Tivoli.

Patch Management for Windows

User's Guide

IBM

Note: Before using this information and the product it supports, read the information in Notices.

Contents

Part One

Introduction

BigFix has provided highly scalable, multi-platform, automated patch management solutions since 1997. Today, over six million computers around the globe rely on the BigFix 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. BigFix deploys in days—not months—allowing you to realize business value by meeting compliance requirements, reducing organizational risk and containing costs.

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

How Patch Management for Windows works

BigFix Patch Management *for Windows* keeps your Windows Clients current with the latest security updates from Microsoft. Patch Management is available through the Enterprise Security Fixlet site from BigFix. For each new patch issued by Microsoft, BigFix releases a Fixlet that can identify and remediate all the computers in your enterprise that need it. With a few keystrokes, the BigFix Console Operator can apply the patch to all relevant computers and view its progress as it deploys throughout the network.

The BigFix agent checks the registry, file versions, the language of the system, and other factors to determine if a patch is necessary. There are two main classes of Fixlets for Windows patches:

- ***The patch has not been installed.*** These Fixlets check the registry to determine whether or not a patch has been previously installed.

- ***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 explains the nature of the vulnerability and then allows you to re-apply the patch.

This dual approach allows you to differentiate between unpatched computers and those that have regressed due to installation of an older application or service pack.

BigFix tests each Fixlet in its lab before it is released. This testing process often reveals issues that are addressed by attaching extra “notes” to the Fixlet. These notes allow the Console Operator to work around the problem, adding extra value to the patching process. BigFix also incorporates user feedback into notes.

Some examples include:

- **Note:** The default IE upgrade package will force affected computers to restart.
- **Note:** An Administrative Logon is required for this IE patch to complete upon reboot.
- **Note:** Do NOT install MDAC 2.7 on computers that are part of a Windows cluster.
- **Note:** BigFix has received feedback of a potential issue with this patch. Application of this patch without restarting the patched computer may cause Acrobat 5.0 (but not 6.0) to crash until the computer is restarted. You may wish to consider deploying this patch with a restart command.

System Requirements

BigFix provides coverage for Windows updates on the following operating systems and applications:

Operating Systems

- Apple Mac OS X
- HP-UX
- IBM AIX
- Novell SUSE Linux
- Red Hat Enterprise Linux
- Sun Solaris
- VMware ESX
- zLinux
- Windows ME
- Windows NT Workstation 4.0, Server 4.0, Server 4.0 Enterprise Edition, Server 4.0 Terminal Server Edition
- Windows 2000 Professional, Server, Datacenter Server, Advanced Server
- Windows XP Professional, Home Edition
- Windows Server 2003 Datacenter Edition, Server 2003 Enterprise Edition, Standard Edition, Web Edition (x86 and x64)
- Windows Vista Home, Home Premium, Business, Ultimate and Enterprise (x86 and x64)
- Windows 7

Microsoft Applications

- Office
- IIS
- FrontPage
- Internet Explorer
- MSDE
- SQL Server
- Visual Basic
- Messenger

> ***Note:*** *See additional information below about patching Microsoft Office and other Windows applications.*

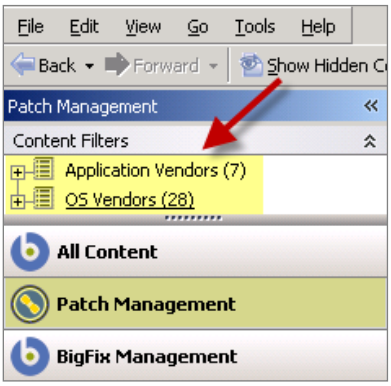
Other Applications

- Adobe Acrobat
- Adobe Reader
- Apple iTunes
- Apple QuickTime
- Adobe Flash Player
- Adobe Shockwave Player
- Mozilla Firefox
- RealPlayer
- Skype
- Oracle Java Runtime Environment
- WinAmp
- WinZip

Navigate Patch Management in the BigFix Console

The navigation tree in the BigFix Console, which is available for all BigFix products, serves as your central command for all Patch Management functions. The navigation tree gives you easy access to all reports, wizards, Fixlets, analyses and tasks related to the available updates and service packs for the computers in your network.

The content in the Patch Management "domain" is organized into two separate "sites" – *Application Vendors* and *OS Vendors*.



Components

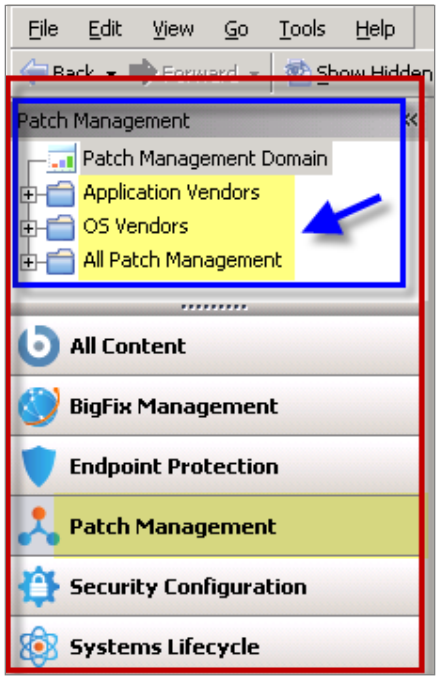
The BigFix Console organizes content into four parts:

- *Domain Panel – Includes the navigation tree and a list of all domains*
- *Navigation Tree – Includes a list of nodes and subnodes containing site content*
- *List Panel – Contains a list of tasks and Fixlets*
- *Work Area – Work window where Fixlets and dialogs display*

In the context of the BigFix Console, products or *sites* are grouped by categories or *domains*. The domain panel is the area on the left side of the Console that includes a navigation tree and a list of all domains. The navigation tree includes a list of nodes and sub-nodes containing site content.

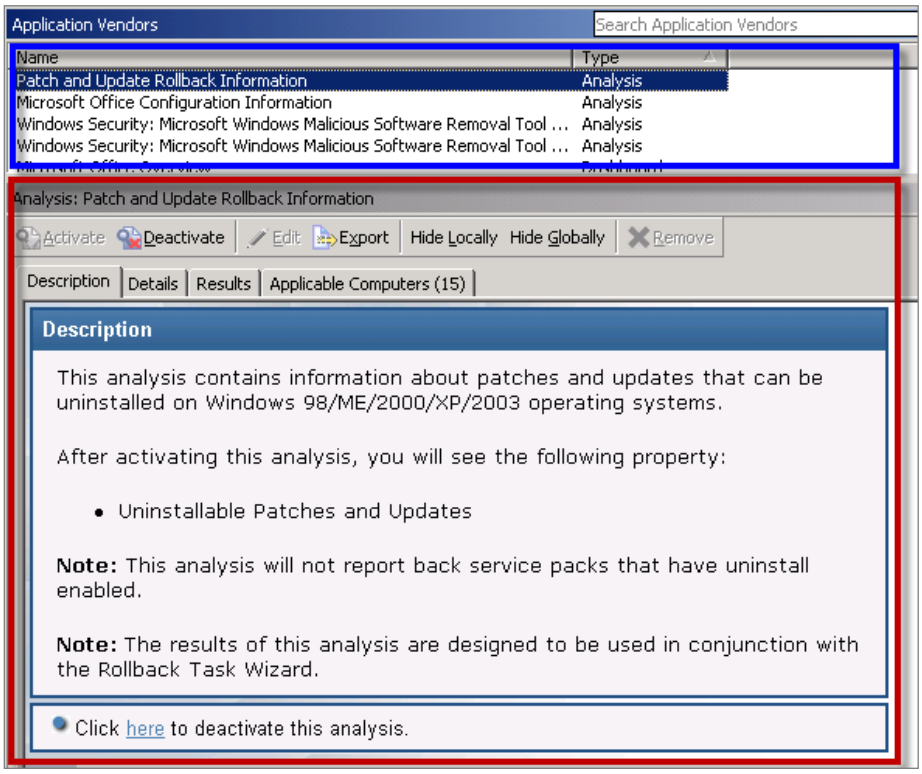
In the image below, the red-outlined area represents the entire Domain Panel, and the blue box contains just the Navigation Tree. The Patch Management domain button is listed at the bottom – use this domain to access Patch Management content.

The Patch Management navigation tree includes three primary "nodes" that each expand to reveal additional content. The top two nodes – *Application Vendors* and *OS Vendors*, expand to include Fixlets, tasks and other content related specifically to either applications or operating systems. The third node – *All Patch Management,* expands to include content that is collectively related to the entire Patch Management domain.



Patch Management tasks are sorted through upper and lower task windows, located on the right side of the Console. The upper panel, called the *List Panel* (blue), contains columns that sort data according to type, such as Name, Source Severity, Site, Applicable Computer Count, and so on.

The lower panel or *Work Area* (red) presents the Fixlet, task screen or Wizard from which you are directed to take specific actions to customize the content in your deployment.

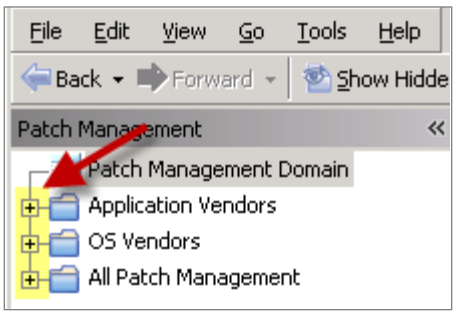


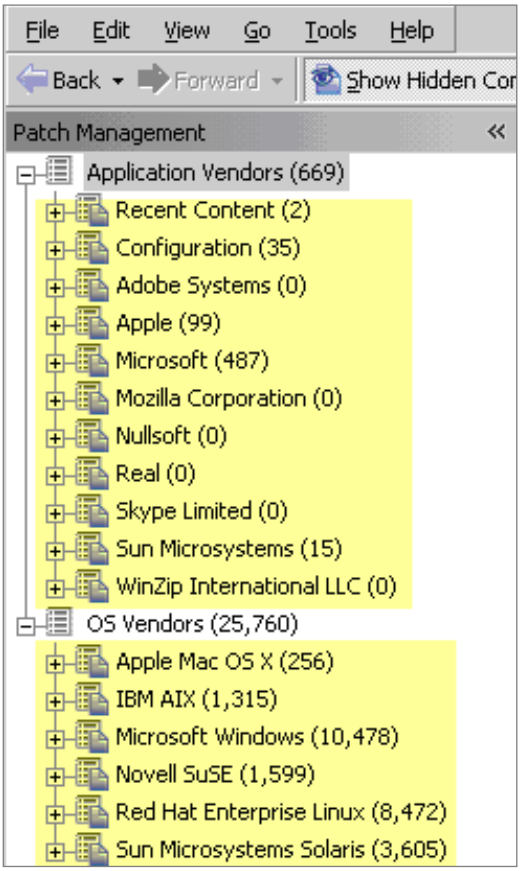
Working with content

The navigation tree organizes Patch Management content into expandable and collapsible folders that you use to easily navigate and manage relevant components in your deployment.

When you click the Patch Management domain at the bottom of your screen, you will see the accompanying Patch Management sites organized into expandable nodes – Application Vendors and OS Vendors. Click the "+" to display the content related to either application or OS vendors within Patch Management.

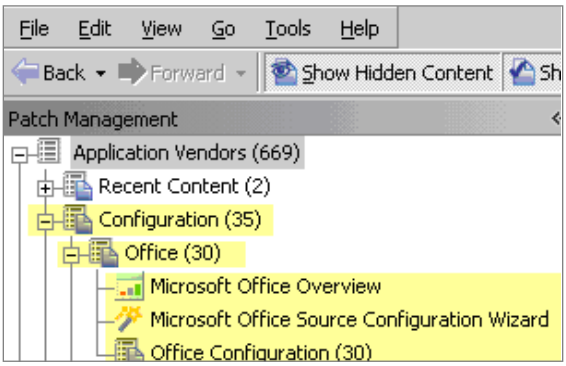
The *All Patch Management* node includes content related to the entire Patch Management domain, which collectively includes all of the sites within this domain.



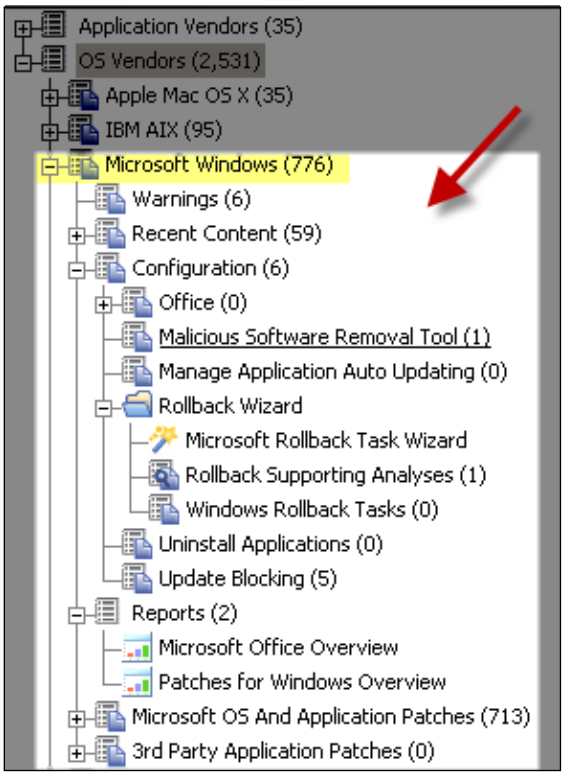


The *Application Vendors* site is organized into 11 primary "nodes" – Recent Content, Configuration, Adobe Systems, Apple, Microsoft, Mozilla Corporation, Nullsoft, Real, Skype Limited, Sun Microsystems, and WinZip International LLC.

Each of these nodes expands into sub-nodes that contain additional content:



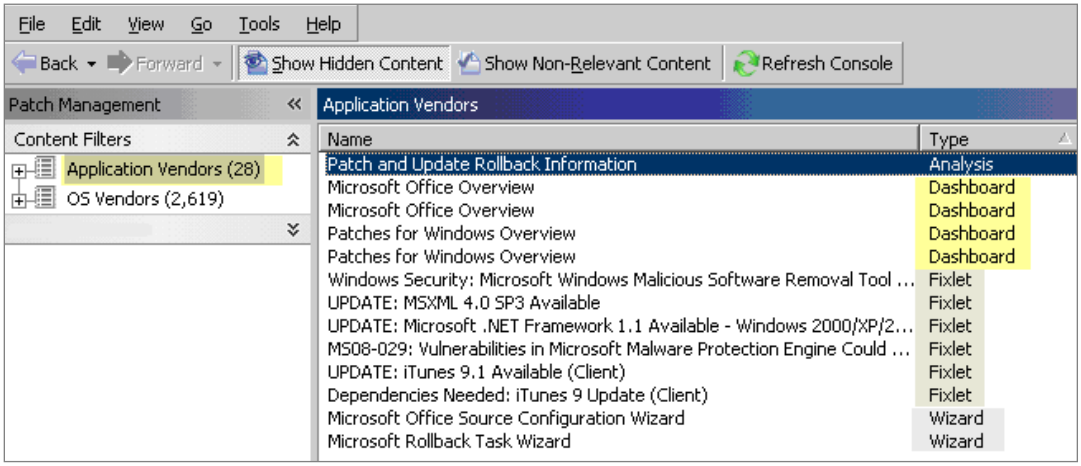
Use the same approach of clicking the "+" and "-" to open and close each node and sub-node. For Windows patches, you mostly use the content contained in the *Microsoft Windows* node under the OS Vendors site in the navigation tree.



Composite view

For an overall view of Patch Management content, click either *Application Vendors* or *OS Vendors* at the top of the navigation tree. This displays content by type:

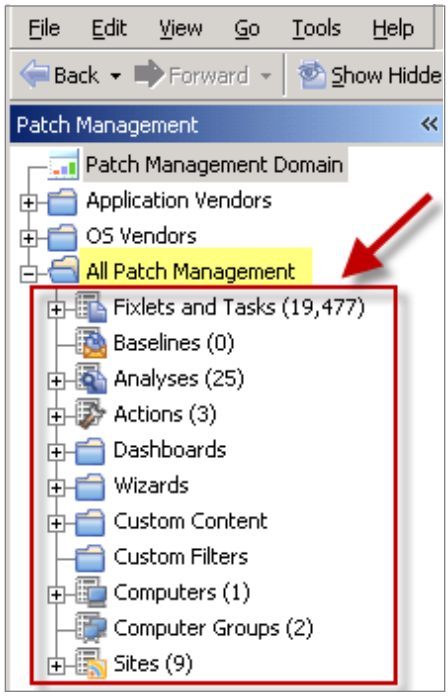
- Analyses
- Dashboards
- Fixlets
- Wizards



This content represents actions that must be addressed to have Patch Management *for Windows* display the most accurate information about security patches and updates for the systems in your deployment.

All Patch Management

The All Patch Management part of the navigation tree contains content relevant to all of the products contained within the Patch Management "domain". From this view, you can see a composite picture of the Fixlets and tasks, analyses, baselines, computer groups and sites related to those BigFix products. This content is visible through expandable and collapsible menus.



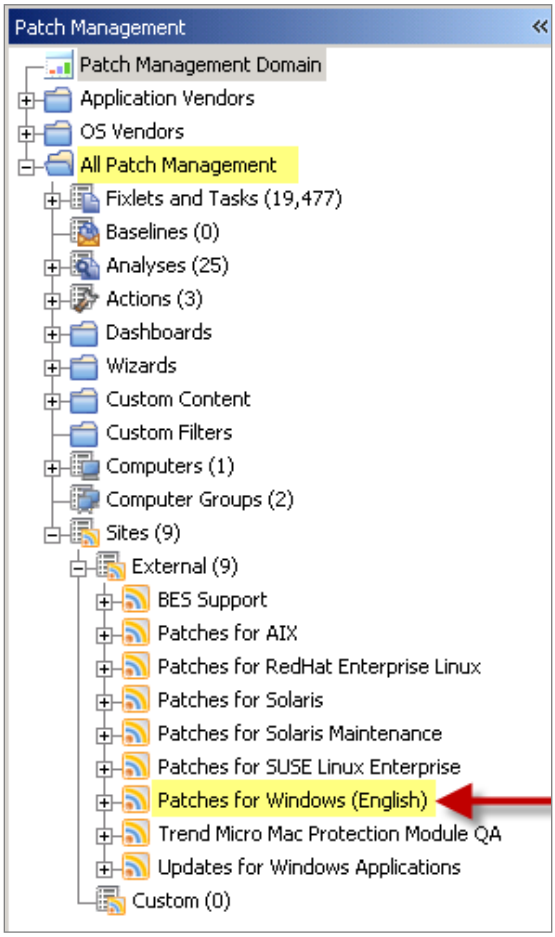
Part Two

Patch Management for Windows

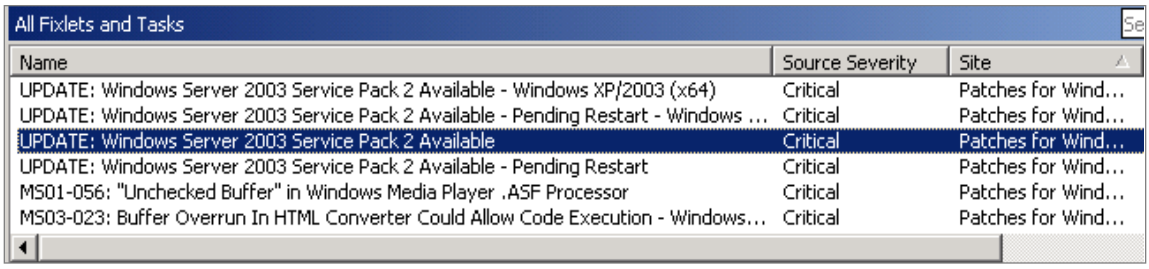
Patch using Fixlets

To deploy patches from the BigFix Console using Fixlets, follow these steps:

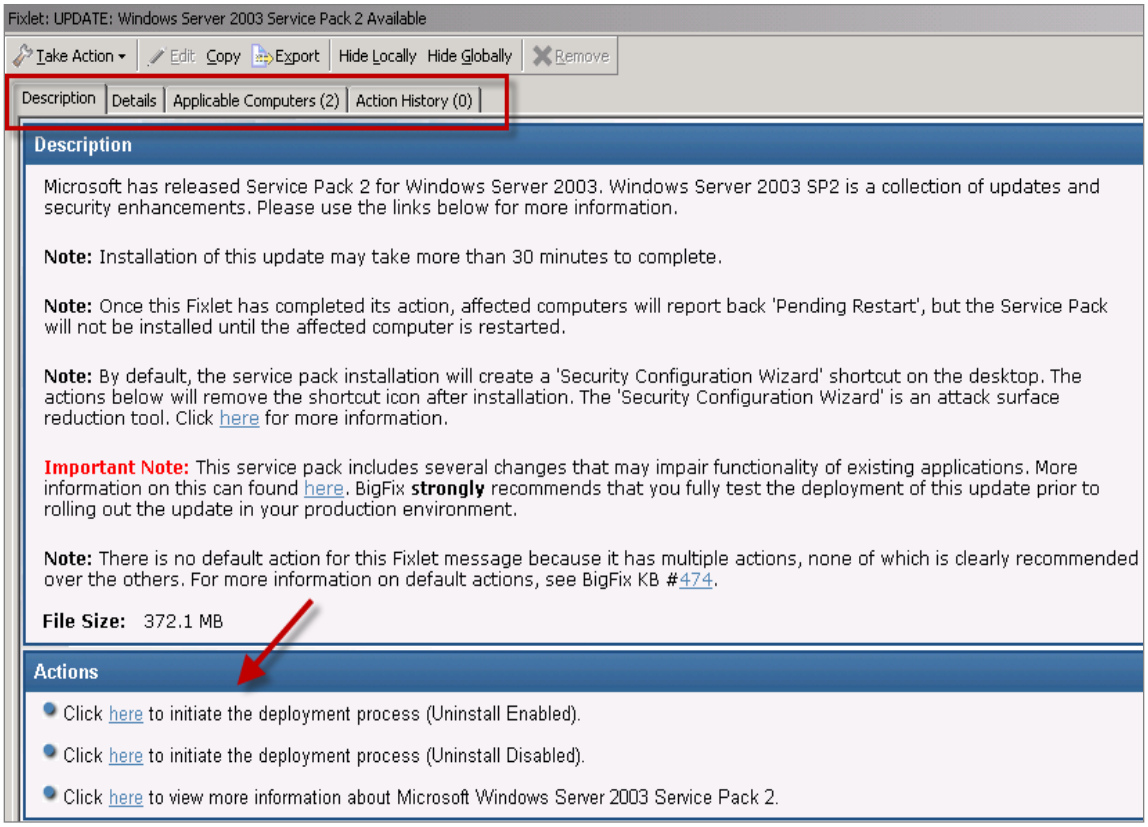
Under *All Patch Management* in the navigation tree, select *All Fixlets and Tasks* and filter *By Site*. Click *Patches for Windows (English).*



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



The Fixlet will open in the work area below:



Click the tabs at the top of the window to review details of this Fixlet. Then click the appropriate link in the Actions box to deploy it. Set additional parameters in the Take Action dialog. Click *OK*, and enter your Private Key Password. The Action propagates across your network, installing the designated patch on the computers that you specified and on the schedule that you selected. You can monitor and graph the results of this action to see exactly which computers have been remediated to ensure compliance.

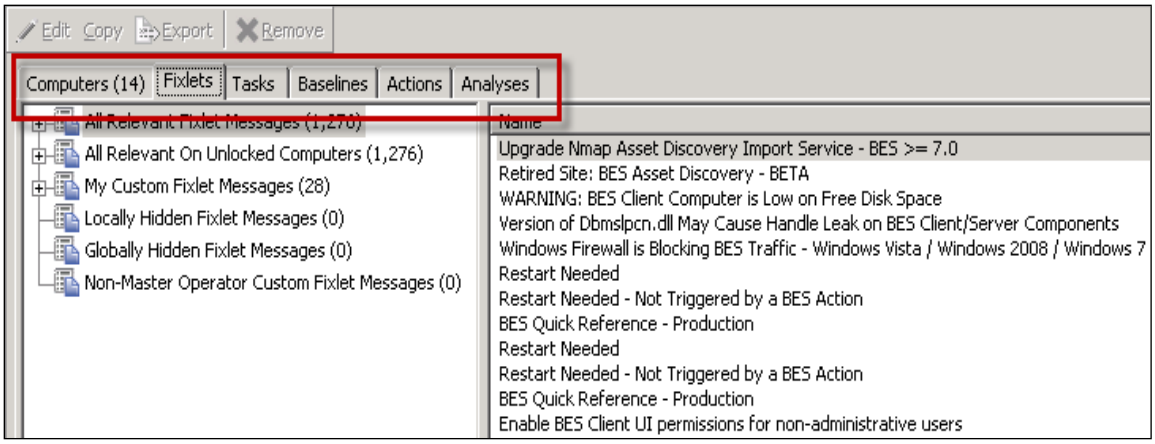
For detailed information about setting parameters with the Take Action dialog, consult the BigFix Console Operators Guide.

Use the Patches for Windows Overview

The Patches for Windows Overview report displays a summary of patch information in your deployment through tables, graphs, and pie charts. Specifically, the Overview report displays Microsoft patch information, deployment information, a Total Patches Needed by Severity graph, and a Severity of Relevant Patches pie chart.

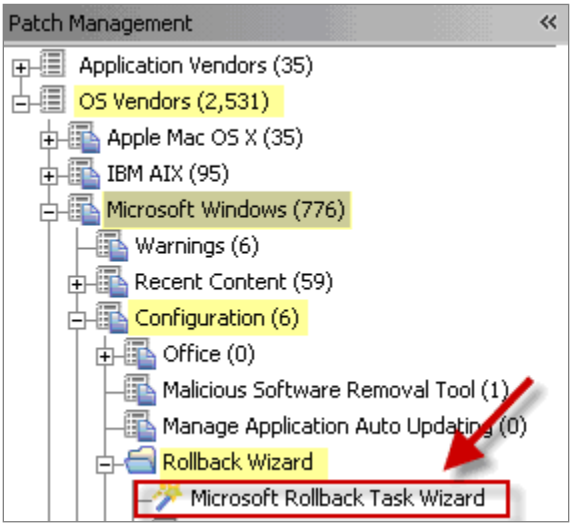
The Overview report provides a quick summary of your Windows remediation, including the number of existing patches, broken down by severity and relevance. It also includes per-computer information, such as average number of patches and critical patches.

Click the link to *Computers Needing at least one Critical Patch* to see the computer listings for this subset. This opens a Fixlet list window, where you can view the relevant Fixlets, Computers, Tasks, Baselines, Actions, and Analyses.

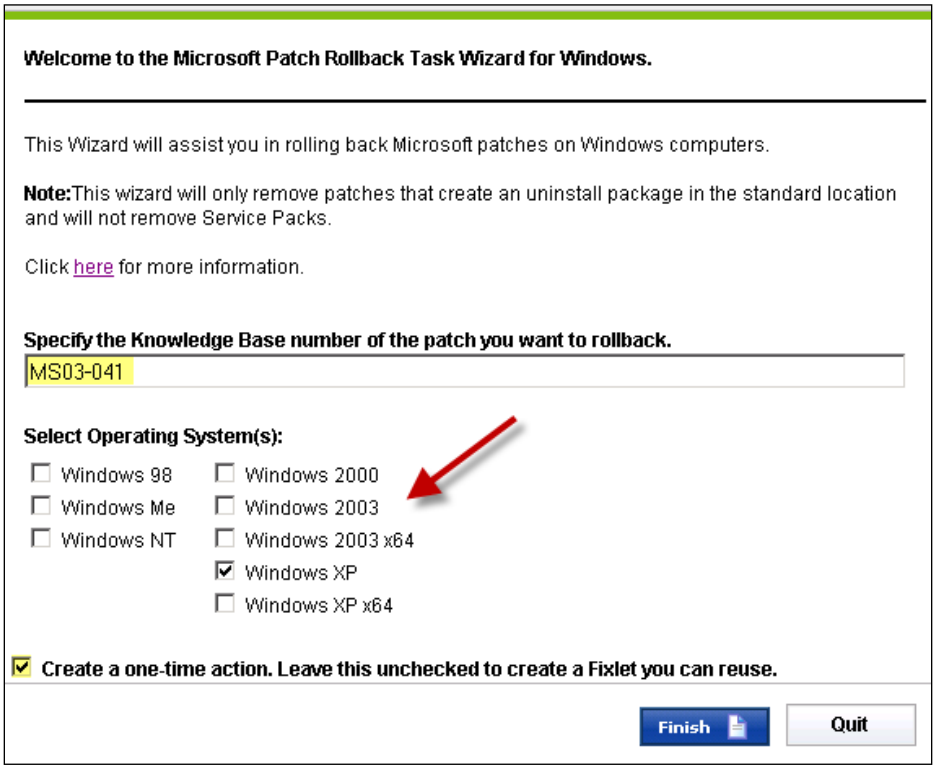


Remove patches with the Rollback Task Wizard

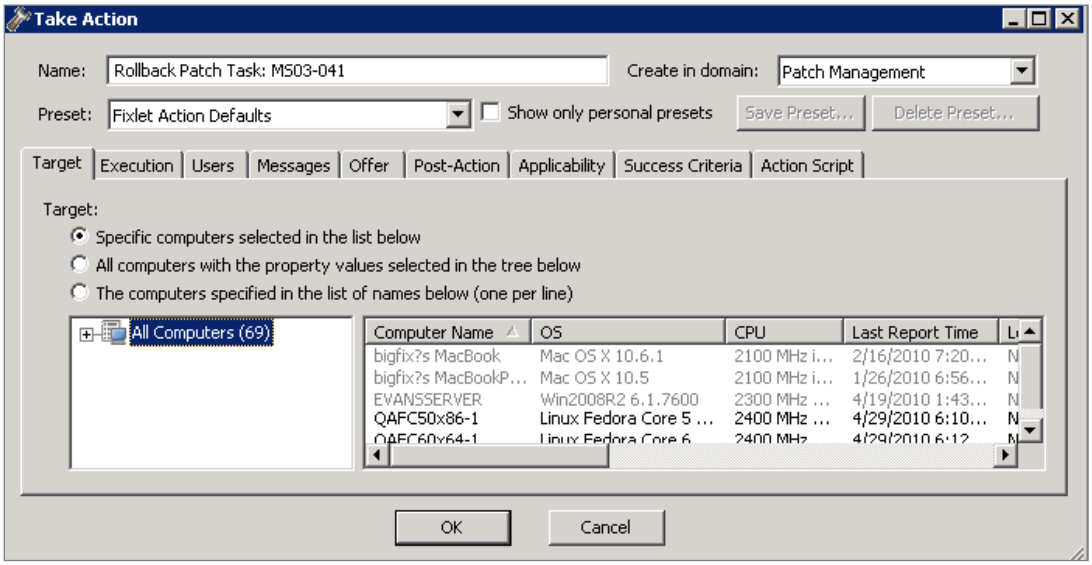
You can remove certain patches using the *Microsoft Patch Rollback Task Wizard*. Access the Wizard by clicking the OS Vendors “site” in the Patch Management navigation tree. Then click Microsoft Windows, Configuration, Rollback Wizard, and *Microsoft Rollback Task Wizard*.



When the Wizard screen opens, enter the Knowledge Base number of the patch in the designated field and select an Operating System. To create a one-time action, click the box in the lower left of the window and then click *Finish.*



This displays the Take Action dialog, where you can set additional parameters:



To initiate the action, Click *OK* and enter your Private Key Password.

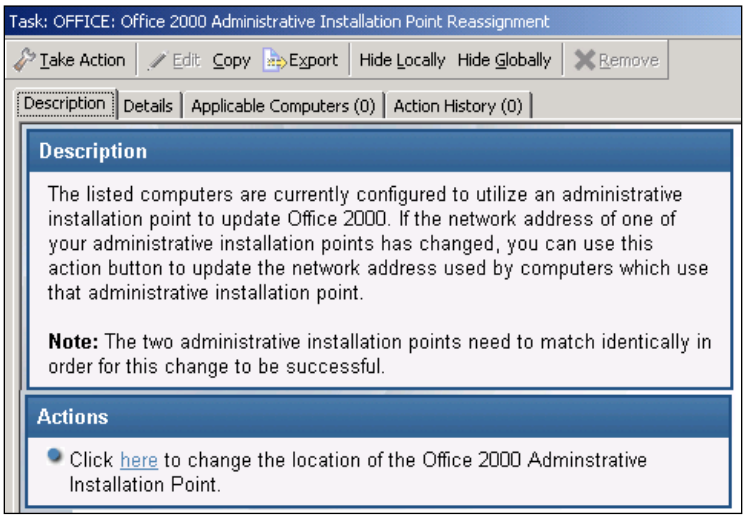
Patch Microsoft Office

Updates to Microsoft Office might require that installation or source files be present for the update to complete successfully. To meet this need, BigFix provides three ways to deploy Microsoft Office updates and patches: *Administrative, Network,* and *Local*. BigFix clients can be configured to use one of these three methods by using the Office Deployment Control tasks in the BES Support site.

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 “admin point” must match the product being patched. For example, an Office 2000 Standard installation cannot point to an Office 2000 Professional admin point. Click the *OS Vendors* site in the navigation tree, and then click *Microsoft Office* and *Configuration.*



- There can only be one Office product present 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, but Office 2000 Small Business and Office XP Professional is.

- The patch must have been correctly applied to the admin point before deploying the action.

- The admin point must be shared, with Read permissions 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.

Network Installation

The Network Installation method uses a network-shared location containing the Office install 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, there can be only one Office product present 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 – see previous section.

- The Office setup files must be shared with Read permissions 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.

Local Installation

The Local Installation method uses source Office install media or source files that are present 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 providing the Office 2000 Professional CD.

- The CD-ROM drive must be recognized by the operating system.

Other languages

In addition to English, there are other international versions of Windows that are supported by Windows Patch Management. Each language is covered by a unique Fixlet site. These languages include:

- Brazilian Portuguese
- Czech
- Dutch
- Finnish
- French
- German
- Hungarian
- Italian
- Norwegian

- Polish
- Spanish
- Turkish
- Japanese
- Korean
- Simplified Chinese
- Swedish
- Traditional Chinese

If you have purchased a Production version of BigFix 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 by visiting the BigFix support website at http://support.bigfix.com.

Part Three

Support

Frequently asked questions

Where are my dashboards located in the new version of the BigFix Console?

The updated BigFix Console contains all of the same content as the previous version, although some content might have moved to a different location.

Expand the *OS Vendors* node in the navigation tree and then click *Microsoft Office* and *Reports* to view the *Microsoft Office Overview* and the *Patches for Windows Overview* dashboards. The *Microsoft Rollback Wizard* is located under the *Configuration* node of the OS Vendors site.

Why does a patch fail, but complete successfully?

Sometimes under very 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.

If a patch fails to install, what should I do?

If a patch fails to install, there are several things 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, and look at the Microsoft Baseline Security Analyzer (MBSA) to see if that tool believes the patch is applicable.

Why is there no default action?

There are a variety of reasons for this. Sometimes a Fixlet or a patch could have catastrophic consequences. It is recommended that you test on a testbed before applying the Fixlet or patch. There also could be multiple actions with the Fixlet, none of which are clearly recommended over other actions. *It is highly recommended that you read the Description text in the Fixlet before initiating the action.*

What does "*Manual Caching Required*" mean?

For whatever reason, 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 BES server.

What are Corrupt Patches and how are they used?

Corrupt patches in Windows are when BigFix 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?

Supersede patches are older versions of patches that no longer need to be applied.

How do I deal with missing patches?

BigFix does not provide every single patch that Microsoft offers. It provides Microsoft security patches on Patch Tuesdays, as well as hotfixes associated with Security Packs.

Technical support

BigFix technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- BigFix Support Site
- Documentation
- Knowledge Base
- Forums and Communities

Part Four

Notices

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 (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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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.

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.

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.

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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