

Radia Client Automation Enterprise Patch Management

For the Windows® and Linux operating systems

Software Version: 9.00

Reference Guide

Document Release Date: April 2013

Software Release Date: April 2013



Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Persistent Systems shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Persistent Systems or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Persistent Systems.

Copyright Notice

© Copyright 2013 Persistent Systems, its licensors, and Hewlett-Packard Development Company, LP.

Trademark Notices

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

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written by Daniel Stenberg (daniel@haxx.se).

This product includes OVAL language maintained by The MITRE Corporation (oval@mitre.org).

Documentation Updates

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<http://support.persistentsys.com/>

This site requires that you register for a Persistent Passport and sign in. Register online at the above address.

For more details, contact your Persistent sales representative.

Support

Persistent Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Submit enhancement requests online
- Download software patches
- Look up Persistent support contacts
- Enter into discussions with other software customers
- Research and register for software training

To access the Self-solve knowledge base, visit the [Persistent Support](#) home page.

Note: Most of the support areas require that you register as a Persistent Support user and sign in. Many also require an active support contract. More information about support access levels can be found on the [Persistent Support](#) site.

To register for a Persistent Support ID, go to: [Persistent Support Registration](#).

Contents

Reference Guide	1
Contents	5
Introduction	9
Patch Management Overview	9
Abbreviations and Variables	10
Terminology	11
Patch Acquisition	13
Patch Acquisition Overview	13
Patch Acquisition Process	13
About Patch Descriptor (XML) Files	14
Embedded Support for the new Microsoft Update Cata (wsusscrn2.cab)	15
Microsoft Update Catalog Requirements: Minimum OS and Service Pack Levels	15
Patch Management Vendor Settings for Microsoft Data Feeds	16
Microsoft Office and Microsoft Update Catalog	16
Windows Installer 3.1 Requirement	16
About Microsoft Automatic Updates	16
About Red Hat Patch Acquisition	18
Creating a Red Hat systemid file	18
Creating Custom Patch Descriptor Files	19
Setting the Manage Installed Bulletins (mib) Option	20
Patch Acquisition Reports	21
Acquisition Summary	21
Acquisition by Bulletin	22
Acquisition by Patch	22
Patch Assessment, Analysis and Reports	23
Product Discovery and Analysis	23
Detecting and Managing Microsoft Office Security Bulletins	24

Best Practices for Managing Microsoft Office Security Bulletins	24
Windows Installer 3.1 Requirement	25
Options for Updating Microsoft Office Products	25
When to use Patch Management to Deploy Microsoft Office Updates	25
Client Automation Management Features that are Disabled when using Patch Management	26
Microsoft Update Catalog Supports Office XP, Office 2003, and Office 2007	26
Microsoft Office Service Packs	27
About Patch Management and Microsoft Update Catalog	27
Enabling Microsoft Office Updates in Patch Management (Versions 3.0.2 and later) ...	28
About Patch Objects used for Device Compliance Reporting	29
Patch Analysis and Reports	30
Filtering Patch Reports with Reporting Server	30
Drilling Down to Detailed Information	31
Available Report Actions include Data Export Options	31
Executive Summaries	32
Overall Device Status	33
Device Status	33
Bulletin Status	33
Vendor Status	34
Patch Compliance Reports	34
Device Status	34
Devices Not Fully Patched	35
Devices Pending Reboot	36
Devices With Bulletin Install Errors	36
Bulletin Status	36
Product Status	37
Release Status	38
Patch Status	38
Devices with Serious Errors	38
Acquisition Reports	39
Research Reports	39

Research by Bulletin	39
Research by Devices	40
Research by Patches	40
Research by Products	40
Research by Releases	40
Compliance and Research Exception Reports	41
Managing Vulnerabilities	41
Instance Naming Convention for SuSE 10 and 11 Bulletins	42
For SuSE 10	42
For SuSE 11	43
Entitle the FINALIZE_PATCH Service	43
Deploying Automatic and Interactive Patches	44
Customizing Reporting Options	44
Disabling Vulnerability Detection and Deployment	46
Controlling Patch Deployment (PATCHARG)	46
Removing a Patch	47
Summary	48
Supported XML Tags for Patch	49
Descriptor Files	49
Bulletin Node	49
Products Node	50
Product Node	51
Releases Node	51
Release Node	51
Patch Node	51
Patch Signature Node	53
FileChg Node	53
RegChg Node	54
HPFileset Node	55
Restarting the Managed Device	57
Application Events	57
Reboot Types	58

Reboot Modifier: Type of Warning Message	58
Reboot Modifier: Machine and User Options	59
Reboot Modifier: Immediate Restart	59
Specifying Multiple Reboot Events	59
Patch.cfg Parameters	61
Patch Management Server Configuration Parameters	61
Patch Acquisition Parameters	65
Database Synchronization Parameters	68
Patch Agent Update Parameters	69
We appreciate your feedback!	71

Chapter 1

Introduction

Patch management enables you to discover, analyze, and deploy patches in your environment. Patch management enables you to acquire patches from vendor web sites, determine the vulnerabilities on the managed devices, deploy applicable patches to managed devices, verify applied patches on managed devices to ensure compliance and security, and generate reports that provide information on which acquired and applicable patches have or have not yet been applied to a managed device.

Note: Patch management enables you to manage security and non-security patches for Microsoft. You can also manage security patches RedHat, SUSE, and HP Softpaq. Patch management does not support Update Rollups as part of non-security patches.

Patch Management Overview

The Radia Client Automation Patch Management provides value for business continuity and security initiatives.

Key capabilities for patch management activities include:

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

Note: There is no support for the acquisition of security bulletins (advisories) for HP-UX and Sun Solaris (Sparc). RCA does not support managing HP-UX or Sun Solaris Agent devices.

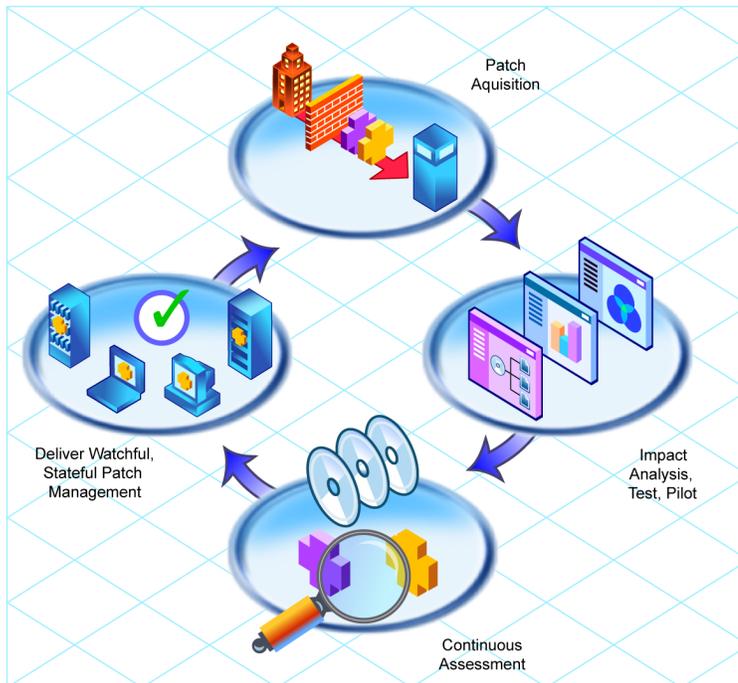
- **Pilot Testing:**
Ability to allow IT administrators to select target pilot groups based on usage or critical need. Radia Client Automation is the only solution with these unique pilot testing capabilities that help ensure the stability of business critical systems.
- **Compliance and Vulnerability Assessment:**
Automatic and continuous discovery of devices on the network, software products that are installed on each device, the patches that are already applied by each software product, and identification of applicable software products. Through this complete discovery and assessment process, the IT administrator can understand the full scope of security vulnerability and system compliance at all times.
- **Deployment:**
Policy-based deployment capabilities that interface directly with a variety of existing policy sources such as Active Directory, LDAP, or SQL databases to enable automatic, rapid, and precise targeting of patches for deployment to servers, desktops, and laptops. HP Client Automation patented differencing, bandwidth optimization, multicast, and checkpoint-restart

capabilities and multi-tiered infrastructure ensure that 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 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.

Patch Management Life Cycle



Abbreviations and Variables

Abbreviations Used in this Guide

Abbreviation	Definition
RCA	Radius Client Automation
Core and Satellite	RCA Enterprise environment consisting of one Core server and one or more Satellite servers.
CSDB	Configuration Server Database

Variables Used in this Guide

Variable	Description	Default Values
<i>InstallDir</i>	Location where the RCA server is installed	For a 32-bit OS: C:\Program Files\Hewlett-Packard\HPCA

Variable	Description	Default Values
		For a 64-bit OS: C:\Program Files (x86)\Hewlett-Packard\HPCA
<i>SystemDrive</i>	Drive label for the drive where the RCA server is installed	C:

Terminology

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

bulletin or security advisory

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

patch

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

Chapter 2

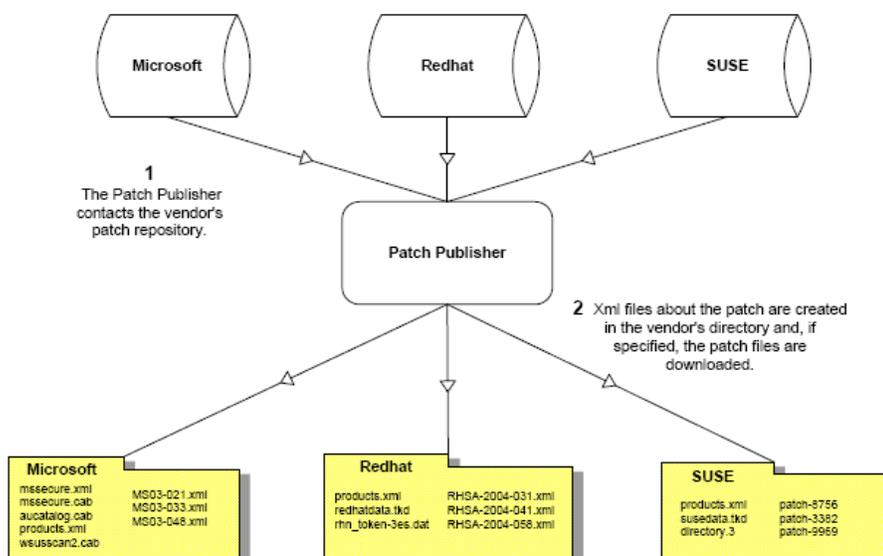
Patch Acquisition

This chapter describes the patch acquisition process and the patch descriptor files created for acquiring patches. This chapter also describes various acquisition-based reports that show the status of the acquisition process.

Patch Acquisition Overview

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

Vendor's patch repository is contacted



Patch Acquisition Process

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

During the acquisition, the following things occur:

- The vendor's web site is contacted to prepare for the acquisition.
- Either the information about the Bulletins, Security Advisories, and Service Packs and the actual patch files or only the information about the patches is downloaded. The information

downloaded contains, but is not limited to, detailed data about each patch, such as supersedence, reboot requirements, and probe information.

- An xml file is created for each bulletin acquired and is put in the vendor's folder in the Patch Management's directory. These files are called patch descriptor files.
- The Configuration Server Database's PATCHMGR Domain is populated with this information.
- Services are created in the PATCHMGR Domain for each of the bulletins acquired.
- The PATCHMGR Domain is synchronized with the ODBC database you created.

About Patch Descriptor (XML) Files

When 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:

```
<InstallDir>\data\PatchManager\patch
```

For example, patch descriptor files for Microsoft bulletins would be in:

```
<InstallDir>\data\PatchManager\patch\Microsoft
```

while those for Red Hat are located in:

```
<InstallDir>\data\PatchManager\patch\Redhat.
```

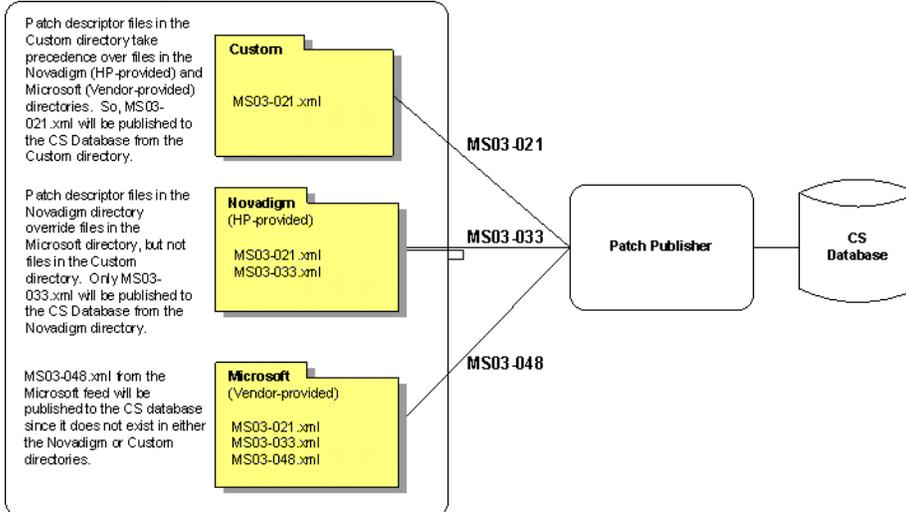
The bulletin number is the file name with an `.xml` extension. If the bulletin is identified by MS03-051, then the patch descriptor will be named `MS03-051.xml`. If you also acquired the actual files associated with the bulletin, a folder is created with the name of the bulletin that contains the patch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

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

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

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

Patch descriptor files



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

Microsoft recently introduced a new Microsoft Update Catalog, (*wsusscn2.cab*) as a centralized repository for all of their currently supported patches. As of this writing: Microsoft has stated patches for new Microsoft Products will only be available through the new Microsoft Update repository.

Presently, Patch Management supports the new Microsoft Update Catalog, as well as an existing Legacy Catalog.

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

Microsoft Update Catalog Requirements: Minimum OS and Service Pack Levels

See Microsoft's website for specific information concerning the minimum Operating System and Service Pack requirements for Microsoft Update Catalog and Windows Update technologies leveraged by Patch Management. As of this writing, the supported OS Versions and languages can be viewed from the Microsoft Update Home page at this link:

<http://update.microsoft.com/microsoftupdate/v6/default.aspx>

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

Customers can continue to patch older operating systems without enforcing the minimum service pack levels required by Microsoft Update Catalog.

Patch Management Vendor Settings for Microsoft Data Feeds

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

- **Microsoft Update Catalog Only**
- **Microsoft Update Catalog, Legacy Catalog**

Microsoft Office and Microsoft Update Catalog

Office patches deployed via the Microsoft Update Catalog will not detect if Office Applications are currently being managed by an Radia Client Automation management application (for example, Application Manager or Application Self-service Manager), or an Administrative Control Point. In either case, if a bulletin affecting an Office application is entitled to a device, Patch Management will manage the Office patch and install it locally onto those devices that are vulnerable. For more information on patching devices with Microsoft Office, see "Detecting and Managing Microsoft Office Security Bulletins" on page 24.

Windows Installer 3.1 Requirement

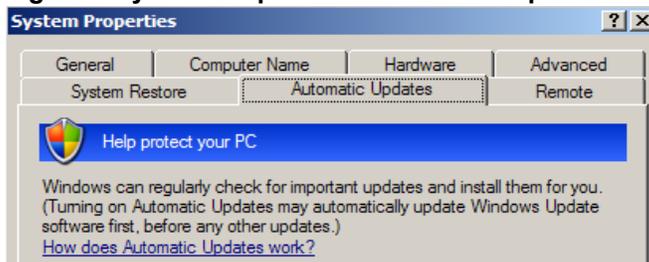
When running Patch Management, Windows Installer Version 3.1 *or above is* required on all target devices. To meet this MSI 3.1 requirement, it is recommended that customers either:

- Deploy the latest MSI 3.1 package manually by downloading it from the Microsoft website. This bulletin is defined for multiple languages. As of this writing, the US-English version is at <http://support.microsoft.com/kb/893803/en-us>, or
- Use Patch Management to acquire, distribute and manage the bulletin MS-KB893803. Specify this bulletin as part of your acquisition list and entitle it to your Windows agent machines.

About Microsoft Automatic Updates

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

Figure 6 System Properties -- Automatic Updates tab



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

1. Download updates for me, but let me choose when to install them
2. Notify me but don't automatically download or install them
3. Turn off Automatic Updates

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

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

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

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

Please consult the following Microsoft KB Articles for more information:

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

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

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

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

For more information about the configuration of Automatic Updates. See the Microsoft article *How to configure and use Automatic Updates in Windows* which is at url <http://support.microsoft.com/kb/306525> at the time of writing.

About Red Hat Patch Acquisition

To acquire security patches for Red Hat:

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

Note: For example, to perform patch acquisitions for Red Hat Enterprise Server (ES) Version 4 on x86 systems only, you will need a Red Hat Network account with one Red Hat Network system entitlement. To perform patch acquisitions for Red Hat ES Version 4 on x86-64 systems, you will need an additional Red Hat Network system entitlement. To perform acquisitions for Red Hat Version 5 Servers, on both x86 and on x86-64 systems, you will need an additional two Red Hat Network system entitlements. To perform acquisitions for Red Hat Version 6 Servers, on both x86 and on x86-64 systems, you will need an additional two Red Hat Network system entitlements.

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

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

If a patch's prerequisite software is not found locally, then the package will be downloaded from the Red Hat Network. To decrease the time needed for acquisition, it is recommended 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 `rhnc_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.

Creating a Red Hat systemid file

To create a Red Hat systemid file:

1. Perform a root login to a Linux Server running the Red Hat OS for which you would like to automatically acquire security patches.
2. Execute the command `rhnclean` on the command line when logged into the system as root.
3. When prompted by the `rhnclean` tool to use an existing or new account, select existing and supply the Red Hat Network username and password you created on the Red Hat web site.
4. Enter a unique profile name for this computer such as the IP address or hostname, and exit the `rhnclean` tool without applying any patches to the system where you ran `rhnclean`. A file called `systemid` is created.
5. Copy the file `/etc/sysconfig/rhn/systemid` produced by the `rhnclean` tool to the `\PatchManager\etc` directory on your Patch Management Server.
6. Rename the file from `systemid` to one of the following `redhat-*.sid` filename conventions. They vary according to the hardware architecture:
 - For x86 systems, rename `systemid` to `redhat-version+release.sid`, where `version+release` represents one of the three combinations of Red Hat Version 4 followed directly by the Release (`as`, `es`, or `ws`), or, for Red Hat Version 5, `version+release` is either `5server` or `5client`, or, for Red Hat Version 6, `version+release` is either `6server` or `6client`.
For example, if the computer was running Red Hat Enterprise Server V 4, then rename the `systemid` file to `redhat-4es.sid`.
 - For x86_64 systems, rename `systemid` to `redhat-version+release-x86_64.sid`. This is the same naming convention as above, except it adds the architecture type of `-x86_64` to the filename, prior to the `.sid` extension.
For example, if an x86_64 computer was running Red Hat Enterprise Server V 4, then rename the `systemid` file to `redhat-4es-x86_64.sid`.

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

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

Creating Custom Patch Descriptor Files

The patch descriptor files that are created using the `acquire` command use the information from the vendor data feeds. These files may be missing information or contain incorrect information regarding the patch. A **probe** defines what is needed to be in compliance with the security issue that the patch fixes. You can create a custom patch descriptor files using supported XML tags. The custom descriptor file must be placed in the custom directory and be named identically to the file it will be overriding in the `microsoft`, `redhat`, `suse`, or `novadigm` directories. The following 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 `<InstallDir>\data\PatchManager\patch\microsoft` directory generated during an acquisition into the `<InstallDir>\data\PatchManager\patch\custom` directory.
2. Use a text or xml editor to view the patch descriptor file. Validate the data with the releases itemized in the URL located at the top of the xml. Change Source to Custom.


```
<Bulletin PopularitySeverityID="0"
URL="http://www.microsoft.com/technet/security/bulletin"
FAQURL="http://www.microsoft.com/technet/security/bulletin"
MitigationSeverityID="0" Supported="Yes" ImpactSeverityID="0"
SchemaVersion="1.0" PreReqSeverityID="0" DateRevised="20021119"
Source="NOVADIGM" Stays NOVADIGM, like the folder name Name="MS02-065"
Title="Buffer Overrun in Microsoft Data Access Components Could
Lead to Code Execution (Q329414)" DatePosted="20021119" >
```

Note: When generating a custom xml, it is recommended including all Product releases. This allows a managed device running any available releases of the product to be discovered.

3. Make any changes required to adjust the data, and save the custom patch descriptor file. Change the Source tag to Custom. This value is reflected in the BULLETIN instance's SOURCE attribute. Use the Patch Management in the RCA Console to publish the custom patch descriptor file. Be sure to set the Replace option to Yes if you wish to entirely replace the bulletin previously published to the Configuration Server.
4. You may view the `patch-acquire.log` to see where the publishing process obtained the xml from:


```
20100722 10:13:09 Info: Syncing bulletin
<InstallDir>/Data/PatchManager/patch/custom/MS10-001.xml
20100722 10:13:09 Info: Publishing bulletin MS10-001, 1 of 1
20100722 10:13:09 Info: Loading XML file
<InstallDir>/Data/PatchManager/patch/custom/MS10-001.xml
20100722 10:13:10 Info: Loading BULLETIN.MS10-001 from RCS
```

Setting the Manage Installed Bulletins (mib) Option

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

The -mib option is available for customers who want Patch Management to skip the processing of applicable bulletins already installed on target machines, and only process the bulletins not already installed on the machines. The

-mib option can take the following values:

-mib none

Manage Patch Management-installed bulletins only, and do not check the service library or binary

resources for alternatively installed bulletins. This is the default behavior since there is no impact on the client agent in terms of vulnerability or re-patching, and it offers greater performance.

`-mib hppm (or n)`

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

`-mib all (ory)`

Manage all installed bulletins, whether installed by Patch Management or an external source. This option is resource intensive.

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

To set the Manage Installed Bulletins (mib) Option:

Use the Agent Options page from the RCA Console to set the Manage Installed Bulletins (-mib) option. The Agent Options page is accessed from the Configuration tab, Patch Management Group.

Patch Acquisition Reports

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

To view the reports, under **Reporting Views**, click **Patch Management Reports** to expand the list of reports. Click **Acquisition Reports** to expand the list of available reports. For more information on using and filtering reports, see the *Radia Client Automation Enterprise Reporting Server Reference Guide*.

Acquisition Summary

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

- Click **# Bulletins Added** or **# Bulletins Updated** to see the acquisition summary sorted by bulletin.
- Click **# Patches Added** or **# Patches Updated** to see the acquisition summary sorted by patch files.
- Click **# Bulletin Dependencies** to see the acquisition summary sorted by dependency bulletins displayed under the "Bulletin Dependencies" report. The bulletin dependencies count will be shown only for the Redhat vendor, since bulletin dependencies are acquired and published only for this vendor. For the other vendors, the bulletin dependencies count will appear as zero.
- 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.

Note: This report *cannot* be filtered by Vendor name.

Acquisition by Bulletin

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

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

- If a bulletin has a patch that applies to a product that Patch Management does not support, an asterisk (*) will be displayed preceding the bulletin name.
- The icon in the Severity column indicates the severity for Windows bulletins. They ratings range from Critical, to Important, to Moderate, to Low. If the bulletin is not for a Windows platform, the Unknown icon is displayed. Click on the icon in the Severity column to see all bulletins with the same severity. Pre-existing bulletins do not have severity ratings. To view severity ratings for existing bulletins and patches, you must re-acquire them using the Force and Replace options.

Note: The severity rating displayed in this report may not match with the Microsoft Security Bulletin Summary Page in the case where the bulletin contains patches not supported by WSUS and where their severity is higher than that of the other patches within the same bulletin. This issue is caused by the fact that the severity rating for the bulletin is determined by the severity of the patches that it contains. If the bulletin contains legacy patches, which would not be supported by WSUS, those will be excluded when the severity rating is determined.

- At the bottom of this report, there is a second section that includes bulletins that apply to products that are not supported by Patch Management. These bulletins will not appear in the Research reports.

Acquisition by Patch

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

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

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

Chapter 3

Patch Assessment, Analysis and Reports

This chapter describes the process to discover which patches are installed on the managed devices in your environment and analyze these patches. This chapter also describes various patch analysis reports.

Product Discovery and Analysis

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

Note: Running the Patch Management agent connect requires that the `dname` parameter be set to `PATCH`. This will keep separate the resolution of services for the Patch Management agent from the resolution of services for the Application Manager agent.

To perform patch discovery:

1. Connect your managed device (e.g. `POLICY.USER.&(ZUSERID)`) directly to the `PRIMARY.PATCHMGR.ZSERVICE.DISCOVER_PATCH` service.
This service is prioritized to run as the first service on Patch Management agents. During a Patch Management Agent connect, this service deploys methods to the patch manager agents, and performs product discovery and vulnerability assessment.
2. Connect your managed device (e.g. `POLICY.USER.&(ZUSERID)`) directly to the `PRIMARY.PATCHMGR.ZSERVICE.FINALIZE_PATCH`.
During a Patch Management Agent connect, applicable patches are downloaded and queued for management by a Patch Management Service called `FINALIZE_PATCH`. This service is prioritized to run as the last service on Patch Management agents. This service is required to report real time patch compliance information.
Add the `FINALIZE_PATCH` service to the policy for all managed devices, in addition to any patch.

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

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

```
radskman ip=<ConfigurationServerIPAddress>,port=  
<ConfigurationServerport>,dname=patch,catexp=runmode:automatic
```


For additional information on creating a `radskman` command line, see the *Radia Client Automation Application Manager and Application Self-service Manager Reference Guide*.

Detecting and Managing Microsoft Office Security Bulletins

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

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

If you would like to begin using Patch Management to update Microsoft Office applications, you must discontinue using an ACP or a Client Automation management application for distributing updates to your Microsoft Office applications. You can continue to use an ACP or a Client Automation management application to deploy Microsoft Office applications; however, updates must be managed solely by Patch Management.

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

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

- ["Best Practices for Managing Microsoft Office Security Bulletins" below](#)
- ["About Patch Management and Microsoft Update Catalog" on page 27](#)
- ["Enabling Microsoft Office Updates in Patch Management \(Versions 3.0.2 and later\)" on page 28](#)

Best Practices for Managing Microsoft Office Security Bulletins

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

Windows Installer 3.1 Requirement

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

Options for Updating Microsoft Office Products

The method initially used for deploying Microsoft Office products determines available options for patching the agent software. Microsoft Office products use Windows Installer technology, which supports installation from compressed media typically found on a CD-ROM or an AIP. For details on Microsoft best practices, see the Microsoft article, [Distributing Office 2003 Product Updates](#).

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

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

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

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

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

When to use Patch Management to Deploy Microsoft Office Updates

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

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

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

Caution: Administrators who manage agent devices running Microsoft Office products currently patched through the AIP synchronization process must be careful not to interchange these patching methods (AIP synchronization process and Patch Management). Doing so may cause a break in the synchronization between the agent device and the AIP. For details about the synchronization process, see the Microsoft article [Updating Office XP Clients from a Patched Administrative Image](#).

Client Automation Management Features that are Disabled when using Patch Management

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

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

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

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

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

Access 2007	PowerPoint 2007
Excel 2007	Project 2007

Groove 2007	Publisher 2007
InfoPath 2007	SharePoint Designer 2007
OneNote 2007	Visio 2007
Outlook 2007	Word 2007

When using the new Microsoft Update Catalog data feed, the Patch Management does not provide support for patching Microsoft Office 2000, or earlier, applications. This restriction is a result of the Patch Management agent's reliance on the Microsoft Update Catalog to detect Microsoft vulnerabilities. See "Embedded Support for the new Microsoft Update Catalog (wsusscn2.cab)" on page 15.

Microsoft Office Service Packs

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

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

- **For Microsoft Update Catalog Only:** Due to changes in this data feed, service pack dependencies cannot be obtained and reported by Patch Management. It is imperative that Administrators research the pre-requisite service packs for applicable bulletins and entitle them to devices.
- **For Microsoft Update Catalog, Legacy:** For devices running Windows 2000 only, Patch Management follows the behavior of the default data feed and will report and deploy dependent service packs to devices entitled to it in policy. For devices running platforms other than Windows 2000, Patch Management follows the behavior of Microsoft Update Catalog and Administrators must research and entitle devices to pre-requisite service packs.

About Patch Management and Microsoft Update Catalog

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

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

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

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

- If you deploy patches for Microsoft Office using Patch Management with Microsoft Update Catalog enabled, then you should no longer publish or deploy patches for Microsoft Office using Application Manager or Application Self-service Manager, or an external ACP. You must choose between the Patch Management solution for patch management and your existing solution.
- If you choose Application Manager or Application Self-service Manager because you would like to leverage a feature derived from the ZCREATE, ZVERIFY, or ZUPDATE methods (such as their ability to manage MSI Features and Properties or install on first use), then you are advised to publish Microsoft Office patches via the Publisher and then deploy and manage them using Application Manager or Application Self-service Manager. You should not introduce Patch Management into this model.
- If you choose to continue to use an external ACP, then you should not introduce Patch Management into this model. Doing so will likely break the synchronization between the agent and the ACP.
- If you choose to enable Patch Management with the Microsoft Update Catalog data feed, perform the tasks in the topic below, Enabling Microsoft Office Updates in Patch Management (Versions 3.0.2 or above).

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

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

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

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

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

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

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

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

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

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

6. Entitle the Microsoft Office bulletins to devices in policy.

About Patch Objects used for Device Compliance Reporting

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

- **DESTATUS** - Device Status Object: Contains a single heap identifying the overall device status, how many bulletins are in each compliance status, and the last scan time. Compliance status values include OK, Warning, Reboot Pending, Error, and Not Applicable.
- **RESTATUS** - Release Status Object: Contains one heap for every release that is present on the device.
- **BUSTATUS** - Bulletin Status Object; Contains one heap for each bulletin and gives the bulletin status.
- **PASTATUS** - Patch Status Object; Contains one heap for each patch and provides the patch status.
- **DEERROR** - Device Error Object: Contains any errors that occurred during discovery or management of the device.

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

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

- `<InstallDir>\ConfigurationServer\data\patch` (Windows).
- `/opt/HP/CM/ConfigurationServer/data/patch` (UNIX®).

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

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

Patch Analysis and Reports

The RCA Reporting Server provides web-based reports for Patch Management.

To view the reports, access the **Reporting** tab in the RCA Console. Under Reporting Views, click **Patch Management Reports** to expand the list of reports.

There are four types of Patch Management reports:

- **"Executive Summaries"** on page 32: Executive Reports provide a snapshot of your environment from the patch-compliance perspective. Use these pie or bar chart reports to drill down into the detail reports about devices in or out of compliance, or about bulletins for which devices are in or out of compliance.
- **"Patch Compliance Reports"** on page 34: The Management Agent sends product and patch information to RCA. This information is compared to the available patches to see if managed devices require certain patches to remove vulnerabilities. Compliance reports show only the information applicable to detected devices in your environment.
- **"Acquisition Reports"** on page 39: Acquisition-based reports show the success and failures of the patch acquisition process from a vendor's web site.
- **"Research Reports"** on page 39: Research-based reports display information about the patches acquired from the software vendor's web site. Research-based reports offer a Filter bar.

Expand each report type to see the list of available reports. View the list of Patch Management Reports.

Filtering Patch Reports with Reporting Server

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

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

Click the magnifying glass  to open the filter lookup window.

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

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

For additional information on creating filters, see the *Radia Client Automation Enterprise Reporting Server Reference Guide*.

Drilling Down to Detailed Information

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

Whenever you see the Details () icon in the data grid, you can click it to display more detailed information.

You can also drill down to more detailed information by clicking the device counts in certain columns in some reports.

Available Report Actions include Data Export Options

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

Report Actions

Icon	Description
	Go back one page in the reports view.
	Return to the Reports home page.
	Refresh the data from the Reporting Server. A refresh also occurs when you apply or remove a filter.
	Add this report to your list of favorites.
	Email a link to this report.
	Open a "quick help" box or tool tip. This applies only to filters.
	Print this report.
	Collapses the data portion of the report view.
	Expands the data portion of the report view.
	Show the graphical view of this report

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

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

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

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

Note: RCA reports are displayed in the Greenwich Mean Time (GMT) time zone.

Executive Summaries

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

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

Patch Status on Executive Summary Reports

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

Sample Executive Summary Reports follow.

- ["Overall Device Status" below](#)
- ["Device Status" below](#)
- ["Bulletin Status" below](#)
- ["Vendor Status" on next page](#)

Overall Device Status

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

Applicable Filters: None.

Device Status

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

- **Device Status:** This graphical report appears in the upper panel. The graphs provide percentages for devices in various states that include Patched, returned Warnings, Reboot Pending, Other Errors, or Not Patched.
 - Single-click on an individual status label or section to display the number of devices in that state.
 - Double-click on an individual status label or section to access a report that lists the devices in that state. Single-click on the name of a device in the device list to find the patch status for that particular device.
- **Device Patch Compliance Status:** This graphical report appears in the lower panel. The graphs provide patch percentages for devices indicating their patch compliance level. The patch compliance levels are shown in percentage bands of roughly 20%, except for the last band, which shows the 99 to 100% compliance level percentage band. For example, if a device requires 10 bulletins, but only 5 patches have been applied, this device will be 50% patched and hence will be included in the 41-60% Patched band of the pie chart and bar graph.
 - Single-click on a band in the pie chart to display the list of devices that fall into this band.
 - Single-click on the name of a device in the device list to see patch compliance information specific for that particular device.

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

Bulletin Status

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

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

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

Vendor Status

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

Applicable Filters: None.

Patch Compliance Reports

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

The Patch Compliance Reports include:

- "Device Status" below
- "Devices Not Fully Patched" on next page
- "Devices With Bulletin Install Errors" on page 36
- "Bulletin Status" on page 36
- "Product Status" on page 37
- "Release Status" on page 38
- "Patch Status" on page 38
- "Devices with Serious Errors" on page 38

Note: The Patch Compliance Reports documented in this guide require the servers and agents in your Patch Management environment to be at Version 7.50 or above. In particular, the Product Status, Release Status, and Patch Status reports documented in this guide cannot be populated by pre-Version 7.50 Patch Agents.

Device Status

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

Note: The Report title shows Device Status.

Applicable Filters: Device name and Patch Compliance Status. For example, Patched, Not patched, and Reboot Pending.

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

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

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

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

- A question mark indicates that at least one vulnerability could not be confirmed.
- A red X indicates that at least one vulnerability is not patched for this device.
- An exclamation point indicates a warning.
- A lower-case letter 'i' indicates *Not Applicable*.

For each device, you can:

- Click the magnifying glass for additional detail.
- Click the number in the Applicable Products column to see the products discovered for that device.
- Click the number in the Applicable Bulletins column to see the applicable bulletins for that device.
- Click the number in the Patched column to see the list of bulletins that were installed as patches on this device.
- Click the number in the Warning column to see vulnerabilities that the Patch Management cannot confirm as patched because there may be some discrepancy in the patch verification process.
For example, a patch for Microsoft SQL server or Microsoft MSDE may show up as a warning. MSDE installs fewer files than SQL Server. A device with MSDE may qualify for the same patch as a device with SQL server, but does not require all the files in the patch. Since Patch Management cannot report the vulnerability as being patched, this would be reported as a warning.
Another example may be that a file version on the device is newer than the one delivered by the patch. Again, in this case, Patch Management cannot report the vulnerability as being patched so it reports a warning.
- Click the number in the Not Patched column to see what patches are available but have not been applied to this device.
- Items in the Other column represent patches that Patch Management was not able to verify or was not able to patch due to a device error.
- Items in the Reboot Pending column represent patches that will be complete after the device is rebooted. These devices will also have a power button icon next to the device name.

Devices Not Fully Patched

Use this Compliance report to focus on the devices that are not in compliance with your patch policy. The devices included on this report show one or more Applicable Bulletins with a status of Not Patched, Other (includes device errors) or Pending Reboot. This report is similar to the "[Device](#)

Status" on [previous page](#), except that it eliminates any devices considered in compliance because all of their applicable bulletins are either patched or just report warnings.

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

- For each device, you can perform the same operations as discussed with the Compliance report for "Device Status" on [page 34](#).
- The last column indicates the number days since the device was last scanned.

Devices Pending Reboot

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

Applicable Filters: Device name.

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

Devices With Bulletin Install Errors

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

Applicable Filters: Device name.

- Click the number in the **Other** column to link to list of bulletin(s) for that device which encountered errors and the error description.

Bulletin Status

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

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

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

- A check mark indicates that this bulletin has been patched on all applicable devices.
- A power button indicates that at least one device is pending a reboot to be in compliance.

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

- A question mark indicates that this vulnerability could not be confirmed on at least one device.
- A red X indicates at least one device is not patched for this bulletin.
- An exclamation mark indicates a warning.

For each bulletin, you can:

- Click the bulletin number in the Bulletin column to go to the vendor's web site for more information on the bulletin.
- Click the CVE number in the CVE column to go the Common Vulnerabilities and Exposures web site.
- Click the number in the Applicable Devices column to see the applicable devices for that bulletin.
- Click the number in the Patched column to see the patched devices.
- Click the number in the Warning column to see vulnerabilities that the Patch Management cannot confirm as patched because there may be some discrepancy in the patch verification process.

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

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

- Click the number in the Not Patched column to see what patches are available but have not been applied.
- Items in the Other column represent patches that Patch Management was not able to verify or encountered an error.
- Items in the Reboot Pending column represent patches that will be complete after the device is rebooted.

Product Status

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

- Product names appended with (MSFT) were distributed with "Enable Download of Metadata" turned on.
- Product names without qualification were distributed with "Enable Download of Metadata" turned off.

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

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

For each product, you can:

- View detected vulnerabilities
- Click a number in one of the count columns to see the details of the devices with the number of Applicable Bulletins for that product.
- From the resulting view, click on Applicable Bulletins to see the list of bulletins applicable for the selected device for the product release.

Release Status

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

- Release names appended with (MSFT) have bulletins distributed with "Enable Download of Metadata" turned on.
- Release names without qualification have bulletins distributed with "Enable Download of Metadata" turned off.

Click to see Applicable Bulletins.

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

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

- Click the number of Applicable Devices to see a list of devices with the number of applicable bulletins for each device for a this product release.
- Click the number of Applicable Bulletins to see the list of bulletins applicable for this device for this product release.

Patch Status

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

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

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

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

Devices with Serious Errors

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

To use this report, ensure the FINALIZE_PATCH service has been entitled to the managed devices in your environment, as discussed in the section "[Entitle the FINALIZE_PATCH Service](#)" on page 43

Acquisition Reports

There are three Acquisition Reports:

- [Acquisition Summary](#)
- [Acquisition Bulletin](#)
- [Acquisition by Patch](#)

For information on the Acquisition reports, see "[Patch Acquisition Reports](#)" on page 21.

Research Reports

Research based reports display information about the patches acquired from the software vendor's web site. Research based reports offer a Filter bar.

The Research Reports include:

- ["Research by Bulletin"](#) below
- ["Research by Devices"](#) on next page
- ["Research by Patches"](#) on next page
- ["Research by Products"](#) on next page
- ["Research by Releases"](#) on next page
- ["Compliance and Research Exception Reports"](#) on page 41

Research by Bulletin

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

Note: This report *cannot* be filtered using the bulletin name filter.

Note: The severity rating displayed in this report and the Acquisition By Bulletins report may not match with the Microsoft Security Bulletin Summary Page in the case where the bulletin

contains patches not supported by WSUS and where their severity is higher than that of the other patches within the same bulletin. This issue is caused by the fact that the severity rating for the bulletin is determined by the severity of the patches that it contains. If the bulletin contains legacy patches, which would not be supported by WSUS, those will be excluded when the severity rating is determined.

Research by Devices

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

Research by Patches

Use this report to view information on patch files including on acquisition status. Click the number in the CVE column to go to the Common Vulnerability Exposures web site. Click the icon in the Down column to download the patch file. The icon in the Severity column indicates the severity for Windows patches. The severity ratings range from Critical, to Important, to Moderate, to Low. If the patch is not for a Windows platform, the Unknown icon is displayed. Click on the icon in the Severity column to see all patches with the same severity. Pre-existing patches do not have severity ratings. To view severity ratings for existing bulletins and patches, you must re-acquire them using the Force and Replace options.

Research by Products

Use this report to drill down to all bulletins filtered by product. If you click the number in the Applicable Bulletins column for the "redhat-nonexistent" product in this report, you will see the list of Redhat dependency bulletins displayed under the "Bulletin Dependencies" report.

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. If you click the number in the Applicable Bulletins column for the "redhat-nonexistent" product in this report, you will see the list of Redhat dependency bulletins displayed under the "Bulletin Dependencies" report.

Compliance and Research Exception Reports

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

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

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

Managing Vulnerabilities

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

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

Note: SuSE 10 and 11 bulletins will have Persistent-assigned instance names that are derived from the original bulletin names. For details, see "[Instance Naming Convention for SuSE 10 and 11 Bulletins](#)" on next page.

To manage a vulnerability:

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

6. Click **Copy**.
7. Click **Yes** to confirm the connection.

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

Instance Naming Convention for SuSE 10 and 11 Bulletins

As the instance field length in the CSDB is limited to 32 characters, all SuSE 10 and 11 bulletins will be published using Persistent-reformatted instance names that are shorter and easier to distinguish than the actual SuSE 10 and 11 bulletin names.

For SuSE 10

During acquisition the SuSE10 bulletin name will be converted into a new name and given to the instance names under PRIMARY.PATCHMNGR.BULLETIN and PRIMARY.PATCHMGR.ZSERVICE.

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

For example, Radia Patch Management will convert the SuSE 10 bulletin name entered for acquisition as follows:

On SuSE Linux Enterprise Server 10:

`SUSE-patch-MozillaFirefox-2683`

to:

`SLES10SP0-2683-MOZILLAFIREFOX`

On SuSE Linux Enterprise Desktop 10:

`SUSE-patch-MozillaFirefox-2683`

to:

`SLED10SP0-2683-MOZILLAFIREFOX`

On SuSE Linux Enterprise Server 10SP3:

`SUSE-patch-SLESP3-MozillaFirefox-2683`

to:

`SLES10SP3-2683-MOZILLAFIREFOX`

On SuSE Linux Enterprise Desktop 10SP3:

`SUSE-patch-SLESP3-MozillaFirefox-2683`

to:

`SLED10SP3-2683-MOZILLAFIREFOX`

The reformatting drops the SUSE-PATCH prefix and reorders the remaining content to move the unique numbering scheme earlier in the format. For the above example, the CSDB instance under PRIMARY.PATCHMGR.BULLETIN and PRIMARY.PATCHMGR.ZSERVICE will be created using the name SLES10SP0-2683-MOZILLAFIREFOX.

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

For SuSE 11

During acquisition, the SuSE 11 bulletin names will be converted into a new name and the instance name under PRIMARY.PATCHMGR.BULLETIN and PRIMARY.PATCHMGR.ZSERVICE will be created in the newly formed name.

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

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

```
UPDATEINFO-SLESSP0-MOZILLAFIREFOX-1234
```

to:

```
SLES11SP0-1234-MOZILLAFIREFOX
```

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

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

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

Entitle the FINALIZE_PATCH Service

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

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

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

Deploying Automatic and Interactive Patches

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

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

When the bulletin is published to the Configuration Server Database, the RUNMODE attribute of the ZSERVICE class of the PATCHMGR Domain defines the type of patch. Use the catexp parameter of the radskman command line to limit your installation to bulletins marked as automatic only. The format would be catexp=runmode:automatic. If the catexp parameter does not exist, all bulletins will be processed. For a typical Patch Management 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 Client Automation Enterprise Application Manager and Application Self-Service Manager Reference Guide*.

Customizing Reporting Options

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

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

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

- **DesiredState**
This attribute maps to the DSTATE attribute in the OPTIONS, FILECHG, and REGCHG classes. Use this attribute to set what the return code should be based on the criteria stated in the USE variable.
- **Report Threshold**
This xml attribute maps to the REPORT attribute in the OPTIONS, FILECHG, and REGCHG classes. The properties of the file or registry key will be sent to the Patch Management based on this value. If the return code is greater than or equal to the value of the REPORT attribute, the

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

Note: Setting REPORT to 0 will send the information for all files that show an OK status. This may overburden the Patch Management Server.

- **Use**

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

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

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

To customize reporting options:

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

1. In the USE attribute in the appropriate class (or in the patch descriptor file), specify what properties of the file or registry key you want to evaluate. For example, if you were only interested in the date of a file, set USE to GMTDATE.
2. Set DesiredState (DSTATE) by equating a state with a return code. Separate multiple conditions with commas. Use the appropriate state from the list below.
 - Use state E (exists) if your only criterion for status is the existence of the file or registry key.
 - Use state !E (does not exist) if your only criterion for status is whether the file or registry key does not exist.
 - Use state EQ (equal) if the file or registry key meets the exact criteria.
 - Use state !EQ (not equal) if the file or registry key does not meet at least one of the criteria.
 - Use state LT (less than) if the file or registry key is less than at least one of the criteria.
 - Use state GT (greater than) if the file or registry key is greater than at least one of the criteria.Use the appropriate return code from the list below.
 - Use 0 to represent a status of OK.
 - Use 4 to represent a warning status.

- Use 8 to represent an error status.

Follow these rules for valid DSTATE values:

- At least one of the conditions should have a return code of 0 (OK), but you could have more than one condition return a non-zero value (4, 8).
- Testing for Equality (EQ) implies that the component should exist and need not be expressed in the DSTATE variable.

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

- Return a status of OK if the file does not exist (!E=0).
- Return a Warning status if the VERSION, GMTDATE or SIZE of the file are greater than the patched file (GT=4).
- Return an Error status if the VERSION, GMTDATE or SIZE of the file is less than the patched file (LT=8).

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

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

3. Set a REPORT threshold. The properties of the file or registry key will be sent to the Patch Management based on this value. If the return code is greater than or equal to the value of the REPORT attribute, the file and registry information will be sent to the Patch Management and will be available in Patch Management reports. For example, set REPORT to 1 to send the properties if the return code is either 4 (Warning) or 8 (Error).

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

Disabling Vulnerability Detection and Deployment

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

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

Controlling Patch Deployment (PATCHARG)

For each patch file, Patch Management 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.

Note: When patches are acquired from Microsoft Update, the Source column in the report will show “Microsoft Update” instead of “Microsoft.”

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

To create alternate command line parameters using PATCHARG:

1. Use the Admin CSDB Editor to navigate to the PATCHARG Class in the PATCHMGR Domain.
2. Right-click **PATCHARG** and create a new instance. A new instance called WSPARGS has been created in our example.
3. Type the new parameters that you want to use. There are two attributes in the PATCHARG Class: OCREATE to install the patch, and ODELETE to remove the patch.
4. Type the path to the PATCHARG Instance in place of the PATCHARG Attribute for the patch file in the BULLETIN Class.

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

Removing a Patch

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

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

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

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

See "[Removing a Patch](#)" above for additional information.

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

1. Use the Admin CSDB Editor to navigate to the MANAGE Instance of the Client Method (CMETHOD) Class in the PATCHMGR Domain.
2. Double-click the ZDELETE Attribute in the tree view, and in the text box, type:
`hide nvdkit &(ZMASTER.ZSYSDRV) &(ZMASTER.ZSYSDIR) patchagt.tkd manage`

3. Click **OK** to change the instance. The Instance Edit Confirmation opens.
4. Click **Yes** to confirm the changes.
The Patch Management Agent must make a connect in order for the managed device to receive the necessary configuration change to allow the removal of patches.

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

Summary

- Patch Management supplies you with research, patch acquisition, and vulnerability reports.
- Use the reports to identify vulnerabilities in your enterprise.
- Manage vulnerabilities by assigning the patch's service to your devices.

Appendix A

Supported XML Tags for Patch

This chapter describes the XML tags supported in various Patch Manager classes. You can use the tags that are supported to create custom patch descriptor files.

Descriptor Files

The patch descriptor files from Persistent contain information about Products, Releases, Patches, and Patch Manifests. These are shown in tables following the figure below.

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

Sample patch descriptor file

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

Bulletin Node

Node name: Bulletin

Parent node: None

Children: Products

XML Tags in the BULLETIN class

XML Tag	RCA Attribute	Description
PopularitySeverityID	POPULAR	Popularity ID
URL	URL	Bulletin URL
FAQURL	FAQURL	Frequently Asked Questions (FAQ) URL
Supported	SUPPORT	Supported [Y/N]

Reference Guide

Appendix A: Supported XML Tags for Patch

XML Tag	RCA Attribute	Description
ImpactSeverityID	IMPACT	ImpactID Source: Red Hat Network, Novell (SuSE) data feeds
MitigateSeverityID	MITIGATE	Mitigate ID
PreReqSeverityID	PREREQ	Prereq ID
DateRevised	REVISED	Bulletin Revised On Date the bulletin was revised in YYYYMMDD format. Source: Red Hat Network, Novell (SuSE) data feeds
Source	SOURCE	Source [MICROSOFT] NOVADIGM CUSTOM REDHAT SUSE] Directory from which the patch descriptor file was published.
Vendor	VENDOR	MICROSOFT/REDHAT/SUSE
Type	TYPE	Type of Bulletin Security/ServicePack/Other
Platform	PLATFORM	winnt//redhat/suse
Name	NAME	External ID Source: Red Hat Network, Novell (SuSE) data feeds
Title	TITLE	Title Bulletin title. Source: Red Hat Network, Novell (SuSE) data feeds
DatePosted	POSTED	Bulletin Posted On Date the bulletin was posted in YYYYMMDD format. Source: Red Hat Network, Novell (SuSE) data feeds
Schema Version		The patch schema version currently 1.0
	MTIME	Time the instance was modified in the CSDB.
	CTIME	Time the instance was created in the CSDB.
	ID	Internal instance ID.
HPPosted	HPPOSTED	Date the bulletin was initially posted by Persistent.
HPRevised	HPREVISD	Date the bulletin was revised by Persistent.
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

XML Tags in the PRODUCT class

XML Tag	RCA Attribute	Description
Name	NAME	Source: Red Hat Network, Novell (SuSE) data feeds
Name	NAME	Source: Red Hat Network, Novell (SuSE) data feeds

Releases Node

Node name: Releases

Parent node: Product

Children: Release

Attributes: None

Release Node

Node name: Release

Parent node: Releases

Children: Patch

XML Tags in the RELEASE class

XML Tag	RCA Attribute	Description
Name	NAME	Source: Red Hat Network, Novell (SuSE) data feeds

Patch Node

Node name: Patch

Parent node: Release

Children: Package

XML Tags in the PATCH class

XML Tag	RCA Attribute	Description
PatchURL	PATCHURL	A URL that points to an .EXE or .MSI file. Source: SUS, Red Hat Network, Novell (SuSE) data feeds
Reboot	REBOOT	Specified if the device should be rebooted, after the patch is installed. Source: SUS, Red Hat Network, Novell (SuSE) data feeds
Architecture	ARCH	x86 i64 Source: SUS, Red Hat Network, Novell (SuSE) data feeds
Language	LANG	en,fr,de Source: SUS
MSSUSName	SUSNAME	The SUS name for the patch
SupersededByBulletin	SUPERBU	The bulletin name that supersedes this patch. Source: Red Hat Network, Novell (SuSE) data feeds
Superseded	SUPERCED	Specifies if the patch has been superseded. Valid values are Y or N. Source: Red Hat Network, Novell (SuSE) data feeds
OSVersion	OSVER	Operating System Version
OSType	OSTYPE	The operating system type, such as server or workstation.
OSSuite	OSSUITE	The operating system suite, e.g., datacenter, blade.
Platform	PLATFORM	The platform type: winnt, redhat, suse
InstallCmdline	OCREATE	This is the arguments that are passed to the create procedure. Source: SUS, Red Hat Network, Novell (SuSE) data feeds
VerifyCmdline	OVERIFY	The Verify Arguments.
UninstallCmdline	ODELETE	The Uninstall Arguments.
ObjectType	OTYPE	Format: namespace=script filename Default: winnt.patch This specifies the type of the object and the name of the script file that would have the following procedures defined verify create delete assert The procedures should have the namespace as part of the name, e.g., winnt.patch::create. If the script filename is not specified then the filename is {namespace}.tcl. Source: Novadigm
ProbeCmdline	OVERIFY	The probe command line. Source: Novadigm
	ID	The unique ID created in the HPCA-CSDB for this

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

Patch Signature Node

Node name: PatchSignature

Parent node: Patch

Children: FileChg, RegChg

Attributes: None

FileChg Node

Node name: FileChg

Parent node: PatchSignature

Children: None

XML Tags in the FILECHG class

XML Tag	RCA Attribute	Description
Name	NAME	File name.
Path	PATH	The directory name, this can contain environment variables, e.g., %windir%, and is used by the appropriate scripts for Windows and Linux.
CRC32	CRC32	The CRC of the data.
Gmttime	GMTTIME	The GMTDATE expressed as YYYYMMDD.
Gmtdate	GMTDATE	The GMTTIME expressed as HH:MM:SS.
Size	SIZE	The size of the file.
Checksum	CHECKSUM	The checksum of the file.
Version	VERSION	The version of the file.
	DSTATE	The desired state of the FILECHG instance, this is usually classed in from another instance in the CSDB. Source: Novadigm
	REPORT	The report threshold. If on evaluation of this file change instance the RC is greater than the threshold then we will create a ZOBJSTAT for that instance. Source: Novadigm
	USE	The variables to use during comparison, e.g., Version,Checksum,Gmtdate. Source: Novadigm

RegChg Node

Node name: RegChg

Parent node: PatchSignature

Children: None

XML Tags in the REGCHG class

XML Tag	RCA Attribute	Description
Name	NAME	Value Name.
Path	PATH	The fully qualified Registry Key Name.
Value	VALUE	The Data value stored in the registry.
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

XML Tag	RCA Attribute	Description
	DSTATE	Desired state of FILECHG instance, this is usually classed in from another instance in the RCS database. Source: Novadigm
	REPORT	Report threshold. If on evaluation of this file change instance, the RC is greater than the threshold then we will create a ZOBJSTAT for that instance. Source: Novadigm
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
	DSTATE	Desired state of FILECHG instance, this is usually classed in from another instance in the RCS database. Source: Novadigm

HPFileset Node

Node name: HPFileset

Parent node: PatchSignature

Children: None

XML Tags in the HPFSET class

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

Appendix B

Restarting the Managed Device

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

- Set the type of warning message
- Handle a reboot with either a machine or user connect
- Cause an immediate restart after the application event.

This chapter describes the tasks that you perform to restart a managed device.

Application Events

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

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

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

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

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

Reboot Types

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

- **Hard Reboot (H)**

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

- **Soft Reboot (S)**

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

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

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

Reboot Modifier: Type of Warning Message

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

Note: The Application Manager for Linux does not display reboot panels.

- **Quiet (Q)**

No reboot panel will be displayed.

- **OK Button (A)**

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

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

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

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

For example, the default Reboot panel displays both an **OK** and **Cancel** as shown in the following screenshot:

View the default reboot

If you 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.

Reboot Modifier: Machine and User Options

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

Note: Patch Management Agent connects occur in the machine context.

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

Reboot Modifier: Immediate Restart

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

Specifying Multiple Reboot Events

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

Reference Guide

Appendix B: Restarting the Managed Device

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

Appendix C

Patch.cfg Parameters

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

Patch Management Server Configuration Parameters

It is recommended that you configure the Patch Management parameters in the RCA Console. If you cannot use the console, you can make changes directly in the `patch.cfg` file. The default location is `<InstallDir>\PatchManager\etc`. The parameters are listed in this appendix.

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

- **admin_date_fmt:** Specify the date and time format for the RCA Console. The default is `{%Y-%m-%d %H:%M:%S}` where `%Y` is the year with century, `%m` is the month number, `%d` is the day of the month, `%H` is the hour in 24-hour format, `%M` is the minute, and `%S` is the seconds.
- **data_dir:** Specify the directory on the local computer (Patch Management Server) where you want the patches downloaded to before they are sent to your Configuration Server. Use this parameter to set where to store your patch descriptor files and patch data files in an alternate directory. If you choose to perform an acquisition using a directory that is pre-populated with data from a previous acquisition, specify a different directory in this parameter. The default is `<InstallDir>\data\PatchManager\patch`.
- **db_type:** Specify the database type. The two possible values are `mssql` for Microsoft SQL Server (the default) and `oracle` for Oracle. If you are using Oracle, change this value to `oracle` before doing a patch acquisition or a database synchronization. This parameter is required to synchronize with an Oracle database.
- **dsn:** Specify the **Data Source Name (DSN)** the Patch SQL database. This parameter is required.
- **dsn_user:** Specify the SQL user for the DSN for the Patch SQL database.
- **dsn_pass:** Specify the password for the SQL user for the DSN for the Patch SQL database.
- **ftp_proxy_pass:** If you use a proxy server for FTP traffic, specify your password.
- **ftp_proxy_url:** If you use a proxy server for FTP traffic, specify its URL in the format `ftp://ip:port`. At the time of this writing, Patch Management supports basic authentication only.
- **ftp_proxy_user:** If you use a proxy server for FTP traffic, specify your user ID.

- **history:** Specify how many days to keep the Patch Auth Store (PASTORE) instances. This class contains one instance for each patch acquisition session. It is recommended specifying this in the `patch.cfg` file, not on the command line. If `history` has a smaller value than `purge_errors`, then `purge_errors` will be set to the value for `history`. The default of 0 means never delete any history of Patch Acquisition.
- **http_proxy_pass:** If you use a proxy server for HTTP traffic, specify your password.
- **http_proxy_url:** If you use a proxy server for HTTP traffic, specify its URL in the format `http://ip:port`. At the time of this writing, Patch Management supports basic authentication only.
- **http_proxy_user:** If you use a proxy server for HTTP traffic, specify your user ID.
- **http_timeout:** Set the total amount of time to wait for the file to be completely downloaded. If the acquisition session is unable to download the file in this time, then the acquisition will abort the current HTTP location, and will continue the acquisition with the next HTTP location. Increase the `http_timeout` if you need to allow additional time for a bulletin to download. This parameter is expressed in seconds in the `setup.tsp` page. Specify `http_timeout` in either the `patch.cfg` file or on the command line in milliseconds. This is reflected in `patch.cfg` as 3600000. If you specify `http_timeout` on the command line, it will be for this acquisition session only.
- **lang:** Patch Management supports non-double byte languages. Specify the abbreviation of the languages for which you want to acquire patches. Precede any products you want excluded with an exclamation point (!). The default is `en` (English). If you wanted to include French and English, specify, `- lang fr, en`.
- **microsoft_sus_url:** Specify the URL for the Microsoft SUS feed. The default is <http://www.msus.windowsupdate.com/msus/v1/aucatalog1.cab>.
- **nvdms_url:** Specify the URL to connect to the Patch Update web site provided by Persistent. This is the same as the `nvdms_url` parameter in `patch.cfg`. The default is http://managementsoftware.hp.com/Radia/patch_management/data.
- **purge_errors:** Specify how many days to keep the Publisher Error (PUBERROR) instances. This class contains one instance for each patch acquisition error. It is recommended specifying this in the `patch.cfg` file, not on the command line. If `history` has a smaller value than `purge_errors`, `purge_errors` will be set to the value for `history`. The default is 7.
- **rps_pass:** If authentication has been enabled on your Configuration Server, specify the password for the `rps_user`.
- **rps_url:** Specify the location of your Configuration Server in URL format. This parameter is required. Use the format `radia://ipaddress:port`, where:
 - `radia` indicates the session type to be opened to the Configuration Server
 - `ipaddress` is the hostname or IP address of the computer hosting the Configuration Server
 - `port` is the port number of the Configuration Server.
- **rps_user:** If authentication has been enabled on your Configuration Server, specify the `rps_user`.
- **reporting_url:** Specifies the URL of your Reporting Server. The default is `http://localhost/reportingserver`.

- **retire**: Specify the bulletins to retire separated by commas. Use the `-retire` parameter to:
 - Delete specified bulletins if they exist in the Configuration Server database during the current publishing session.
 - Not publish the bulletins specified in the retire parameter to the Configuration Server database during the current publishing session. The use of the retire option supersedes the bulletins option.

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

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

Note the following:

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

Example: `-retire MS00-001,MS00-029`

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

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

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

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

The default is No.

- **rhn_url**: Specify the URL for the Red Hat Security Network. The default is <http://xmlrpc.rhn.redhat.com/XMLRPC>.
- **suse_pass**: Specify the password for the Novell web site that is hosting SuSE 9 patches.
- **suse_urls**: Specify the URLs for the Novell web site that is hosting SuSE patches. The defaults are:
9:
<https://you.novell.com/update/i386/update/SUSE-CORE/9/>
<https://you.novell.com/update/i386/update/SUSE-SLES/9/>
9-x86_64:
https://you.novell.com/update/x86_64/update/SUSE-CORE/9/
https://you.novell.com/update/x86_64/update/SUSE-SLES/9/
- **suse_user**: Specify the user for the Novell web site that is hosting SuSE 9 security patches.
- **suse10_pass**: Specify the password for the Novell web site that is hosting SuSE 10 and 11 patches.
- **suse10_urls**: Specify the URLs for the Novell web site that is hosting SuSE 10 and 11 patches. The defaults are:
10:
[https://nu.novell.com/repo/\\$RCE/SLES10-Updates/sles-10-i586](https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-i586)
[https://nu.novell.com/repo/\\$RCE/SLED10-Updates/sled-10-i586](https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-i586)
10SP1:
[https://nu.novell.com/repo/\\$RCE/SLES10-Updates/sles-10-i586](https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-i586)
[https://nu.novell.com/repo/\\$RCE/SLED10-Updates/sled-10-i586](https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-i586)
10SP2:
[https://nu.novell.com/repo/\\$RCE/SLES10-SP2-Updates/sles-10-i586](https://nu.novell.com/repo/$RCE/SLES10-SP2-Updates/sles-10-i586)
[https://nu.novell.com/repo/\\$RCE/SLED10-SP2-Updates/sled-10-i586](https://nu.novell.com/repo/$RCE/SLED10-SP2-Updates/sled-10-i586)
10-x86_64:
[https://nu.novell.com/repo/\\$RCE/SLES10-Updates/sles-10-x86_64](https://nu.novell.com/repo/$RCE/SLES10-Updates/sles-10-x86_64)
[https://nu.novell.com/repo/\\$RCE/SLED10-Updates/sled-10-x86_64](https://nu.novell.com/repo/$RCE/SLED10-Updates/sled-10-x86_64)
10SP1-x86_64:
[https://nu.novell.com/repo/\\$RCE/SLES10-SP1-Updates/sles-10-x86_64](https://nu.novell.com/repo/$RCE/SLES10-SP1-Updates/sles-10-x86_64)
[https://nu.novell.com/repo/\\$RCE/SLED10-SP1-Updates/sled-10-x86_64](https://nu.novell.com/repo/$RCE/SLED10-SP1-Updates/sled-10-x86_64)
10SP2-x86_64:
[https://nu.novell.com/repo/\\$RCE/SLES10-SP2-Updates/sles-10-x86_64](https://nu.novell.com/repo/$RCE/SLES10-SP2-Updates/sles-10-x86_64)
[https://nu.novell.com/repo/\\$RCE/SLED10-SP2-Updates/sled-10-x86_64](https://nu.novell.com/repo/$RCE/SLED10-SP2-Updates/sled-10-x86_64)
10SP3:

```
{https://nu.novell.com/repo/$RCE/SLES10-SP3-Updates/ sles-10-i586}
```

```
{https://nu.novell.com/repo/$RCE/SLED10-SP3-Updates/ sled-10-i586}
```

```
10SP3-x86_64:
```

```
{https://nu.novell.com/repo/$RCE/SLES10-SP3-Updates/ sles-10-x86_64}
```

```
{https://nu.novell.com/repo/$RCE/SLED10-SP3-Updates/ sled-10-x86_64}
```

```
11:
```

```
{https://nu.novell.com/repo/$RCE/SLES11-Updates/sle-11-i586/}
```

```
{https://nu.novell.com/repo/$RCE/SLED11-Updates/sle-11-i586/}
```

```
11SP1:
```

```
{https://nu.novell.com/repo/$RCE/SLES11-SP1-Updates/ sles-11-i586}
```

```
{https://nu.novell.com/repo/$RCE/SLED11-SP1-Updates/ sled-11-i586}
```

```
11-x86_64:
```

```
{https://nu.novell.com/repo/$RCE/SLES11-Updates/sle-11-x86_64/}
```

```
{https://nu.novell.com/repo/$RCE/SLED11-Updates/sle-11-x86_64/}
```

```
11SP1-x86_64:
```

```
{https://nu.novell.com/repo/$RCE/SLES11-SP1-Updates/ sles-11-x86_64}
```

```
{https://nu.novell.com/repo/$RCE/SLED11-SP1-Updates/ sled-11-x86_64}
```

- **suse10_user**: Specify the user for the Novell web site that is hosting SuSE 10 and 11 security patches.
- **sync**: Specify the targets that need to be synchronized. The default is rcs.

Patch Acquisition Parameters

To acquire patches from a command line:

1. From a command prompt on your Patch Management Server, navigate to the Patch Management directory. The default location is
<InstallDir>\data\PatchManager\

Note: You can also use the acquisition file you created from a command line. To do this, use the config parameter.

2. Using the parameters listed in the bulleted list below, create a command line similar to the following:

```
nvdkit ./modules/patch.tkd acquire -bulletins MS04-*
```

where you want to acquire the patch files for only bulletins from the Microsoft web site matching a filter of MS04-*

Note: Parameters specified on the command line overwrite those specified in `patch.cfg`. Use `patch.cfg` for default parameters.

- **arch:** Specify the computer architecture for which you want to acquire patches separated by a comma. Valid values for the arch parameters are given in the Vendor Feed Settings in the Configuration chapter in the *Radia Client Automation Enterprise User Guide*.
- **bulletins:** Specify the bulletins for acquisition separated by commas. The asterisk (*) wildcard character is recognized. This is the same as the bulletins parameter in `patch.cfg`. For Red Hat Security advisories, use a hyphen (-) in place of the colon (:) that appears in the Red Hat Security advisory number as issued by Red Hat.
 - Microsoft Security bulletins use the naming convention `MSYY-###`, where `YY` is the last two digits of the year that the bulletin was issued and `###` is a sequential number of the bulletin number being released for this the year specified. Microsoft service packs are listed in the format `MSSP_operatingsystem_spnumber`. To acquire *sample* Microsoft Operating System service packs, specify `MSSP*`. This will download sample service packs using information in the `novadigm` or `custom` folders. For example, specify `-bulletins MS00-001,MS00-029`.
 - Red Hat Security advisories are issued using the naming convention `RHSA-CCYY:###`, where `CC` indicates the century and `YY` the last to digits of the year when the advisory was issued, and `###` the Red Hat patch number. However, because the colon is a reserved character in Client Automation products, you must use a hyphen (-) in place of the colon (:) that appears in a Red Hat-issued Security advisory. Specify individual Red Hat Security advisories to Patch Management using the modified naming convention of `RHSA-CCYY-###`.
 - SuSE Security patches use the naming convention `SUSE-PATCH-####`, where `###` represents a numbering scheme provided by SuSE.

If you do not want to download any bulletins, use `-bulletins NONE`. You may want to do this when you want to only acquire agent updates.

- **config:** Use this parameter to append an alternate configuration file for acquisition to override settings in `patch.cfg`. The default is `patch.cfg`.
- **data_dir:** Specify the directory on the local computer (Patch Management Server) where you want the patches downloaded to before they are sent to your Configuration Server. Use this parameter to set where to store your patch descriptor files and patch data files in an alternate directory. The default is: `<InstallDir>\Data\PatchManager\data\patch`.
- **force:** Use force in the following situations.
 - You previously ran an acquisition using the mode `MODEL`, and now you want to use `BOTH`.
 - You previously ran an acquisition filtering for one language (`lang`), and now, you need to acquire bulletins for another.
 - You previously ran an acquisition specifying one product, and, now, you need to acquire for another.

For example, suppose that originally you only had Windows XP computers in your enterprise, so you used `-product {Windows XP*}`. A month later, you roll out Windows

Vista®. If you want to acquire the same bulletins, you will need to run the acquisition with `-product {Windows Vista*,Windows XP*}` and `-force y`.

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

- **mode:** Specify BOTH to download patches and the information about the patches. Specify MODEL to acquire only the metadata for patches. Only the Bulletins and Numbers for the patches are downloaded, but not the actual patch files. Use this mode so that you can use the reports to expose vulnerabilities on Agent devices. BOTH is the default.
- **product:** Specify which products you want to include in the acquisition in the format `vendor::product` in a comma separated list. Precede any products you want excluded with an exclamation point (!). If an include filter is not set, all products are assumed. If you provide any included filters, then the excluded filters will be a subset of the included products. Be sure to conform to the vendor's naming standards. For example, Microsoft refers to Internet Explorer using its full name, rather than a common abbreviation such as IE. For example, to include all Windows products except Windows 95, type `{Microsoft::Windows*,Microsoft::~!Windows 95}`.
By default, the following Microsoft products are excluded from patch acquisition and management:

```
!Windows 95,!Windows 98*,!Windows Me,!Access*,!Excel*,!FrontPage
200[023],!FrontPage
9[78-
],!InfoPath*,!Office*,!OneNote*,!Outlook*,!PowerPoint*,!Project
200[023],!Project 98,!Publisher*,!Visio*,!Word*,!Works*
```

The following products are in the exclusion list because they are not supported by Patch Management: Microsoft Windows 95, Windows 98, Windows Me and SuSE specific products `*-yast2`, `*-yast2-*`, and `*-liby2`.

If specifying a product for exclusion on the command line, surround the complete product string filters in quotes.

- **Replace:** Set `replace` to Y to delete old bulletins, specified in the `bulletins` parameter, and then re-acquire them. This will supersede the value for `force`. In other words, if you set `replace` to Y, then any bulletin specified for that acquisition will be deleted and reacquired, whether `force` is set to N or Y. The default is N.
- **superseded_patches:** Set `superseded_patches` to Y if you want to publish the data even if a patch is marked as superseded. The default is N.
- **vendors:** Specify the vendors to acquire patches from. Example: `-vendors Microsoft, RedHat, SuSE, HPUX, SOLARIS`. The default is Microsoft.
- **vendor_os_filter:** Specify a filter for the vendor's operating systems in the format `vendor::operatingsystem`. Red Hat and SUSE filters for x86_64 architectures use the format:
`vendor::operatingsystem-x86-64`.
SUSE 10 filters indicate a relevant service pack (SP1 or SP2) directly after the operating system, as in: `vendor::operatingsystemSP1-x86-64`.
 - RedHat examples:
`REDHAT::4es,REDHAT::4ws,REDHAT::4as;`
`REDHAT::4es-x86_64,REDHAT::4ws-x86_64,`
`REDHAT::5Server, REDHAT::5Client,REDHAT::6Server,REDHAT::6Client`

```
REDHAT::5Server-x86_64, REDHAT::5Client-x86_64, REDHAT::6Server-x86_64, REDHAT::6Client-x86_64
```

- SuSE examples: SUSE::8, SUSE::9, SUSE::10SP1-x86-64; SUSE::11; SUSE::11-x86_64
- Do not use `vendor_os_filter` to specify Microsoft operating systems as they are treated as products. Use the `product` filter for Microsoft operating systems instead.

Database Synchronization Parameters

To synchronize the databases from a command line:

- Run the following command line from the Patch Management directory:


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

`dsn` is a required parameter; `db_type` is also a required parameter when the database type is Oracle.

For example, if you only wanted to update the PRODUCT class for a SQL Server database, you would type:

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

If you wanted to update the PRODUCT class for an Oracle database, you would type:

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

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

The parameters are described below:

- **db_type**: Specify the database type. Valid values are `mssql` for Microsoft SQL Server and `oracle` for Oracle. The default is `mssql`. Specify this parameter (`-db_type oracle`) to synchronize with an Oracle database.
- **dsn**: Specify the Data Source Name (DSN) the Patch ODBC database. This parameter is required.
- **dsn_user**: Specify the user for the `dsn` for the Patch ODBC database.
- **dsn_pass**: Specify the password for the user of the Patch ODBC database.
- **host**: Specify the location of your Configuration Server in URL format. This parameter is required. Use the format `radia://ipaddress:port`
 - `radia` indicates the session type to be opened to the Configuration Server.
 - `ipaddress` is the hostname or IP address of the computer hosting the Configuration Server.
 - `port` is the port number of the Configuration Server.
- **class**: Specify the classes you wish to synchronize between the Configuration Server and the Patch SQL Database. For example, if you want to synchronize only the DEVICE class, specify `class="DEVICE"`. This parameter also accepts a wildcard. The default is `"**"` (synchronize all classes).

- **commit:** Specify 1 if you want to commit changes found in the Configuration Server database to the SQL database. Specify 0 if you do not want change automatically committed. You can view the changes. By default, all changes are committed.
- **rcs_pass:** If authentication has been enabled on your Configuration Server, specify the password for the rcs_user.
- **rcs_user:** If authentication has been enabled on your Configuration Server, specify the rcs_user.

Patch Agent Update Parameters

These settings are for the maintenance of the Patch Management Agent files. For more information on this, see the *View Agent Updates* section in the Operations chapter of the *Radia Client Automation Enterprise User Guide*. The following settings are configured in the Patch Agent section:

- **agent_updates:** Use Publish and Distribute to publish the updates to the PATCHMGR Domain and connect them to the DISCOVER_PATCH instance. This option will distribute the updates to your Patch Management managed devices. Use Publish only to publish the update, but not connect for distribution (deployment) to Patch Management managed devices.
- **agent_os:** Specify for which operating systems to acquire the agent updates. Valid values are win32, linux and suse.
- **agent_version:** Select which Patch Management versions you would like to acquire the agent updates for. You can only publish one version to one Configuration Server.

See the following sample `patch.cfg` file. Note the use of brackets for parameters and *forward slashes* in directory paths. If you are specifying any of these from a command line for acquisition, be sure to use quotes around values containing spaces.

```
patch::init {
  AGENT_UPDATES PUBLISH,DISTRIBUTE
  ARCH REDHAT::*,SUSE::*,HPUX::*,SOLARIS::*,MICROSOFT::x86
  CFG_VER 7.5
  DATA_DIR { C:/Program Files/Hewlett-
Packard/HPCA/Data/PatchManager/data}
  DSN PATCH
  DSN_USER sa
  FORCE no
  FTP_PASS {{AES256}vQP8q3G7N5j4iMhgA2QUuw==}
  HTTP_RETRIES 2
  LANGUAGE {}
  MODE both
  MODULE patch
  RCS_URL radia://localhost:3464
  RCS_USER RAD_MAST
  REPLACE no
  RETIRE {}
  SECTION all
  USING_DEFAULT_PATCH_CFG Y
  VENDOR_OS_FILTER {}
}
```


We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click [here](#).

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to radiadocfeedback@persistent.co.in.

Product name and version: Radia Client Automation Enterprise Patch Management, 9.00

Document title: Reference Guide

Feedback:

Reference Guide

We appreciate your feedback!
