IBM Endpoint Manager
Version 9.0

Patch Management for Windows User's Guide

IBM Endpoint Manager
Version 9.0

Patch Management for Windows User's Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 25.

This edition applies to version 9, release 0, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

IBM® Endpoint Manager Patch Management for Windows provides Fixlets for Microsoft security and non-security patches. Dashboards, wizards, and reports aid you in managing updates for various endpoint devices.

Since 1997, Endpoint Manager has been providing highly scalable, multi-platform, automated patch management solutions since 1997. Today, over 6 million computers around the globe rely on the Endpoint Manager Unified Management Platform to deploy critical updates to workstations, servers and other devices, regardless of location, running a wide variety of operating systems and applications.

Endpoint Manager deploys in days, not months, so you can realize business value by meeting compliance requirements, reducing organizational risk and containing costs.

Endpoint Manager leads the patch management market in terms of breadth of coverage, speed, automation, and cost effectiveness of its solution. The solution, which includes deploying a multi-purpose, lightweight Endpoint Manager agent to all endpoint devices, supports a wide variety of device types that range from workstations and servers to mobile and point-of-sale (POS) devices.

New Features

Patch Management for Windows is updated to include not only security support but also non-security support (critical updates and service packs) for the following products:

- Microsoft Office Family
- Microsoft Office Communications Server
- Microsoft Office Communicator
- Microsoft Office Live
- Microsoft Lync Server
- Microsoft Lync

For more information about the other supported products, see System Requirements.

Patch Management Overview

Patch Management for Windows creates Fixlets for the patches that Microsoft issues. The Endpoint Manager agent checks the registry, systems language, and other factors to determine if the patches are not installed or if an installed patch is corrupt. Notes® placed in the Fixlet® descriptions help Console Operators work around potential issues.

Endpoint Manager Patch Management for Windows keeps your Windows clients current with the latest security and non-security updates from Microsoft. Patch Management is available through the Enterprise Security Fixlet site from Endpoint Manager.

For each new patch issued by Microsoft, IBM Endpoint Manager releases a Fixlet that identifies and remediates all the computers in your enterprise that need it. With a few keystrokes, the Endpoint Manager Console Operator can apply the patch to all relevant computers and view its progress as it deploys throughout the network.

The Endpoint Manager agent checks the registry, file versions, the systems language, and other factors to determine if a patch is necessary. Fixlets for Windows patches are divided into two main classes:

The patch has not been installed.
These Fixlets check a combination of the Windows registry and the Windows file system to determine whether or not a patch is applicable.

An installed patch is corrupt.
These Fixlets check the registry and each file installed by the patch. If any of the files are older than the version installed by the patch, the Console Operator is notified. A Fixlet describes the nature of the vulnerability and you can then re-apply the patch.

With this dual approach, you can differentiate between unpatched computers and those that have regressed due to installation of an earlier version of the application or service pack.

Endpoint Manager tests each Fixlet before it is released. This testing process often reveals issues that are addressed by attaching extra notes to the Fixlet. The Console Operator can use these notes to work around the problem, adding extra value to the patching process. Endpoint Manager incorporates also user feedback into notes.

Examples of notes include:

- **Note:** An Administrative Logon is required for this IE patch to complete upon reboot.
- **Note:** Affected computers might report back as 'Pending Restart' when the update has run successfully, but do not report back their final status until the computer has been restarted.
- **Note:** To deploy this Fixlet, ensure that Windows Update service is not disabled.
- **Note:** Microsoft has announced that this update might be included in a future service pack or update rollup.

System requirements

Endpoint Manager supports security and non-security updates for Microsoft operating systems.

Endpoint Manager provides Windows security updates, critical updates, and service packs on the operating systems listed in the table.

Table 1. Supported operating systems and update types

Supported OS	**Type of Update Supported**		
	Security update	Non-security update	
Office Family		Critical Update	Service Pack
Microsoft Office 2013	*	*	*
Microsoft Office 2010	*	*	*
Microsoft Office 2007	*	*	*

Table 1. Supported operating systems and update types (continued)

Supported OS	Type of Update Supported		
Microsoft Office 2003	*	*	*
Microsoft Office 2002 XP	*	*	*
Windows Family			
Windows 8	*	*	*
Windows 7	*	*	*
Windows XP	*	*	*
Windows XP x64 Edition	*	*	*
Windows Server 2012	*	*	*
Windows Server 2008 R2	*	*	*
Windows Server 2008	*	*	*
Windows Server 2003 Datacenter	*	*	*
Windows Server 2003	*	*	*
Windows 2003 Standard	*	*	*
Windows 2003 Web Edition (x86 and x64)	*	*	*
Windows 2000*	*	*	*
Windows 2000 Professional	*	*	*
Windows 2000 Server	*	*	*
Windows 2000 Datacenter Server	*	*	*
Windows 2000 Advanced Server	*	*	*
Windows NT Workstation	*	*	*
Windows Vista	*	*	*
Windows XP Professional	*	*	*
Windows Home Edition	*	*	*
Embedded Family			
Windows XP Embedded	*	*	*
Windows Embedded POSReady 7	*	*	*

Note: Microsoft Windows 2000, including all its editions such as Windows 2000 Professional, Windows 2000 Server, Windows Server 2000 Datacenter, and Windows 2000 Advanced Server, has reached its end of life (EOL). Microsoft no longer supports and releases updates for these products.

Note: For additional information about patching Microsoft Office and other Windows applications, see the Patch Management for Windows Applications Updates User Guide.

Other languages supported

Patch Management has Fixlets sites for the different Windows language versions that it supports. If you are using the Evaluation version, you can download the Masthead of particular language sites.

In addition to English Patch Management for Windows supports other international versions of Windows. Each language has its own Fixlet site. These languages include:

Table 2. Other languages supported by Patch Management for Windows

Brazilian Portuguese	Japanese
Czech	Korean
Danish	Norwegian
Dutch	Polish
Finnish	Russian
French	Spanish
German	Simplified Chinese
Greek	Swedish
Hebrew	Traditional Chinese
Hungarian	Turkish
Italian	

When you purchase a Production version of Tivoli Endpoint Manager for these languages, you automatically receive the corresponding version of Patch Management. Otherwise, if you are working with an Evaluation version of the program, you can download the appropriate Masthead for these sites from the Tivoli Endpoint Manager support website at http://support.Tivoli Endpoint Manager.com.

Chapter 2. Patch Management for Windows

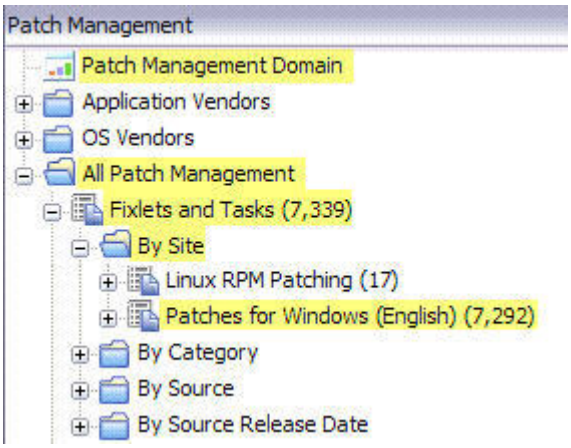
You can manage Fixlets using dashboards, reports, and wizards. You can deploy, fix, and uninstall Fixlets. You can also view the breakdown of Fixlets available or needed in your deployment.

Patch using Fixlets

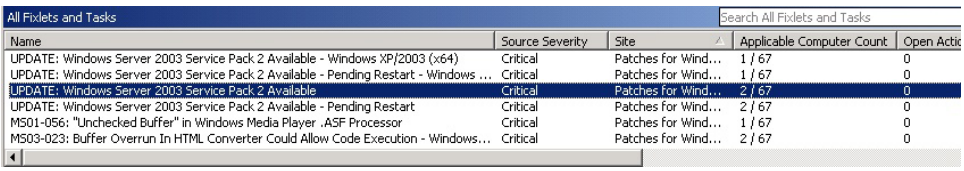
From the console, you can select the action for the appropriate Fixlets that you want to deploy. The action propagates across your deployment. Patches are applied based on the settings that you make in the Fixlet work area and the Take Action dialog.

Follow these steps to deploy patches from the Endpoint Manager Console by using Fixlets.

1. From the All Patch Management navigation tree, click **Fixlets and Tasks** > **By Site** > **External Sites**.
2. Select the site. In the following image, the Patches for Windows (English) site is selected.



3. In the content that is displayed in the list panel, click the Fixlet that you want to deploy.



4. The Fixlet opens in the work area. Click the tabs at the top of the window to review details of the Fixlet.
5. Click **Take Action** to deploy the Fixlet. You can also click the appropriate link in the Actions box.
6. Optional: You can set more parameters in the Take Action dialog.

   For detailed information about setting parameters with the Take Action dialog, see the IBM Endpoint Manager Console Operators Guide.
7. Click **OK**.

Note: In some cases, you must enter your Private Key Password after you click **OK**.

The action propagates across your network, installing the designated patch on the computers that you specified and according to the schedule that you selected. You can monitor and graph the results of this action to see exactly which computers were remediated to ensure compliance.

Patches for Windows Overview dashboard

Use the Patches for Windows Overview Dashboard to view the breakdown of security and non-security patches that are needed in your deployment.

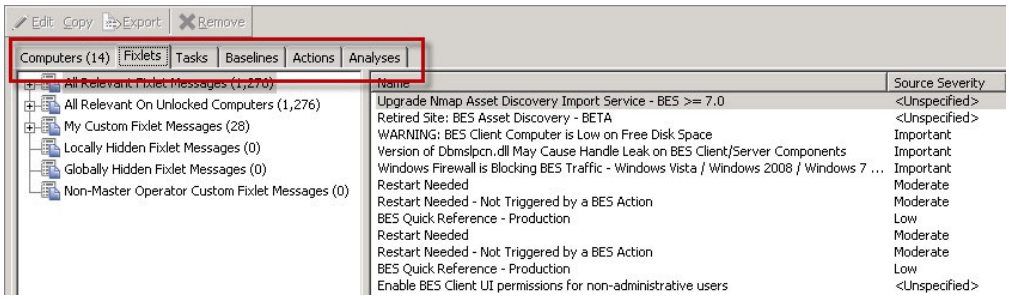
The Patches for Windows Overview dashboard displays a summary of patch information in your deployment using tables, graphs, and pie charts. From the **Patch Management** domain, click **OS Vendors** > **Microsoft Windows** > **Reports** > **Patches for Windows Overview**.

The report has three tabs:

- Patches for Windows Overview
- Security Patches Overview
- Non-Security Patches Overview

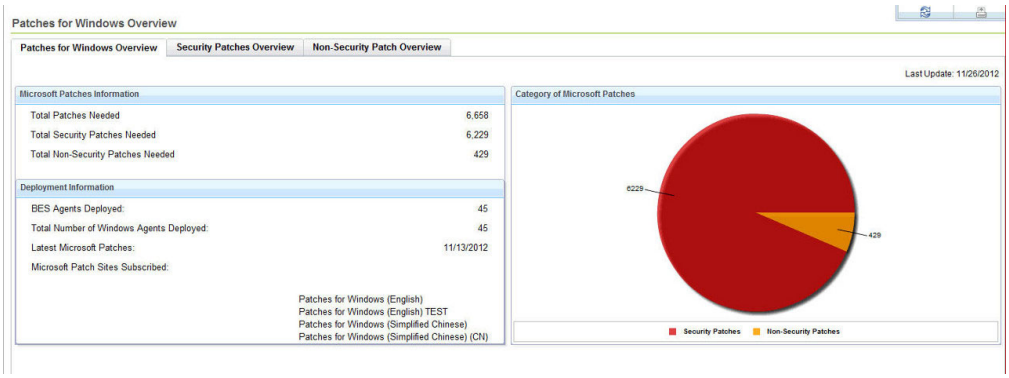
You can change how your data displays in the overview from the legend in the upper-right corner of each graph. Content can be viewed in a column chart, pie chart, or data table.

The Security Patches Overview and Non-Security Patch Overview tabs have a different link for computers that need at least one patch. The Security Patches Overview tab has the *Computers Needing at least one Critical Patch*; the Non-Security Patches Overview tab has the *Computers Needing at least one Non-Security Patch* link. Both links open a Fixlet list window where you can view the relevant Fixlets, Computers, Tasks, Baselines, Actions, and Analyses.



Patches for Windows Overview tab

The Patches for Windows Overview tab displays Microsoft patch information, deployment information, and a chart that displays the category of patches.



The Patch for Windows Overview tab provides a quick summary of your Windows remediation. It shows the Microsoft Patches Information and the Deployment Information. The Microsoft Patches information includes the number of patches and the number of Security and Non-Security patches that the deployment needs.

The tab also includes a Patch Needed chart that shows the breakdown of the computers that need patches, which is based on the following categories:

- Security Patches Needed only
- Non-Security Patches Needed only
- Both Security and Non-Security Patches Needed
- No Patch Needed

Security Patches Overview tab

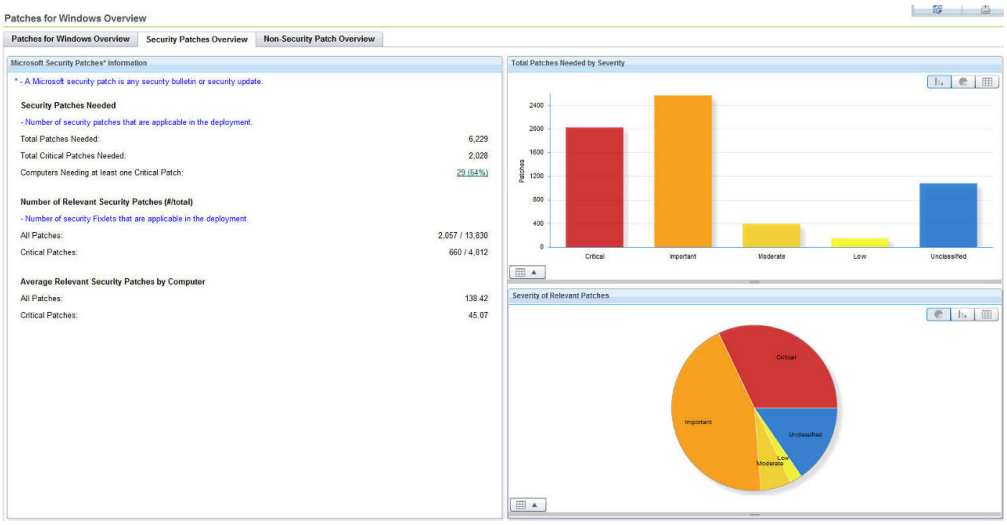
A Microsoft security patch refers to any bulletin or update that is related to a security vulnerability. The Security Patches Overview tab has bar charts and the Microsoft Security Patches Information section, which provides patch information that is divided into the following headings:

Security Patches Needed
: Shows the number of security patches that are applicable in the deployment. It lists the Total Patches Needed and the Total Critical Patches Needed. Total Patches Needed refers to the total number of patches for all Tivoli Endpoint Manager clients, including critical, important, low, and unclassified patches. The section also shows the number and percentage of computers that need at least one critical patch.

Number of Relevant Security Patches
: Shows the number of security Fixlets that are applicable in the deployment. It displays the number of all patches relevant in the deployment and the total number of security Fixlets.

Average Relevant Security Patches per Computer
: Shows the average number of all the relevant patches and the critical patches for every computer.

The Security Patches Overview tab has bar charts of total patches that are needed by severity: critical, important, moderate, low, and unclassified. Another bar chart displays the severity of relevant patches.

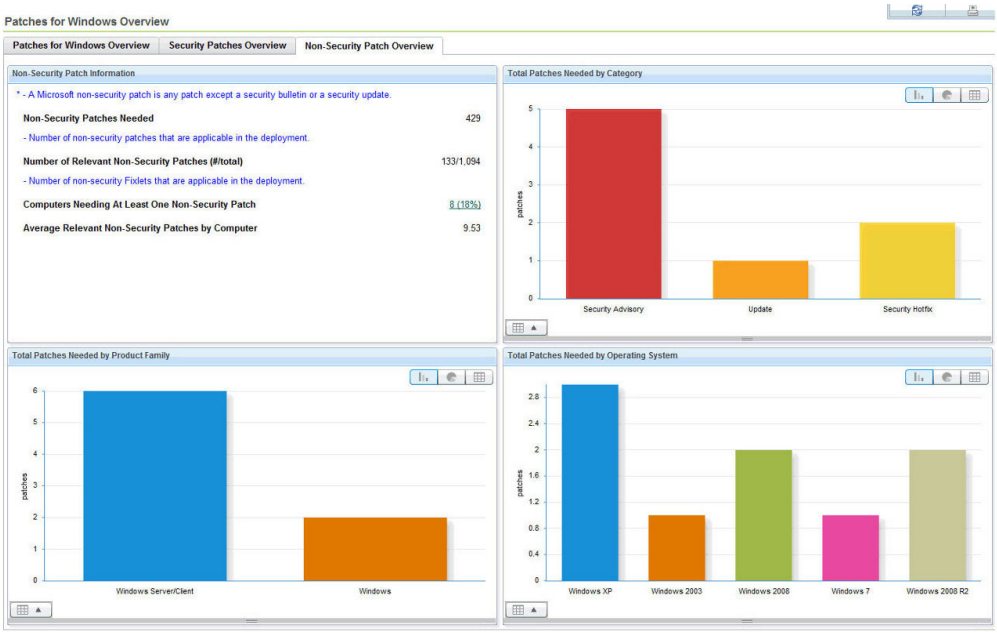


Non-Security Patches Overview tab

The Non-Security Patches Overview tab shows a summary of Microsoft Patch Information. Patch information is broken down to show the following information:

- *Total Patches Needed*
- The date of the *Latest Microsoft Patches*
- The number of relevant patches
- The number and percentage of *Computers Needing at least one Patch* link
- The *Average Relevant Patches per Computer*

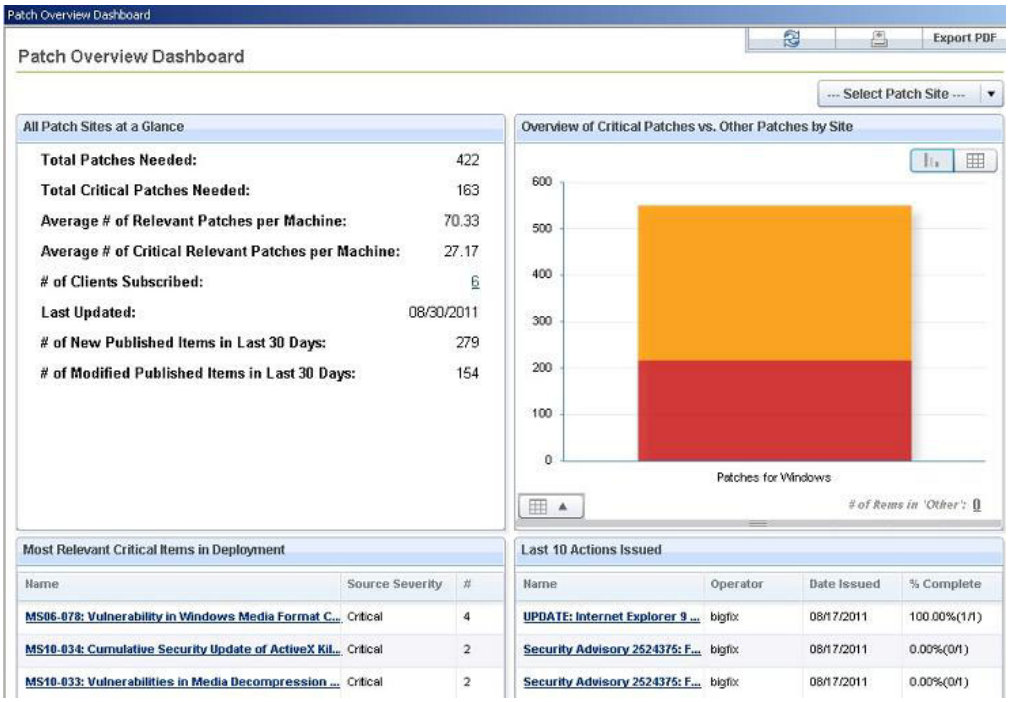
The tab also has a chart that categorizes the total patches that are needed according to product family, category, and operating system.



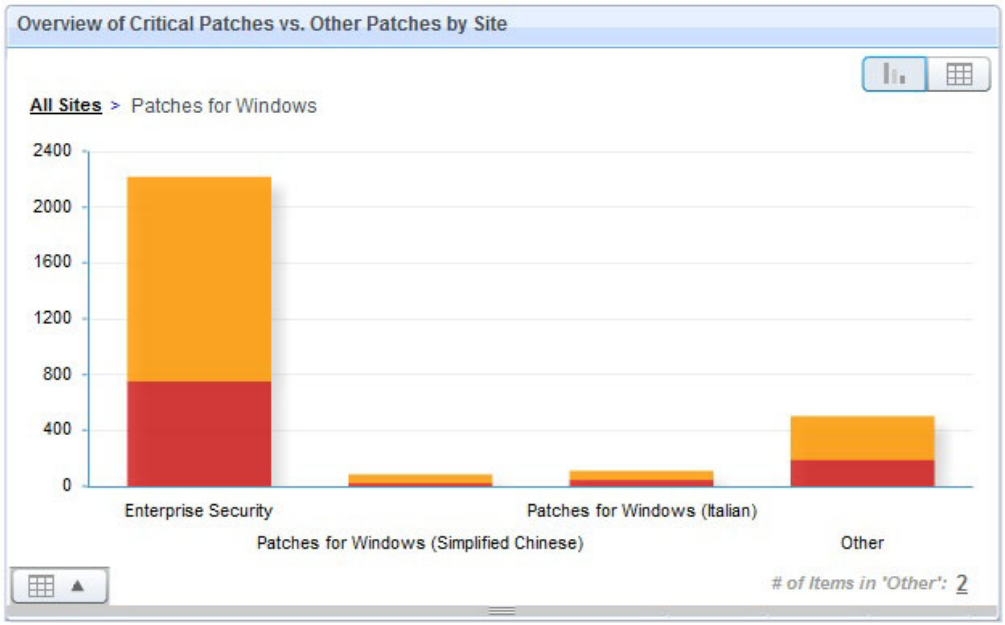
Patch Overview dashboard

View patch site information in your deployment including the most relevant items in deployment and comparisons of critical patches against other patches by site. The dashboard shows all the patches in your deployment, not just those for Windows. Set view options to see the last 10 actions done for every site.

The Patches Overview dashboard displays a summary of patch information in your deployment using tables and graphs for all Tivoli Endpoint Manager patch solutions, not just the statistics for Patches for Windows. The dashboard is located at the top of the Patch Management navigation tree and opens when you click the Patch Management node for the first time.



Click on the bar graph to the right to open a datagrid, with the various sites listed, which you can click to get a more in-depth view of the site. Patches for Windows is organized into one bar graph for each international Windows Patch site subscribed.



The number of items in “Other” determines how many sites can be viewed at the same time, and you can change this value.

For any given section of the dashboard, there are general statistics about the total number of patches, the number of clients subscribed, the most relevant critical items in deployment for that site, and the last 10 actions issued in the site.

Uninstalling patches

Enter the Microsoft Knowledge Base (KB) number in the Rollback Task Wizard to uninstall patches.

You can remove certain patches by using the *Microsoft Patch Rollback Task Wizard*. You need the Microsoft KB number to identify the applicable patch. There might be some patches that require uninstallation without using *Microsoft Patch Rollback Task Wizard*

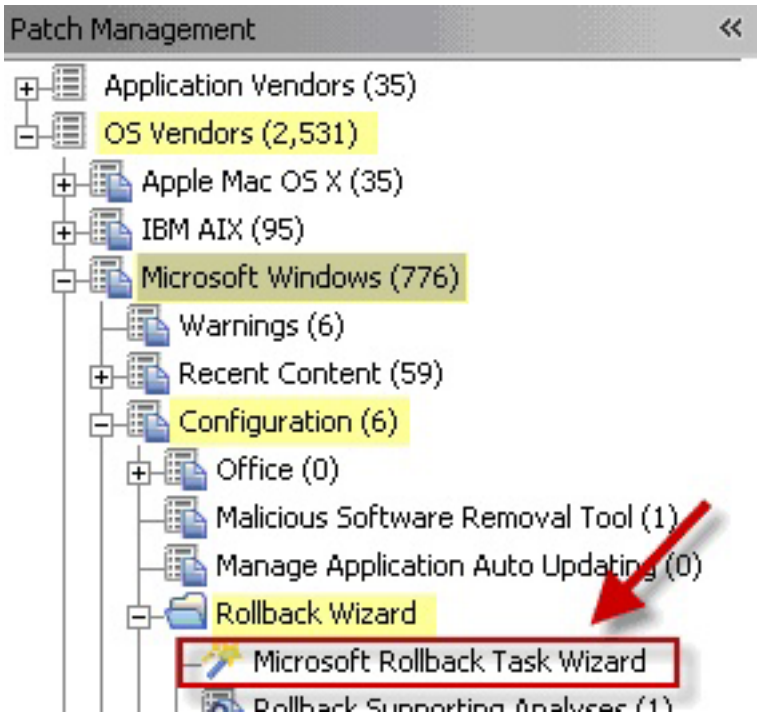
Using the Rollback Task wizard

Uninstall Microsoft patches with the Rollback Task Wizard.

Use the Patch and Update Rollback Information Analysis to know the Microsoft KB number of the patch that you need to install.

Use these steps to uninstall patches that can be uninstalled with the Microsoft Patch Rollback Task Wizard.

1. From the Patch Management navigation tree, click the OS Vendors site.
2. Click **Microsoft Windows** > **Configuration** > **Rollback Wizard** > **Microsoft Rollback Task Wizard**. The Wizard window opens.



3. Enter the Knowledge Base (KB) number of the patch in the designated field.

   The Task Wizard and Analysis looks for Microsoft KB in the following locations in the Windows Registry:

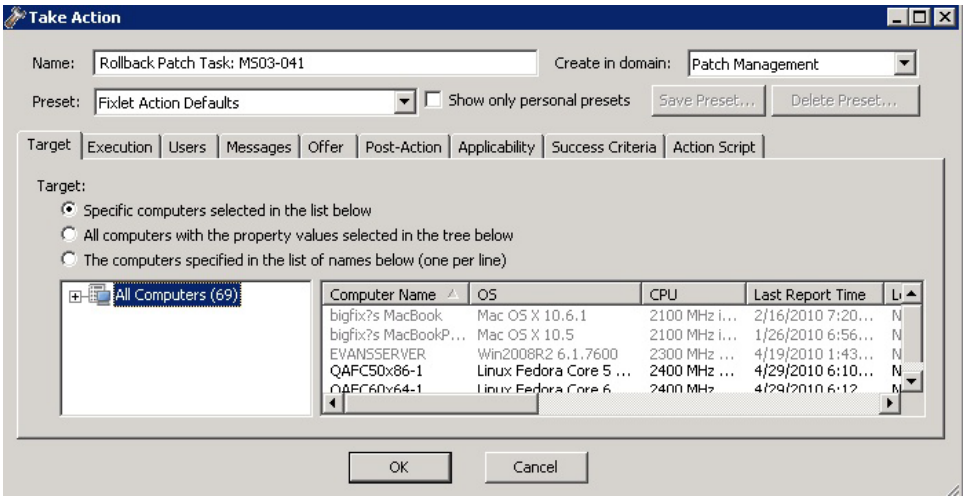
   For Windows XP/2003 and earlier

   in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\key`. The key must be the KB number for the patch you want to roll back.

   For Windows Vista and later

   The Microsoft KB number is embedded in the key names in the Windows Registry location: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ComponentBased Servicing\Packages\`.

4. Select the operating system.
5. Optional: Click the check box to create a one-time action. Leave this unchecked if you want to create a Fixlet.
6. Click **Finish**. The **Take Action** dialog opens.
7. Optional: You can set additional parameters in the Take Action dialog.



8. Click OK to start the action.
9. Enter your Private Key Password.

It is strongly recommended that you test the success of the rollback to avoid restarting machines that might fail to roll back.

Troubleshooting uninstallation of patches

You can troubleshoot patches that do not uninstall using the Rollback Task Wizard using different methods.

Some Windows patches require different steps for uninstallation other than using the Rollback Task Wizard. Rollback might fail because of the following reasons:

- A patch cannot be uninstalled.
- The method the Rollback Task Wizard uses to generate an uninstall command might not work for the patch.

Use the following ways to uninstall patches:

- The task might report back as completed on Windows Vista and later even when it failed. Check that the task is no longer relevant to ensure success of the rollback.
- If the task fails, make sure that the patch can be uninstalled from the Control Panel, using **Programs and Features** if you are using the Classic View or **Uninstall a program** under the **Programs** category.
- If the task fails on Windows Vista or Windows 2008, manually generate the `assemblyidentity` tag and command to uninstall. For more information about using Method 2: Use the Command Line of the Microsoft KB Article 940410, see Microsoft Support page.

Note: It is not advisable to deploy a generated Patch Rollback Task as part of a multiple action group because rollback tasks are more likely to fail.

Fixing Corrupt Patches

Use the Corrupt Fixlet Wizard to fix multiple corrupt Fixlets and to create Fixlet copies or baselines without rebooting.

Corrupt patches are one of two major classifications of Fixlet messages for Microsoft. To learn more about the main classes of Fixlets for Windows patches, see “Patch Management Overview” on page 1.

You get a Fixlet message when any of the files have an earlier file version than the version installed by the patch. The Fixlet message notifies you that the patch has been installed, but that not all the files are up-to-date, so you might not be secured against the vulnerability. You can then re-apply the patch using the Fixlet.

This two-step approach works gives you more information about why a patch is needed. This is better than an approach where you are simply informed that you have not installed the patch. For example, when you apply a patch to a group of computers, then later notice that Tivoli Endpoint Manager displays that some computers have "corrupted patches", you will know that something has overwritten some of the files. This usually occurs if you install another application or an earlier service pack that overwrites the newer files.

Note: The Tivoli Endpoint Manager Client continuously checks both the registry and file versions using extremely few computer resources, giving you get the benefit of continuous monitoring without having a large CPU, memory, hard disk, or bandwidth cost.

Corrupt patches can be difficult to correct in a baseline because of their requirement to reboot after application. If testing in your environment has established sequences of corrupt patches that can be safely applied without reboot, you can use the Corrupt Patch Deployment Wizard in the Patching Support site. Use this wizard to create Fixlet copies or baselines without rebooting.

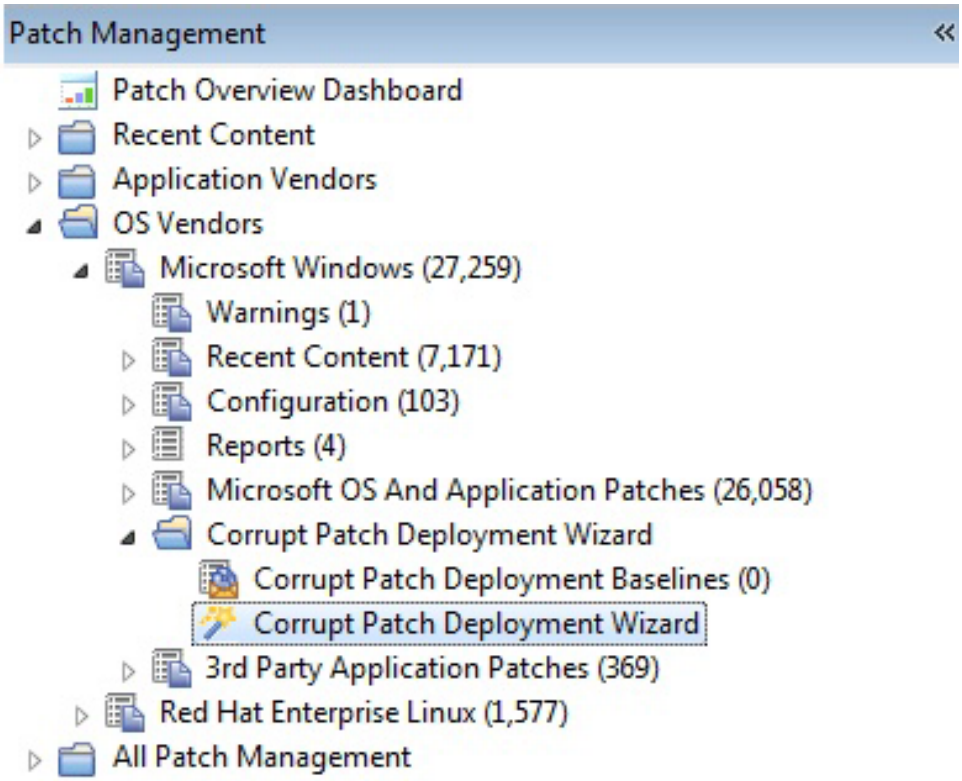
If a machine has multiple corrupt Fixlets that are applicable, you can apply them all at the same time by using the Corrupt Fixlet Deployment Wizard.

Using the Corrupt Patch Deployment wizard

Use the Corrupt Patch Deployment Wizard to fix corrupt Fixlets by using Fixlet copies or existing baselines.

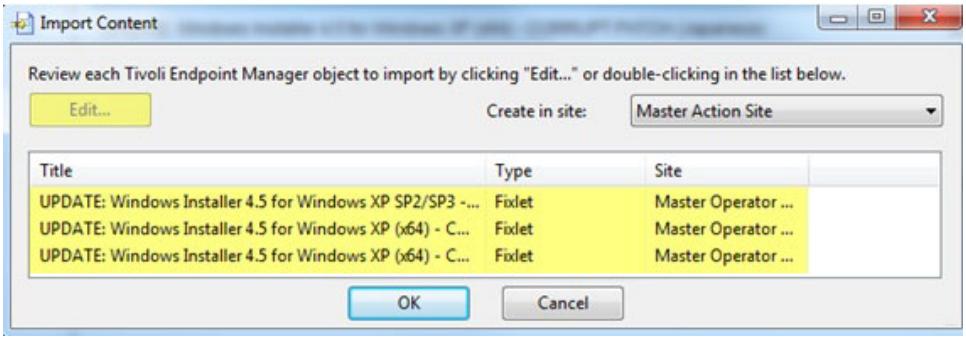
Follow these steps to fix corrupt patches using the Corrupt Patch Deployment Wizard.

1. From the Patch Management navigation tree, click OS Vendors.
2. Click **Microsoft Windows** > **Corrupt Patch Deployment Wizard** > **Corrupt Patch Deployment Wizard**. The Wizard opens.



3. Identify the applicable corrupt Fixlets. You can do one of the following actions:
   - Choose among the Patch for Windows corrupt patches.
   - Select a baseline that has corrupt Fixlets in it.
   - Copy and paste corrupt Fixlets from a console view.

4. You can either select output as a series of custom Fixlets or as a baseline.
5. Review the Fixlets.
6. Click **OK**.



The content that is created is placed in the Patch Domain, under the All Patch Management mode. To view the content, from the Patch Management navigation tree, click **Content** > **Custom Content**.

Patch Microsoft Office

You can deploy Microsoft office updates and patches using Administrative, Network, and Local installation.

Updates to Microsoft Office might require that installation or source files be present for the update to complete successfully. To meet this need, Tivoli Endpoint Manager provides different ways to deploy Microsoft Office updates and patches:

- Administrative
- Network
- Local

You can configure Tivoli Endpoint Manager clients to use one of these methods by using the Office Deployment Control tasks in the BES Support site.

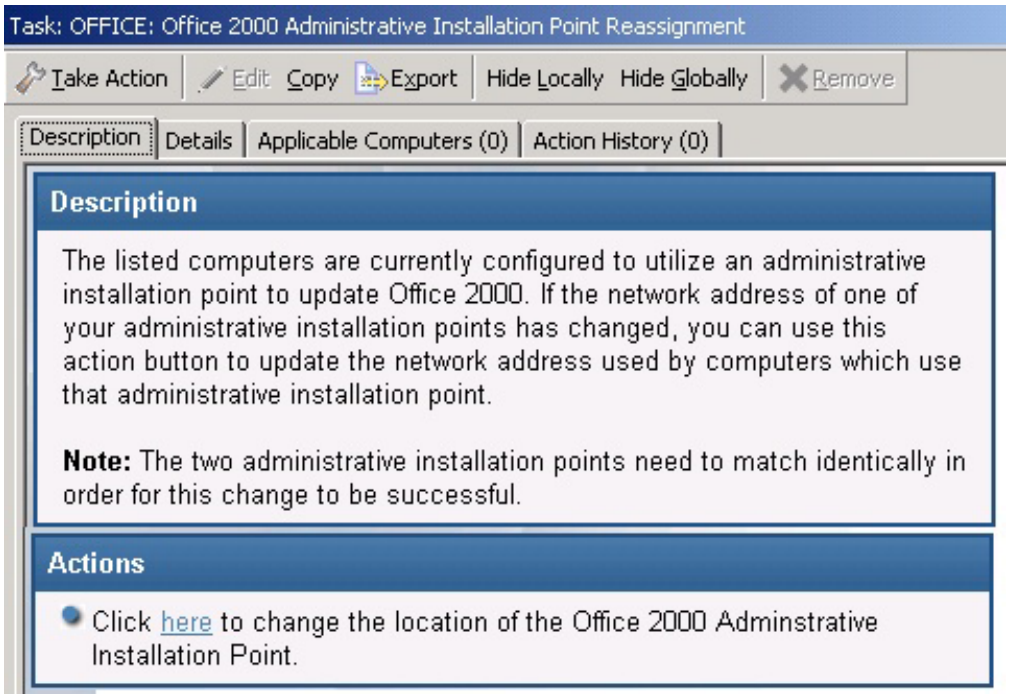
Note: The deployment of updates and patches using *Administrative*, *Network*, and *Local* ways apply to Microsoft Office versions earlier than Microsoft Office 2007.

Administrative Installation

Follow best practices to ensure successful deployment of Microsoft Office updates using the administrative installation.

The Administrative Installation method uses Microsoft Office Administrative Installation Points to provide Office updates. The following caveats apply to this installation method:

- The Office product being patched must point to the correct administrative installation point, and this administration point must match the product being patched. For example, an Office 2000 Standard installation cannot point to an Office 2000 Professional administrative point. Click the *OS Vendors* site in the navigation tree, and then click *Microsoft Office* and *Configuration.*



- Only one Office product can be present on the computer. However, multiple installations of different Office versions also works. For example, Office 2000 Small Business and Office 2000 Professional is not supported, but Office 2000 Small Business and Office XP Professional is.
- The patch must be correctly applied to the administrative point before deploying the action.
- The administrative point must be shared, with *read permission* given to ANONYMOUS LOGON, NETWORK, or EVERYONE on a Windows NT, Windows 2000, Windows XP, Windows 2003, or Windows 7 system.
- Null session must be enabled for the share. For more information, see Creating a Null Session Share.

Network Installation

Follow best practices to ensure the successful deployment of Microsoft Office updates using network installation.

The Network Installation method uses a network-shared location containing the Office installation media or source files. The following caveats apply to this installation method:

- When deploying the action, you must supply a valid UNC path (\\server_name\share_name) to the appropriate Office setup files. The shared setup files must match the product being patched; an Office 2000 Standard installation cannot be patched by providing the Office 2000 Professional setup files.
- For Office 2000, only one Office product can be installed on the computer, however multiple installations of different Office versions will work. For example, Office 2000 Small Business and Office 2000 Professional is not supported, whereas Office 2000 Small Business and Office XP Professional is supported – see previous section.

- The Office setup files must be shared with *read permission* given to ANONYMOUS LOGON, NETWORK, or EVERYONE on a Windows NT, Windows 2000, Windows XP, or Windows 2003 system.
- Null session must be enabled for the share. For more information about enabling a null session, see Creating a Null Session Share.

Local Installation

Follow best practices to ensure successful deployment of Microsoft Office updates using local installation.

The Local Installation method uses source Office installation media or source files that are installed locally on every computer to be updated. The following caveats apply to this installation method:

- Before performing Action, the appropriate Office CD must be placed in the local CD-ROM drive of each computer you want to update. The CD provided must match the product being patched; the Office 2000 Standard installation cannot be patched by using the Office 2000 Professional CD.
- The CD-ROM drive must be recognized by the operating system.

Appendix A. Frequently asked questions

Learn the answers to frequently asked questions.

Where are my dashboards located in the Tivoli Endpoint Manager Console?

The updated Tivoli Endpoint Manager Console contains the same content as the previous version, although some content might have moved to a different location.

The following list shows the contents and their locations:

- The Patches Overview dashboard is in the Patch Management domain, on the upper part of the page.
- The Patch Overview Dashboard is in under **All Patch Management**, Alternatively, you can also find the dashboard under the **Patch Support** site.
- Some dashboards are located under **OS Vendors** > **Microsoft Windows**.

What do I do if a patch fails to install?

If a patch fails to install, there are several things that you can try:

- Determine if you have applied the patch to the correct computers.
- Try running the patch manually by downloading it from the Microsoft website.
- Review Windows updates.
- Look at the Microsoft Baseline Security Analyzer (MBSA) to see that the tool considers the patch to be applicable.

If the patch still fails to install, contact IBM Software Support.

Why does a patch fail, but complete successfully?

Sometimes under specific circumstances, a patch is successfully applied but the relevance conditions indicate that it is still needed. Check to see if there are any special circumstances associated with the patch, or contact IBM Software Support.

Why is there no default action?

There are various reasons for why there is no default action. Sometimes a Fixlet or a patch might have catastrophic consequences. It is highly suggested that you test the Fixlet on a test bed you apply the Fixlet or patch. There might also be multiple actions with the Fixlet, none of which are clearly suggested over other actions. *It is highly suggested that you read the Description text in the Fixlet before you start the action.*

What does "*Manual Caching Required*" mean?

In some instances, a particular vendor might not be providing a download directly to their link. In this case, click through that vendor's End User License Agreement and manually download it to your Tivoli Endpoint Manager server.

What are Corrupt Patches and how are they used?

Corrupt patches in Windows are when Tivoli Endpoint Manager detects that a patch looks like it began running but did not complete. These patches become

relevant to indicate that something is wrong with the security patch. To remediate, take the appropriate action to reapply the patch.

What are superseded patches?

Superseded patches are earlier versions of patches that no longer need to be applied.

How do I deal with missing patches?

Tivoli Endpoint Manager does not provide Fixlets for every patch that Microsoft offers. For more information, see the related FAQ entry on the types of patches that are supported by Tivoli Endpoint Manager. You can also contact IBM Software Support.

What are non-security updates?

Non-security updates are all updates except security updates. Non-security updates include critical updates, service packs, and update rollups. Tivoli Endpoint Manager supports critical updates and service packs. For more information about the types of updates that are supported by Tivoli Endpoint Manager, see the wiki article on Supported OS.

What types of patches are supported by Tivoli Endpoint Manager?

Tivoli Endpoint Manager supports security and non-security updates. Non-security updates include critical updates and service packs. For more information about the types of updates that are supported by Tivoli Endpoint Manager, see the wiki article on Supported OS.

What does 'Known Issue' mean?

A 'Known Issue' is a term that is used by Microsoft in the KB articles. You are advised to refer closely to details of known issues that are indicated in the KB articles.

Are hotfixes supported by Tivoli Endoint Manager?

Hot fixes are not supported. Customers are advised to contact IBM Software Support for critical hot fix requests.

What is an audit Fixlet?

A Tivoli Endpoint Manager audit Fixlet is a Fixlet that does not have an action script that is associated with it. An audit Fixlet does not change anything; it just alerts you about an issue. Audit Fixlets do not have action scripts; they require manual intervention. For example, an audit Fixlet might become available regarding a software patch upgrade where you must manually install the patch.

Does Patch Management for Windows still support Microsoft products that reach their end of life?

Microsoft no longer releases updates for Microsoft products that reach their end of life (EOL). Patch Management for Windows also no longer releases new content for Microsoft products that reach their end of life. One example is Microsoft Windows

2000 and all its editions. These editions include Windows 2000 Professional, Windows 2000 Server, Windows Server 2000 Datacenter, and Windows 2000 Advanced Server.

Appendix B. Support

For more information about this product, see the following resources:

- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the “Web at Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Printed in USA