Radia Patch Manager.

Table 14: 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.

Table 14: Reboot Events and Codes

Application Events	Code	Description
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

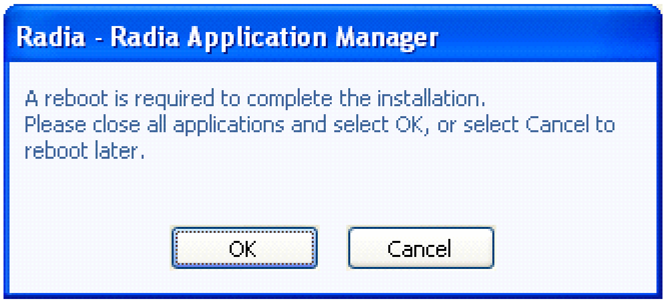
You can specify the type of warning message you want to send to the subscriber before the restart occurs. If you specify a type of reboot, but do not specify a type of warning message, the default warning message for that type will be displayed. There are three types of warning messages. Warning messages are displayed automatically for the Radia Software Manager and for Radia 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.

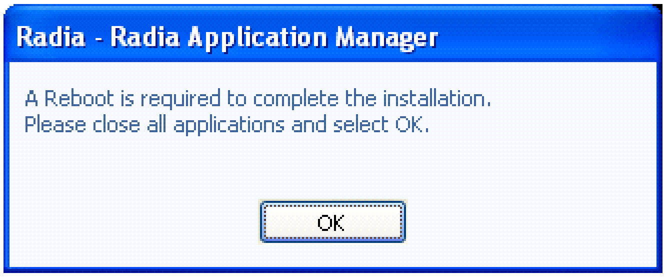


Radia - Radia Application Manager

A reboot is required to complete the installation.
Please close all applications and select OK, or select Cancel to reboot later.

Figure 20 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.



Radia - Radia Application Manager

A Reboot is required to complete the installation.
Please close all applications and select OK.

Figure 21 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.

Radia 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 Radia Policy Server Integration

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

If you are using Radia Policy Server with Radia Patch Manager, you will want to separate resolution of regular software services from those for Radia Patch Manager. Radia Policy Server filters services based on the dname passed on the radskman command line. The Radia 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 Radia 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 Radia 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 }
```

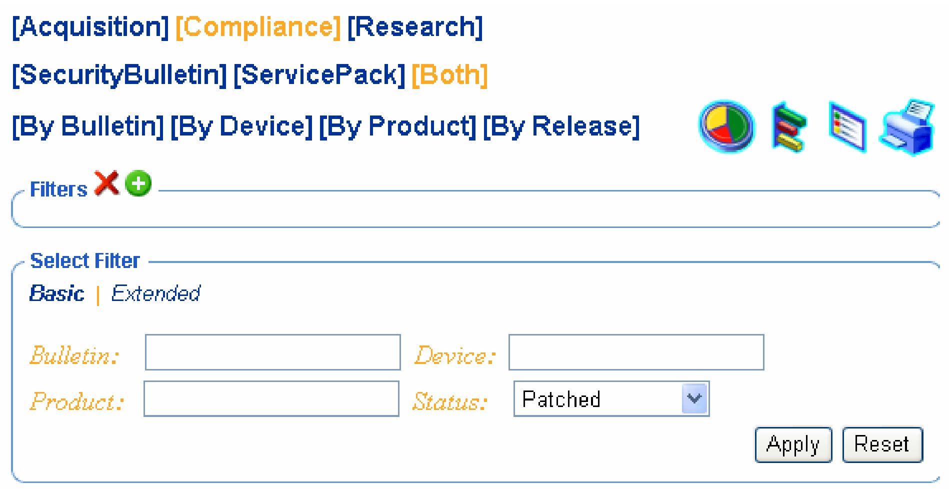
In this configuration the default rule (*) will ignore PATCHMGR and OS domains and allow everything else as denoted by the use of "!". PATCH and OS rules allow only policies for PATCH and OS domains respectively. If for instance, we wanted to allow any policies for OS manager resolution we would change the last filter to: `DNAME=OS   { * }`.

D Radia Patch Manager Reports

If you are not using the Radia Reporting Server, these are the reports that you will see. These reports have a more limited functionality than those for the Radia Reporting Server.

Radia Patch Manager provides web-base reports to analyze the patches. To view the reports, type `http://<patchserveripaddress>:<port>` in any web browser. From the Radia Integration Server page, click **PATCH**. The Compliance filter screen will display.

The Java Virtual Machine (JVM) needs to be installed on the computer that you are using to view Radia Patch Manager reports. As of this printing, you will need to install the Java virtual machine on Windows 2003 Server, when using Internet Explorer. In addition, you should be aware that Microsoft has extended an End of Support for JVM and that in some cases, installing a service pack may remove its support from Internet Explorer.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters
Select Filter
Basic | Extended
Bulletin:
Device:
Product:
Apply
Reset

Status: Patched

The Radia Patch Manager reports allow you to quickly access information for each patch available. Reports are divided into separate sections:

- **Acquisition**
  Use this report to check on the status of a patch acquisition session. See Patch Acquisition Reports on page 81.
- **Compliance**
  Use these reports to examine the vulnerabilities of devices in your enterprise.
- **Research**
  Use these reports to learn about the patches, bulletins, and files.

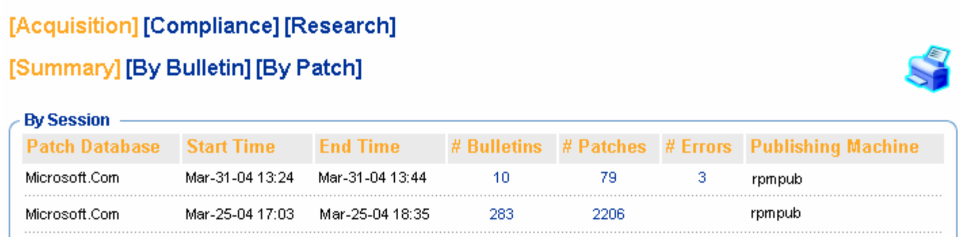
A "New" or "Updated" indicator marks any Bulletins that have been posted or updated by Microsoft within a 14-day period. To change the number of days, set ALERT_DAYS in the `Patch.cfg` to number of days. Set ALERT_DAYS to 0 to prevent the indicator from appearing.

The date and time stamps for Radia Patch Manager are stored in Greenwich Mean Time (GMT) on the SQL Server. The date and time stamps display in the reports based on the time zone where the Radia Patch Manager is located.

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, type **`http://<patchserveripaddress>:<port>`** in any web browser. From the Radia Integration Server page, click **PATCH**. Then click **Acquisition** to go to the Acquisition Reports.

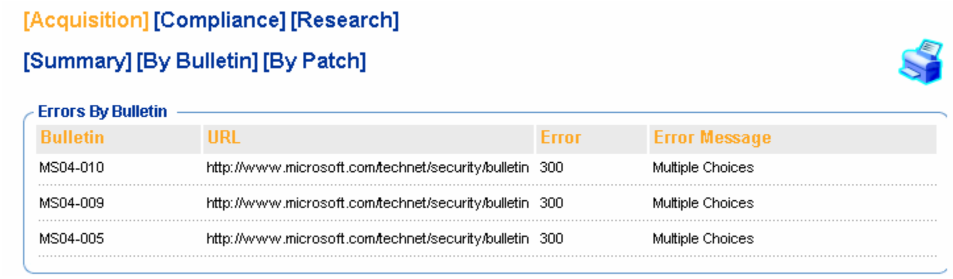
The Acquisition Summary by Session report shows the number of bulletins, patches, and errors for each acquisition session. In addition, it provides links to the vendor's patch web site and a link to the acquisition reports for all bulletins and patches. The date and time of the publishing session is also listed.


[Acquisition] [Compliance] [Research]
[Summary] [By Bulletin] [By Patch]
By Session

Patch Database	Start Time	End Time	# Bulletins	# Patches	# Errors	Publishing Machine
Microsoft.Com	Mar-31-04 13:24	Mar-31-04 13:44	10	79	3	rpmpub
Microsoft.Com	Mar-25-04 17:03	Mar-25-04 18:35	283	2206		rpmpub

Click on the number of Bulletins to see acquisition summary sorted by bulletin or Patches to see the acquisition summary sorted by patch files.

Click on **Errors** to see further explanations of why the acquisition failed.



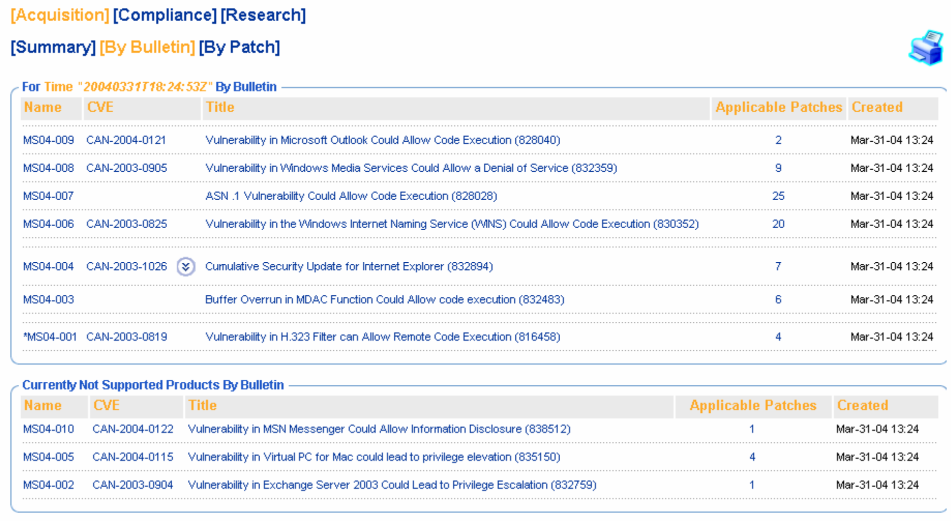
[Acquisition] [Compliance] [Research]

[Summary] [By Bulletin] [By Patch]

Errors By Bulletin

Bulletin	URL	Error	Error Message
MS04-010	http://www.microsoft.com/technet/security/bulletin	300	Multiple Choices
MS04-009	http://www.microsoft.com/technet/security/bulletin	300	Multiple Choices
MS04-005	http://www.microsoft.com/technet/security/bulletin	300	Multiple Choices

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



[Acquisition] [Compliance] [Research]

[Summary] [By Bulletin] [By Patch]

For Time "20040331T18:24:53Z" By Bulletin

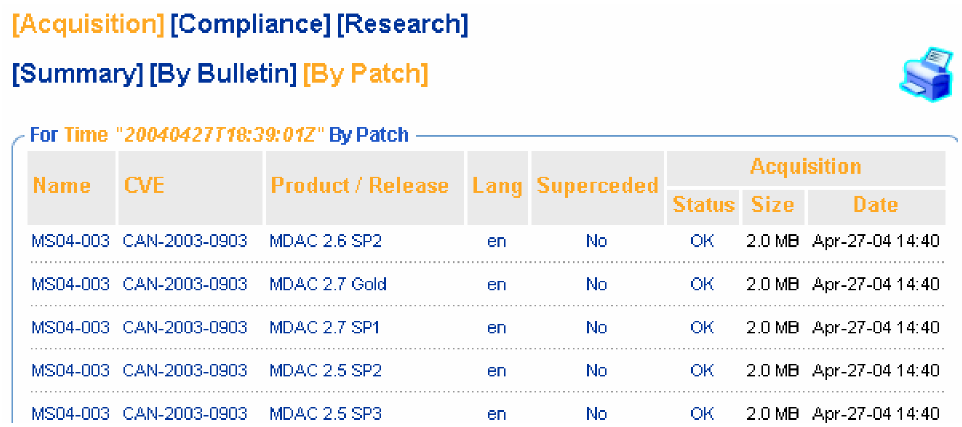
Name	CVE	Title	Applicable Patches	Created
MS04-009	CAN-2004-0121	Vulnerability in Microsoft Outlook Could Allow Code Execution (828040)	2	Mar-31-04 13:24
MS04-008	CAN-2003-0905	Vulnerability in Windows Media Services Could Allow a Denial of Service (832359)	9	Mar-31-04 13:24
MS04-007		ASN .1 Vulnerability Could Allow Code Execution (828028)	25	Mar-31-04 13:24
MS04-006	CAN-2003-0825	Vulnerability in the Windows Internet Naming Service (WINS) Could Allow Code Execution (830352)	20	Mar-31-04 13:24
MS04-004	CAN-2003-1026	Cumulative Security Update for Internet Explorer (832894)	7	Mar-31-04 13:24
MS04-003		Buffer Overrun in MDAC Function Could Allow code execution (832483)	6	Mar-31-04 13:24
*MS04-001	CAN-2003-0819	Vulnerability in H.323 Filter can Allow Remote Code Execution (816458)	4	Mar-31-04 13:24

Currently Not Supported Products By Bulletin

Name	CVE	Title	Applicable Patches	Created
MS04-010	CAN-2004-0122	Vulnerability in MSN Messenger Could Allow Information Disclosure (838512)	1	Mar-31-04 13:24
MS04-005	CAN-2004-0115	Vulnerability in Virtual PC for Mac could lead to privilege elevation (835150)	4	Mar-31-04 13:24
MS04-002	CAN-2003-0904	Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (832759)	1	Mar-31-04 13:24

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 Radia Patch Manager does not support, an asterisk (*) will be displayed preceding the bulletin number. In the figure above, one of the files associated with MS04-001 is not currently supported by Radia 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 Radia Patch Manager. These bulletins will not appear in the Research reports.



[Acquisition] [Compliance] [Research]

[Summary] [By Bulletin] [By Patch]

For Time "20040427T18:39:01Z" By Patch

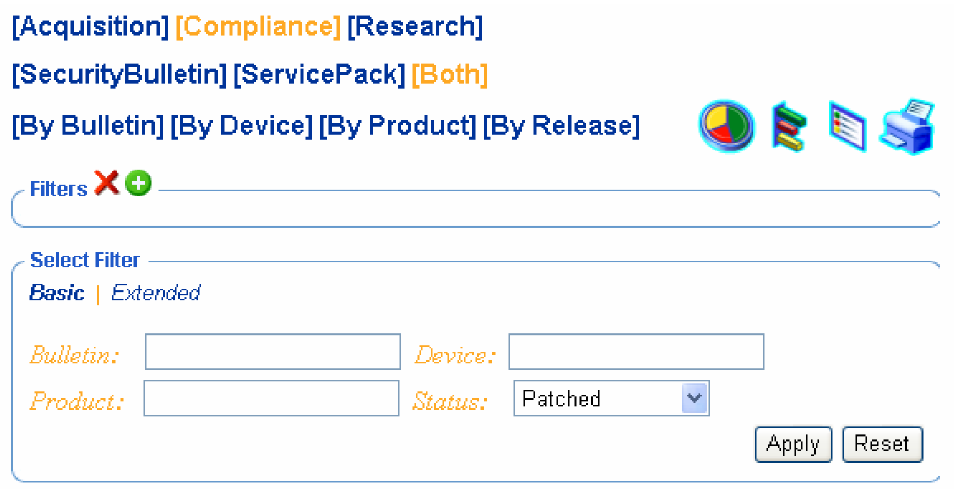
Name	CVE	Product / Release	Lang	Superceded	Acquisition		
					Status	Size	Date
MS04-003	CAN-2003-0903	MDAC 2.6 SP2	en	No	OK	2.0 MB	Apr-27-04 14:40
MS04-003	CAN-2003-0903	MDAC 2.7 Gold	en	No	OK	2.0 MB	Apr-27-04 14:40
MS04-003	CAN-2003-0903	MDAC 2.7 SP1	en	No	OK	2.0 MB	Apr-27-04 14:40
MS04-003	CAN-2003-0903	MDAC 2.5 SP2	en	No	OK	2.0 MB	Apr-27-04 14:40
MS04-003	CAN-2003-0903	MDAC 2.5 SP3	en	No	OK	2.0 MB	Apr-27-04 14:40

Possible acquisition statuses are:

- **Multiple Choices**
  The bulletin requires a choice before downloading a file.
- **OK**
  The patch file was successfully downloaded.
- **Not Downloaded**
  Either the acquisition was run with mode set to MODEL or the mode was set to BOTH but the patch was superceded.
- **Not Found**
  The actual patch file was requested, but Radia Patch Manager was unable to download it. In this case, you can download the file manually, and create a custom xml file to correct download URL locations.

Compliance Reports

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


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters
Select Filter
Basic | Extended
Apply
Reset

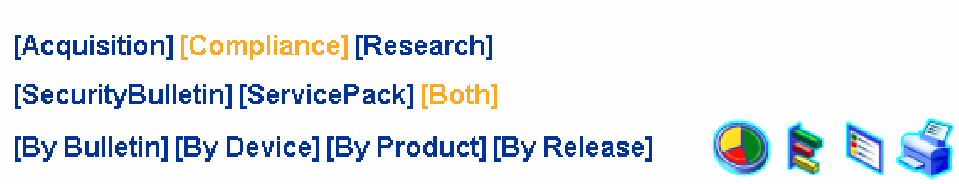
Bulletin:

Device:

Product:

Status: Patched

For all of the Compliance Reports, a navigation bar is provided at the top of the report to easily view by bulletin, device, product, or release. You can also select to view by Security Bulletins, Service Packs, or both at the same time. Use the navigation bar to maintain your current filter and browse by a different category. If you click on Filter bar's X, the filter will be cleared. Click the bar or pie chart button to toggle between the two types of charts where applicable. The detail button gives you a list view. Click the printer button to get a printer friendly format of the report. You can build filters for Compliance reports using either basic or extended methods.

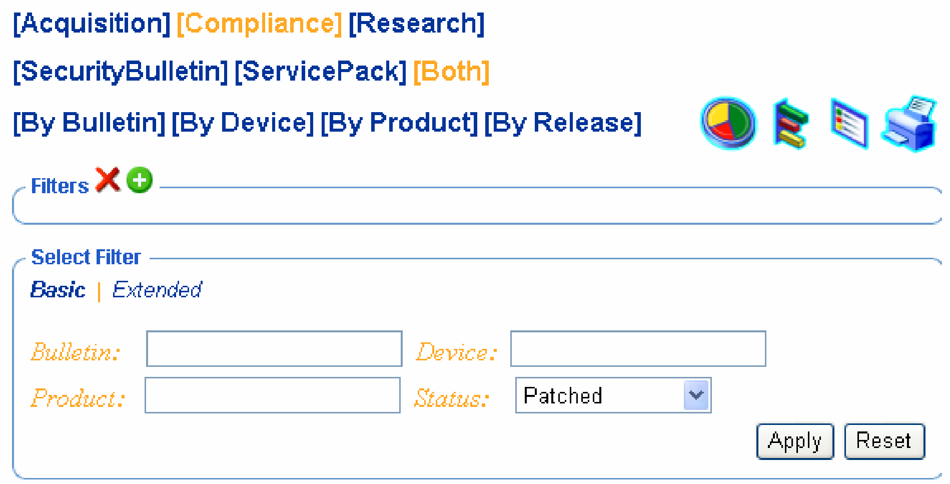

[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]

Use the asterisk (*) to represent any characters for any number of characters. Use "!" to represent a not condition.

To create a Compliance filter

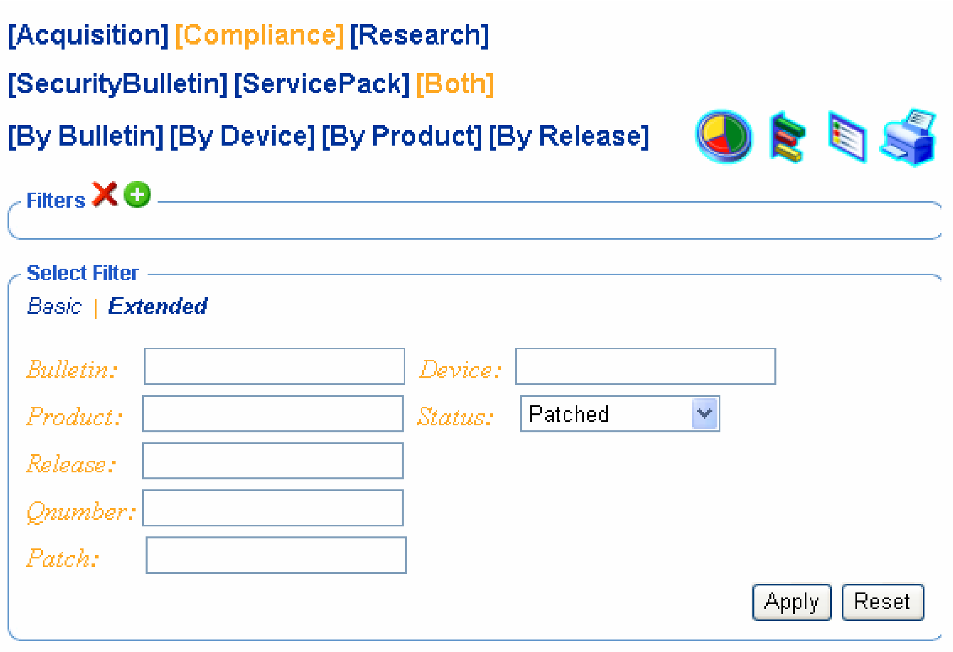
1 From any Compliance report, click the plus sign to create a filter.

2 Click **Basic** if you want to create a filter based on only a Bulletin, Product, Device or Status.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters
Select Filter
Basic | Extended
Bulletin:
Device:
Product:
Apply
Reset

Status: Patched

Click **Extended** if you want to create a filter based on Bulletin, Product, Release, Qnumber, Patch, Device or Status.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters
Select Filter
Basic | Extended
Bulletin:
Device:
Product:
Release:
Qnumber:
Patch:
Apply
Reset

Status: Patched

3 Click **Apply** to apply the filters.

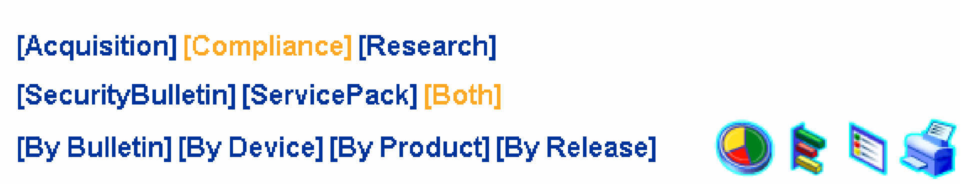
Click **Reset** to remove any text you have typed into the filter fields.

The filter is applied and the filter you used is shown in the Filter bar.

To remove a filter, click the X in the Filter bar.

There are Compliance views for Bulletins and Service Packs or both. Under these three views you can see compliance reports by bulletin, device, product, or release.

- **Compliance by Security Bulletin, Service Pack, or Both**
  Use this navigation bar to see the vulnerabilities by Security Bulletin, Service Pack, or Both. Each row contains information relating to a specific bulletin or service pack and an icon.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]

- **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.

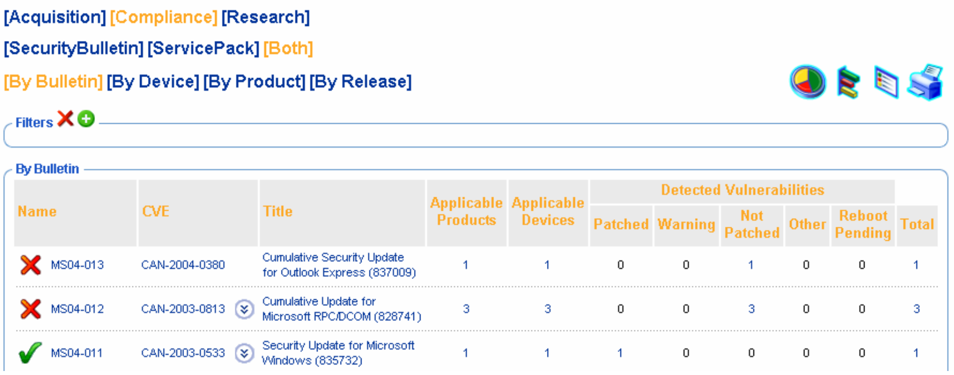
  — A power button indicates that at least one device is pending a reboot to be in compliance.

  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.



[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters
By Bulletin

Name	CVE	Title	Applicable Products	Applicable Devices	Detected Vulnerabilities					
					Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗ MS04-013	CAN-2004-0380	Cumulative Security Update for Outlook Express (837009)	1	1	0	0	1	0	0	1
✗ MS04-012	CAN-2003-0813	Cumulative Update for Microsoft RPC/DCOM (828741)	3	3	0	0	3	0	0	3
✓ MS04-011	CAN-2003-0533	Security Update for Microsoft Windows (835732)	1	1	1	0	0	0	0	1

For each bulletin, you can

- Click the name of the bulletin in the Name column to go to the vendor's web site for more information on the bulletin.
- Click the CVE number in the CVE column to go the Common Vulnerabilities and Exposures web site.
- Click the title in the Title column to see all patches for the 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 all patches for that bulletin.
- Click the number in the Warning column to see vulnerabilities that the Radia 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 Radia Patch Manager cannot report the vulnerability as being patched, this would be reported as a warning.

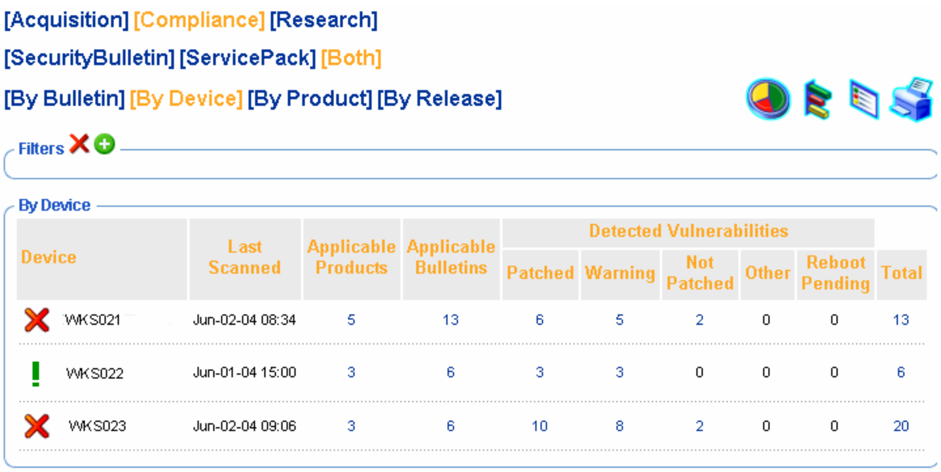
  Another example may be that a file version on the device is newer than the one delivered by the patch. Again, in this case, Radia Patch Manager cannot report the vulnerability as being patched so it reports a warning.

  - 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 Radia Patch Manager was not able to verify.
  - Items in the Reboot Pending column represents 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 at least one vulnerability could not be confirmed.
  - A red X indicates at least one vulnerability is not patched for this device.
  - An exclamation mark indicates a warning.



[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters ✗ ⊕
By Device

Device	Last Scanned	Applicable Products	Applicable Bulletins	Detected Vulnerabilities					Total
				Patched	Warning	Not Patched	Other	Reboot Pending	
✗ WKS021	Jun-02-04 08:34	5	13	6	5	2	0	0	13
! WKS022	Jun-01-04 15:00	3	6	3	3	0	0	0	6
✗ WKS023	Jun-02-04 09:06	3	6	10	8	2	0	0	20

For each device, you can

- 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 Radia Patch Manager cannot confirm as patched because there may be some discrepancy in the patch verification process.

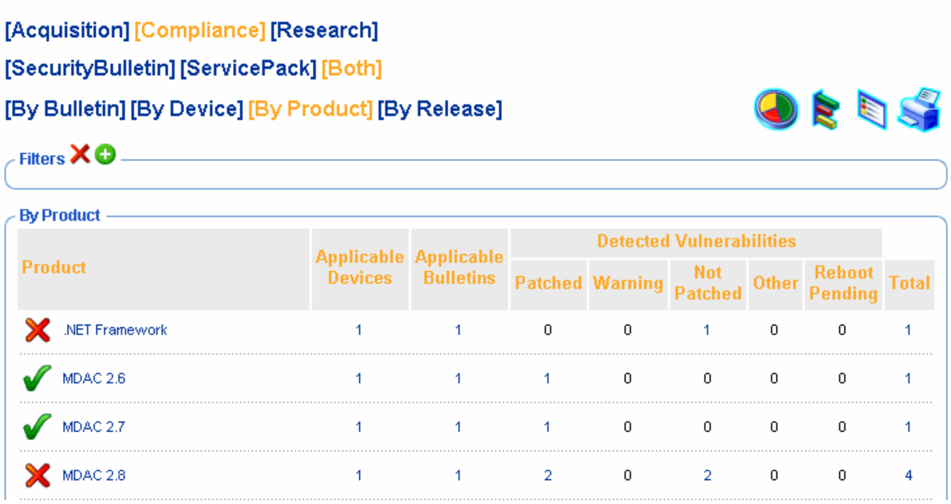
  For example, a patch for Microsoft SQL server or Microsoft MSDE may show up as a warning. MSDE installs fewer files than SQL Server. A device with MSDE may qualify for the same patch as a device with SQL server, but does not require all the files in the patch. Since Radia Patch Manager cannot report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

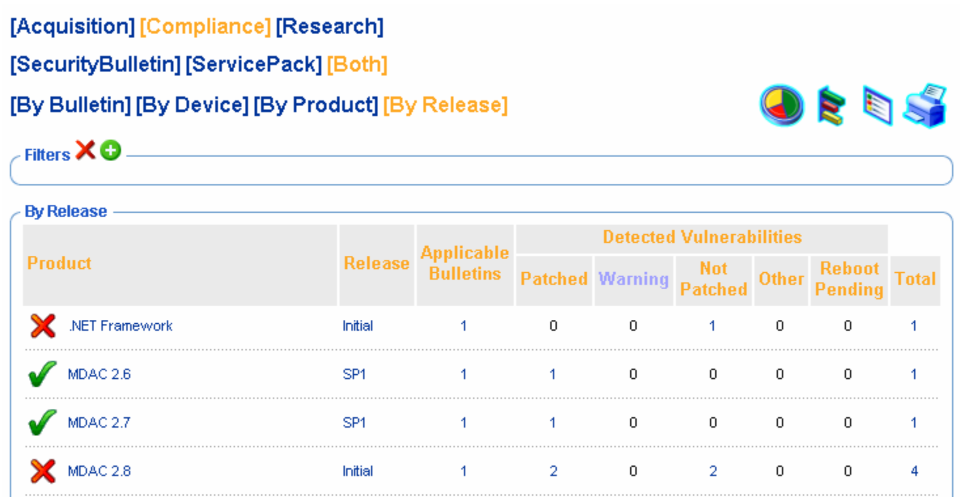
- **Compliance by Product**
  This report displays one row for each product. For each product, you can
  - Click the number in the Applicable Devices column to see the devices affected by the vulnerability.
  - Click the number in the Applicable Bulletins column to see bulletins for the product.
  - View detected vulnerabilities.



[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Product] [By Release]
Filters ✗ ⊕
By Product

Product	Applicable Devices	Applicable Bulletins	Detected Vulnerabilities					
			Patched	Warning	Not Patched	Other	Reboot Pending	Total
✗ .NET Framework	1	1	0	0	1	0	0	1
✓ MDAC 2.6	1	1	1	0	0	0	0	1
✓ MDAC 2.7	1	1	1	0	0	0	0	1
✗ MDAC 2.8	1	1	2	0	2	0	0	4

- **Compliance by Release**
  This report lists products by release. There is one row for each release of each product. Click to see **Applicable Bulletins** and **Detected Vulnerabilities** by status.



[Acquisition] [Compliance] [Research]

[SecurityBulletin] [ServicePack] [Both]

[By Bulletin] [By Device] [By Product] [By Release]

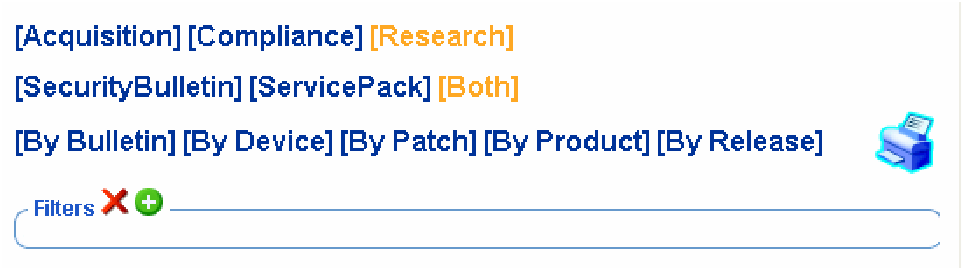
Filters ✗ ⊕

By Release

Product	Release	Applicable Bulletins	Detected Vulnerabilities					Total
			Patched	Warning	Not Patched	Other	Reboot Pending	
✗ .NET Framework	Initial	1	0	0	1	0	0	1
✓ MDAC 2.6	SP1	1	1	0	0	0	0	1
✓ MDAC 2.7	SP1	1	1	0	0	0	0	1
✗ MDAC 2.8	Initial	1	2	0	2	0	0	4

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. You can build filters for Research reports using either basic or extended methods.



[Acquisition] [Compliance] [Research]

[SecurityBulletin] [ServicePack] [Both]

[By Bulletin] [By Device] [By Patch] [By Product] [By Release]

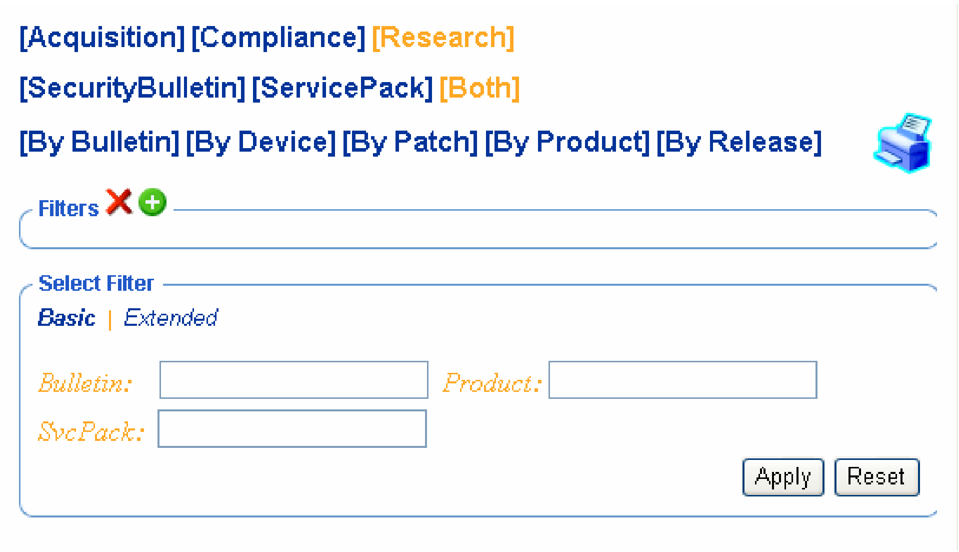
Filters ✗ ⊕

Use the asterisk (*) to represent any characters for any number of characters. Use "!" to represent a not condition.

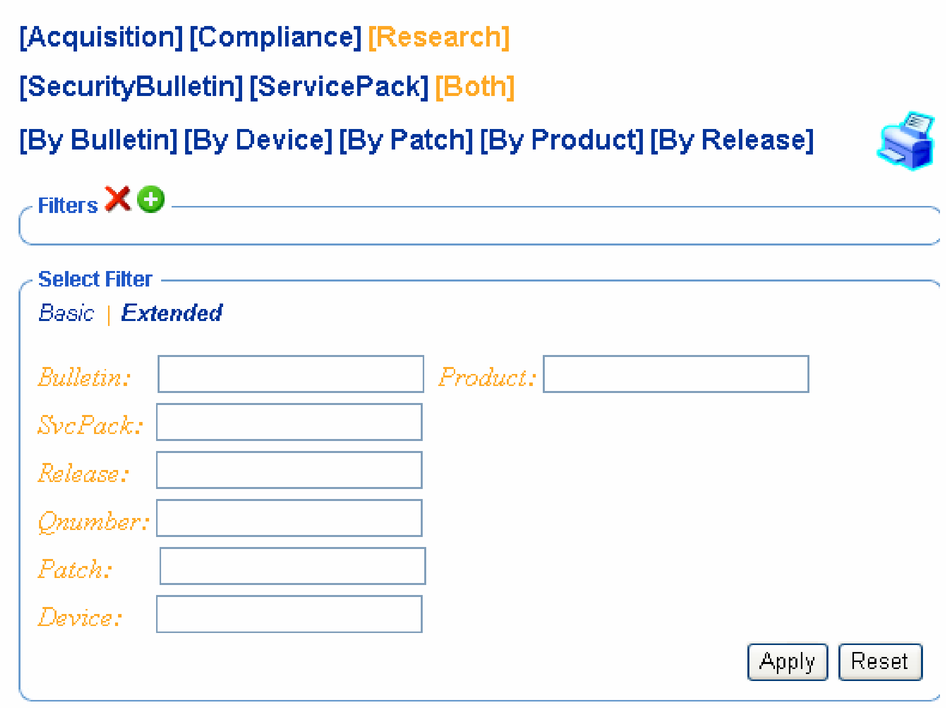
To create a Research filter

1 From any Research report, click the plus sign to create a filter.

2 Click **Basic** if you want to create a filter based on only a Bulletin, Service Pack, or Product.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]
Filters
Select Filter
Basic | Extended
Bulletin:
Product:
SvcPack:
Apply
Reset

Click **Extended** if you want to create a filter based on Bulletin, Service Pack, Release, Qnumber, Patch, Device, or Product.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]
Filters
Select Filter
Basic | Extended
Bulletin:
Product:
SvcPack:
Release:
Qnumber:
Patch:
Device:
Apply
Reset

3. Click **Apply** to apply the filters.

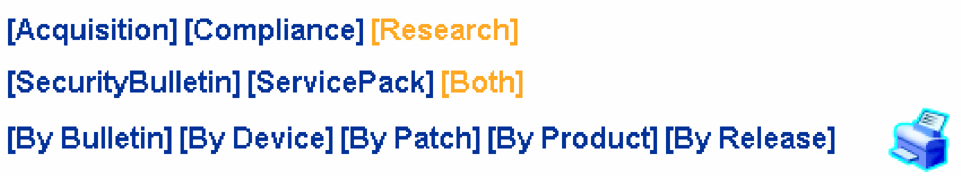
   Click **Reset** to remove any text you have typed into the filter fields.

4. The filter is applied and the filter you used is shown in the Filter bar.

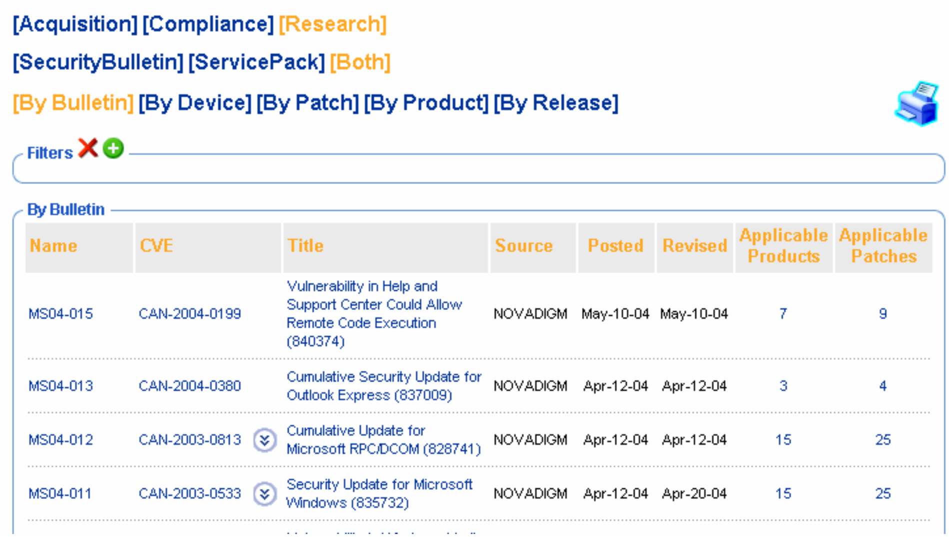
If you want to remove a filter, click the X in the Filter bar.

There are Research views for Bulletins and Service Packs or both. Under these three views you can see research reports by Device, Patch, Product, or Release.

- **Research by Bulletin, Service Pack, or Both**
  Use this to view all security bulletins, service packs, or both sorted by the bulletin number.


[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]

- **Research by Bulletin**
  Use this report to drill down to all bulletins. Click on the bulletin's number (Name) to go to the vendor's web site for more information. Click on the CVE (Common Vulnerability Exposure) number to go to the Common Vulnerability Exposures web site. Click **Title** or **Applicable Patches** 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 **Applicable Products** to see which products are influenced by this bulletin.



[Acquisition] [Compliance] [Research]

[SecurityBulletin] [ServicePack] [Both]

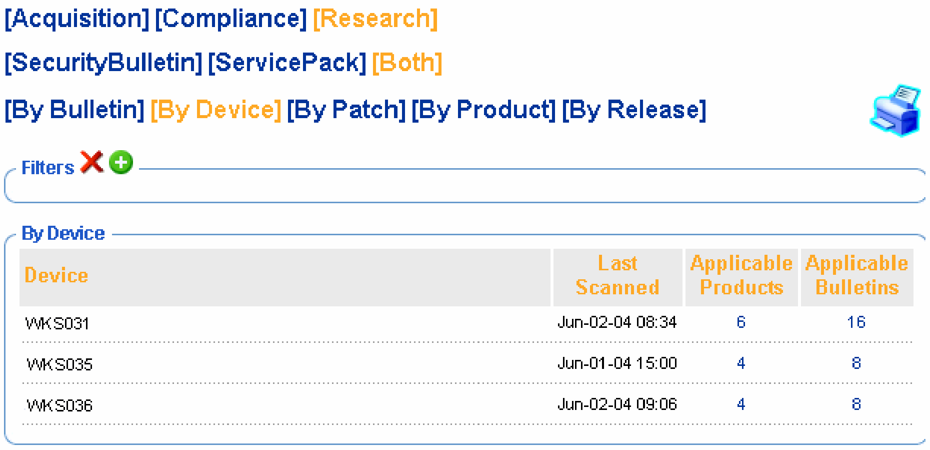
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]

Filters ✕ ⊕

By Bulletin

Name	CVE	Title	Source	Posted	Revised	Applicable Products	Applicable Patches
MS04-015	CAN-2004-0199	Vulnerability in Help and Support Center Could Allow Remote Code Execution (840374)	NOVADIGM	May-10-04	May-10-04	7	9
MS04-013	CAN-2004-0380	Cumulative Security Update for Outlook Express (837009)	NOVADIGM	Apr-12-04	Apr-12-04	3	4
MS04-012	CAN-2003-0813	Cumulative Update for Microsoft RPC/DCOM (828741)	NOVADIGM	Apr-12-04	Apr-12-04	15	25
MS04-011	CAN-2003-0533	Security Update for Microsoft Windows (835732)	NOVADIGM	Apr-12-04	Apr-20-04	15	25

- **Research by Device**
  Use this report to drill down to all bulletins filtered by a particular device. For example, to see all the applicable bulletins for WKS001, click on **WKS001**. Click **Applicable Products** to see the discovered products on the device.



[Acquisition] [Compliance] [Research]

[SecurityBulletin] [ServicePack] [Both]

[By Bulletin] [By Device] [By Patch] [By Product] [By Release]

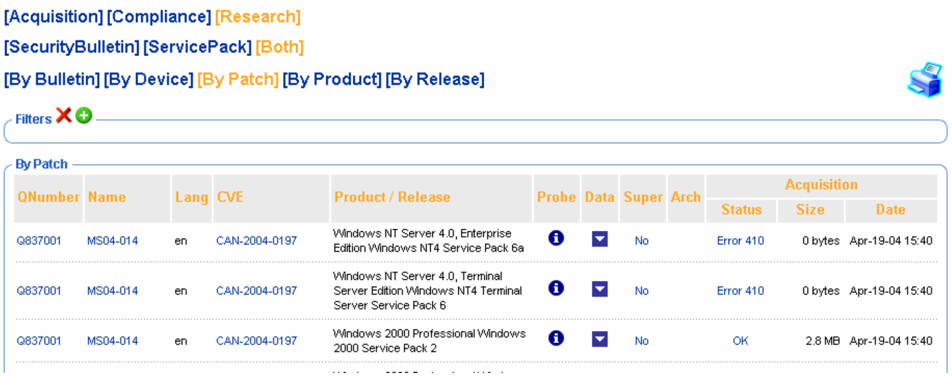
Filters ✕ ⊕

By Device

Device	Last Scanned	Applicable Products	Applicable Bulletins
WKS031	Jun-02-04 08:34	6	16
WKS035	Jun-01-04 15:00	4	8
WKS036	Jun-02-04 09:06	4	8

- **Research by Patch**
  Use this report to view information on patch files including on acquisition status. Click on the CVE (Common Vulnerability Exposure) number to

go to the Common Vulnerability Exposures web site. Click the **Data** column to download the patch file.



[Acquisition] [Compliance] [Research]

[SecurityBulletin] [ServicePack] [Both]

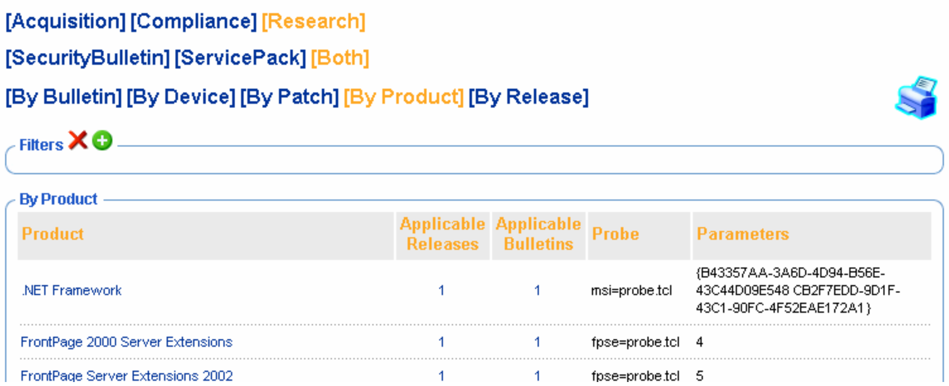
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]

Filters

By Patch

QNumber	Name	Lang	CVE	Product / Release	Probe	Data	Super	Arch	Acquisition		
									Status	Size	Date
Q837001	MS04-014	en	CAN-2004-0197	Windows NT Server 4.0, Enterprise Edition Windows NT4 Service Pack 6a	ℹ	▼	No		Error 410	0 bytes	Apr-19-04 15:40
Q837001	MS04-014	en	CAN-2004-0197	Windows NT Server 4.0, Terminal Server Edition Windows NT4 Terminal Server Service Pack 6	ℹ	▼	No		Error 410	0 bytes	Apr-19-04 15:40
Q837001	MS04-014	en	CAN-2004-0197	Windows 2000 Professional Windows 2000 Service Pack 2	ℹ	▼	No		OK	2.8 MB	Apr-19-04 15:40

- **Research by Product**
  Use this report to drill down to all bulletins filtered by product. For example, to see all the bulletins for FrontPage 2000 Service Extensions, click **FrontPage 2000 Server Extensions.**



[Acquisition] [Compliance] [Research]

[SecurityBulletin] [ServicePack] [Both]

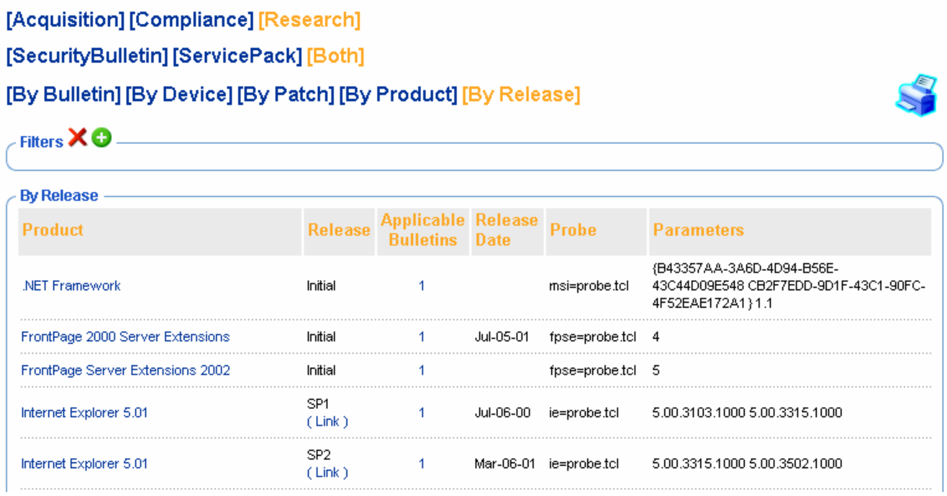
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]

Filters

By Product

Product	Applicable Releases	Applicable Bulletins	Probe	Parameters
.NET Framework	1	1	msi=probe.tcl	{B43357AA-3A6D-4D94-B56E-43C44D09E548 CB2F7EDD-9D1F-43C1-90FC-4F52EAE172A1}
FrontPage 2000 Server Extensions	1	1	fpse=probe.tcl	4
FrontPage Server Extensions 2002	1	1	fpse=probe.tcl	5

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



[Acquisition] [Compliance] [Research]
[SecurityBulletin] [ServicePack] [Both]
[By Bulletin] [By Device] [By Patch] [By Product] [By Release]
Filters

By Release

Product	Release	Applicable Bulletins	Release Date	Probe	Parameters
.NET Framework	Initial	1		msi=probe.tcl	{B43357AA-3A6D-4D94-B56E-43C44D09E548 CB2F7EDD-9D1F-43C1-90FC-4F52EAE172A1 } 1.1
FrontPage 2000 Server Extensions	Initial	1	Jul-05-01	fpse=probe.tcl	4
FrontPage Server Extensions 2002	Initial	1		fpse=probe.tcl	5
Internet Explorer 5.01	SP1 (Link)	1	Jul-06-00	ie=probe.tcl	5.00.3103.1000 5.00.3315.1000
Internet Explorer 5.01	SP2 (Link)	1	Mar-06-01	ie=probe.tcl	5.00.3315.1000 5.00.3502.1000

Index