BigFix Patch Management

for Windows

User's Guide

July, 2010

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.
1480 64th Street, Suite 200
Emeryville, California 94608

Contents

CONTENTS

Part 1

Getting Started

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—enabling our customers 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, providing comprehensive operating system and third-party application patches. 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 it 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 message 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 Fixlet messages for Windows patches:

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

- **An installed patch is corrupt.** These Fixlet messages 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 message explains the nature of the vulnerability and then allows you to re-apply the patch.

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

BigFix tests each Fixlet message in its lab before it is released. This testing process often reveals issues that are addressed by attaching extra “notes” to the Fixlet message. 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 Office and other Windows applications.

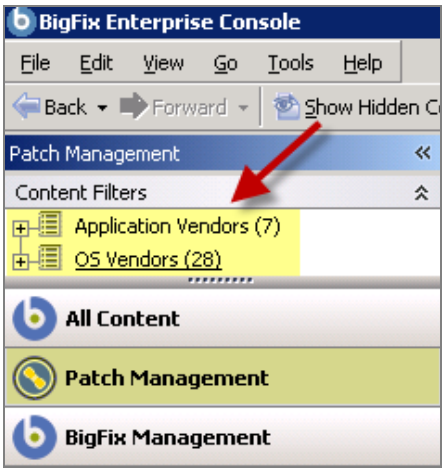
Third-Party Windows Applications:

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

Navigating Patch Management in the BigFix Console

The navigation tree in the BigFix Console, which is available for all BigFix products, will serve as your central command for all Patch Management functionality. The navigation tree gives you easy access to all reports, wizards, Fixlet messages, 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

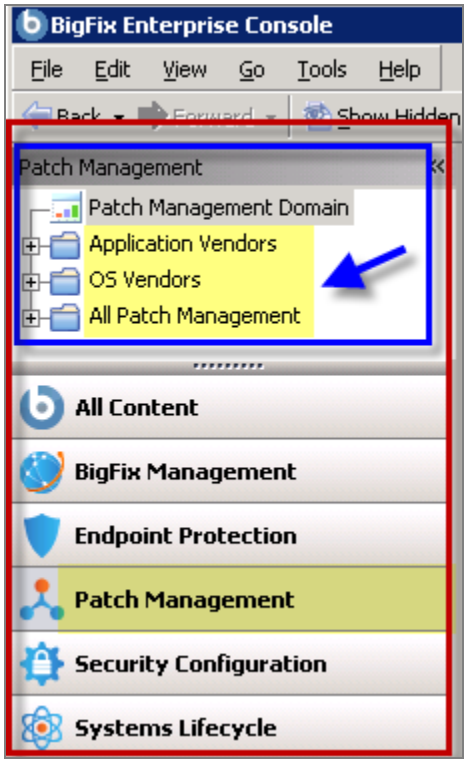
The BigFix Console organizes content into four parts:

- *Domain Panel – Includes navigation tree and list of all domains*
- *Navigation Tree – Includes list of nodes and sub-nodes containing site content*
- *List Panel – Contains listing of tasks and Fixlets*

- *Work Area – Work window where Fixlet and dialogs display*

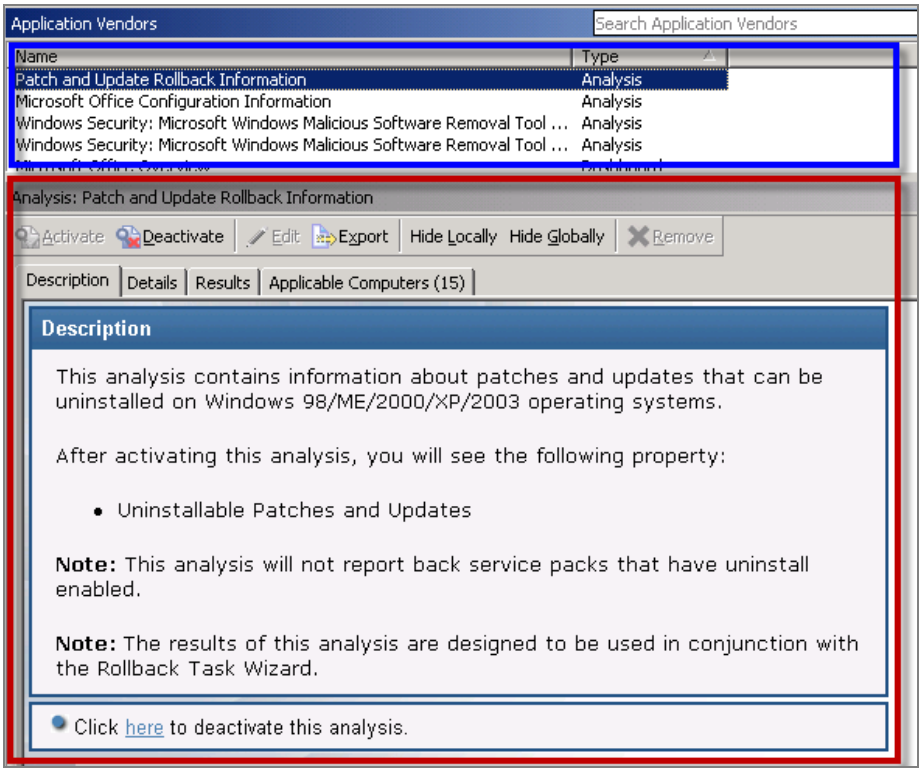
In the context of the BigFix Console, products or *sites* are grouped by categories or *domains*. The Domain Panel is the area on the left side of the Console that includes a navigation tree and a list of all domains. The Navigation Tree includes a list of nodes and sub-nodes containing site content.

The red-outlined area below represents the entire Domain Panel, and the blue box contains just the Navigation Tree. 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 OSs. The third node – *All Patch Management,* expands to include content related to the entire Patch Management domain.



Patch Management "tasks" are sorted through upper and lower task windows, which are 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, etc.

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

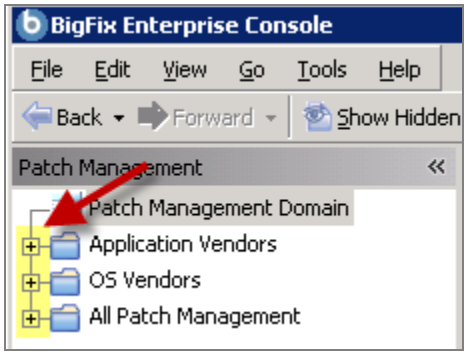


Working with Content

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

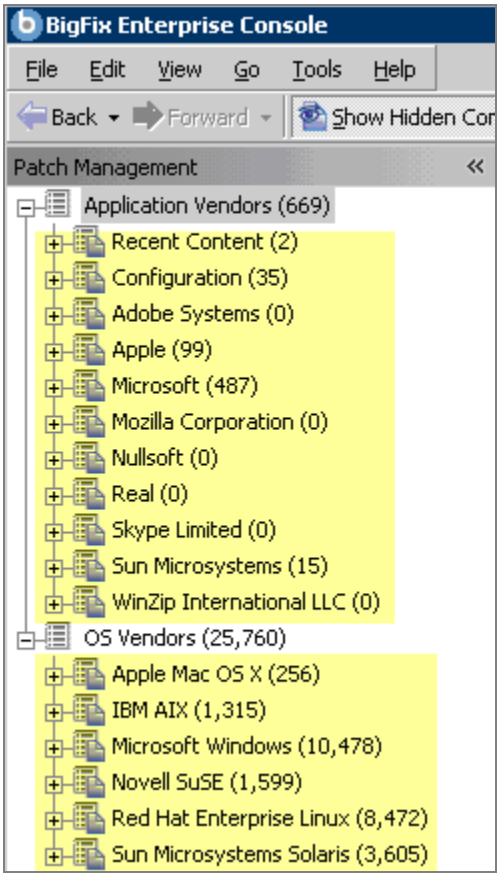
When you click on the Patch Management “domain” at the bottom of your screen, you will see the accompanying Patch Management “sites” organized into expandable nodes – Application Vendors and OS Vendors.

You will see the *Application Vendors* and *OS Vendors* sites are located at the top of the Patch Management navigation tree. Click the “+” to display the content related to either application or OS vendors within Patch Management.



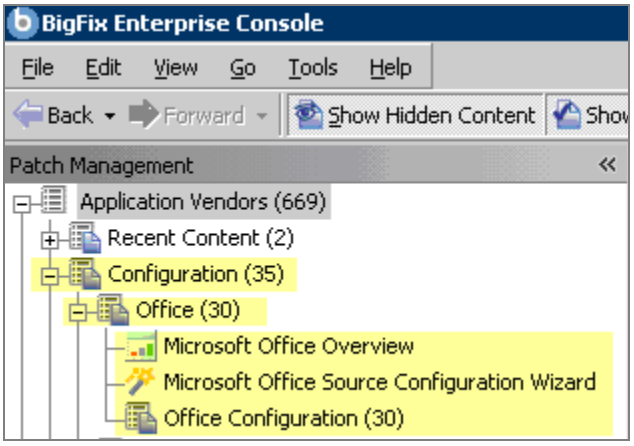
> **Note:** Depending on your operating system, your system may display the "+" and "-" buttons in the navigation tree as triangles. Specifically, the "+" and "-" icons will display on Windows XP/2003/2008/2008R2 machines, and triangles will display on Windows Vista/7. This feature was designed so that the Console matches the standards and conventions of your specific operating system. Regardless of the particular icon, the functionality of these buttons works the same way to either expand or collapse content.

You will use this same expand/collapse method to move through the entire navigation tree. Click each "+" to display each piece of related application or OS Patch Management content.



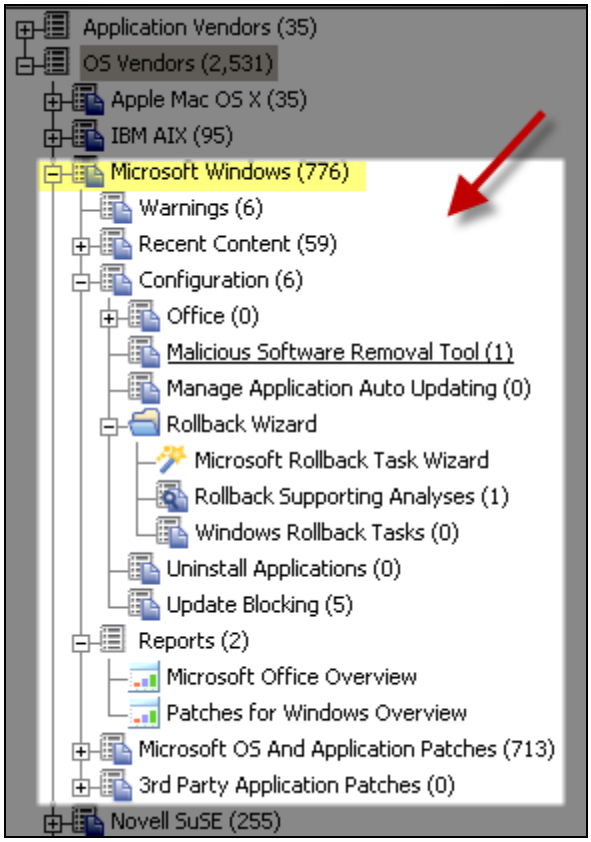
You can see that the *Application Vendors* site is organized into 11 primary "nodes" – Recent Content, Configuration, Adobe Systems, Apple, Microsoft, Mozilla Corporation, Nullsoft, Real, Skype Limited, Sun Microsystems, and WinZip International LLC.

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.

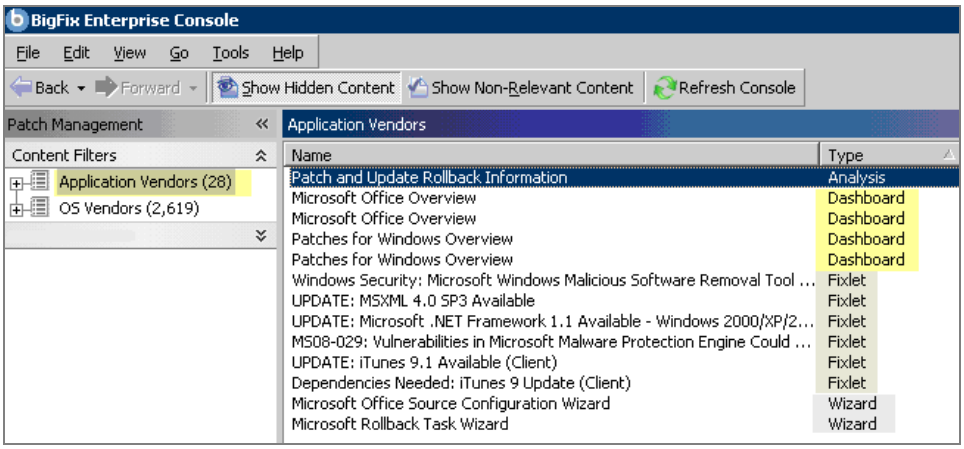
For Windows patches, you will mostly be using the content contained in the *Microsoft Windows* node under the OS Vendors site in the navigation tree.



Composite View

For an overall view of all Patch Management content, click either *Application Vendors* or *OS Vendors* at the top of the navigation tree. This will display all content organized by "type".

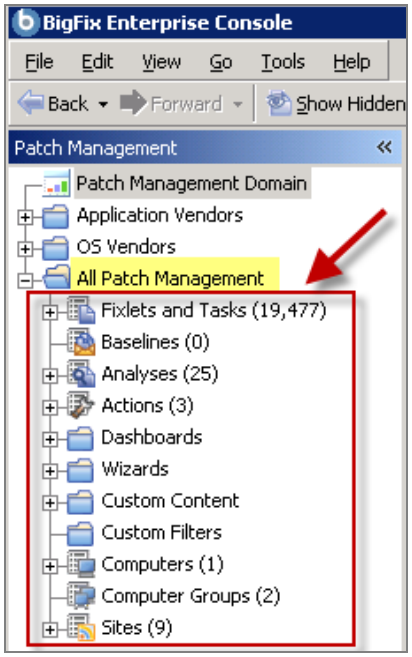
- Analyses
- Dashboards (includes Overview reports and Tasks)
- Fixlets
- Wizards



This content represents actions that need to be addressed so that Patch Management *for Windows* can display the most accurate and up to date 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 Fixlet messages and tasks, analyses, baselines, computer groups and sites related to those BigFix products. This content is visible through expandable and collapsible menus.



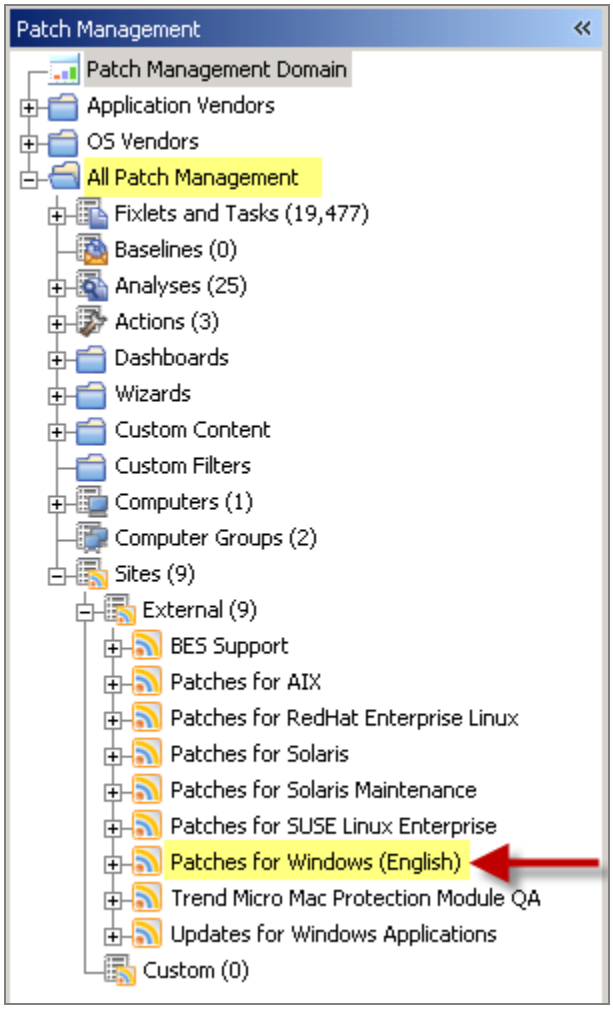
Part 2

Patch Management

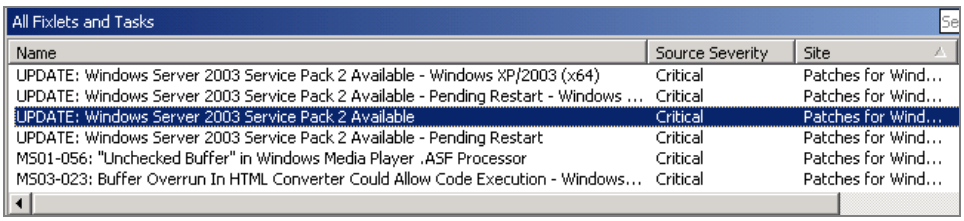
Patching Using Fixlet Messages

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

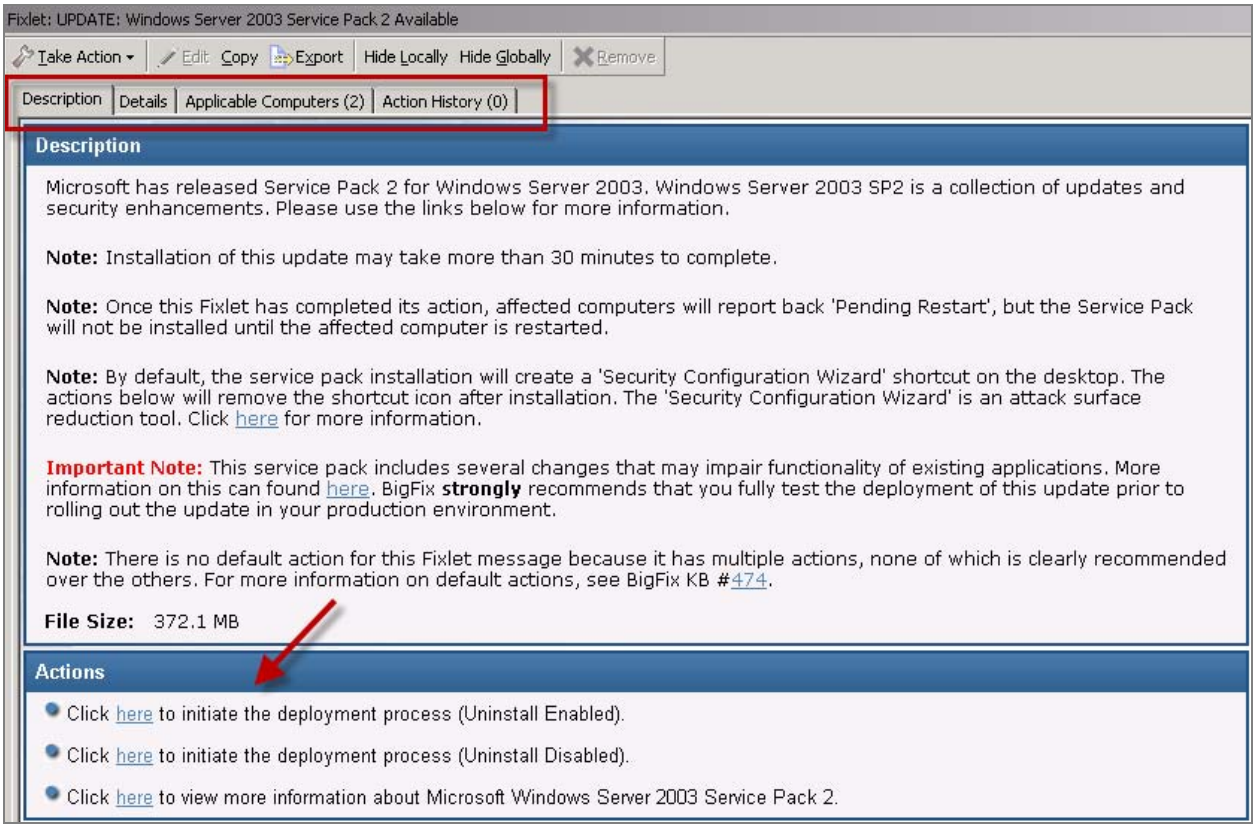
Under *All Patch Management* in the navigation tree, select *All Fixlets and Tasks* and filter *By Site*. Click on *Patches for Windows (English).*



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



The Fixlet message will open in the work area below:

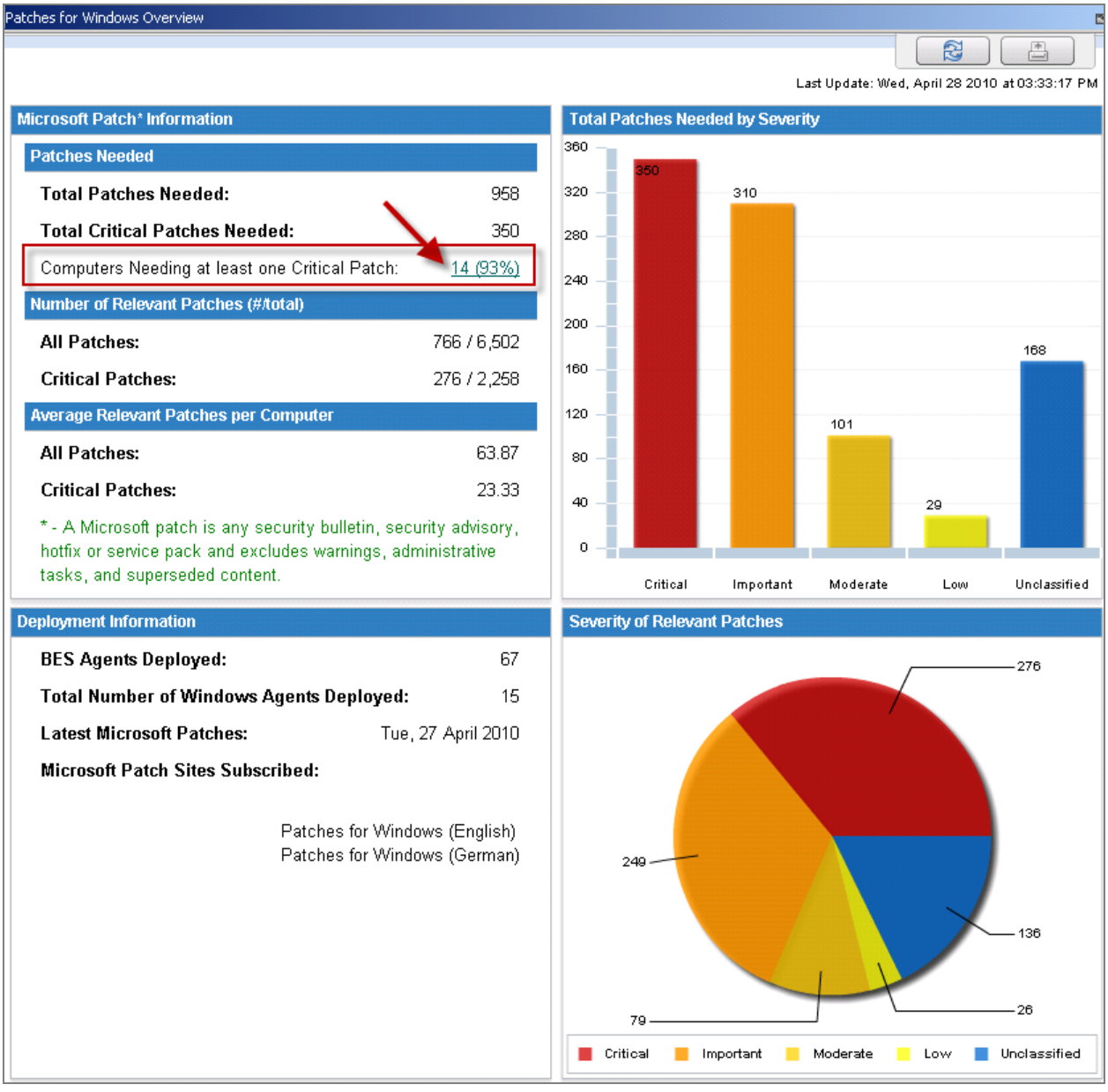


Click the tabs at the top of the window to review details of this Fixlet. Then click the appropriate link in the Actions box to deploy it. Set additional parameters in the Take Action dialog. Click *OK*, and enter your Private Key Password. The Action will propagate across your network, installing the designated patch to the machines you specified and on the schedule 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.

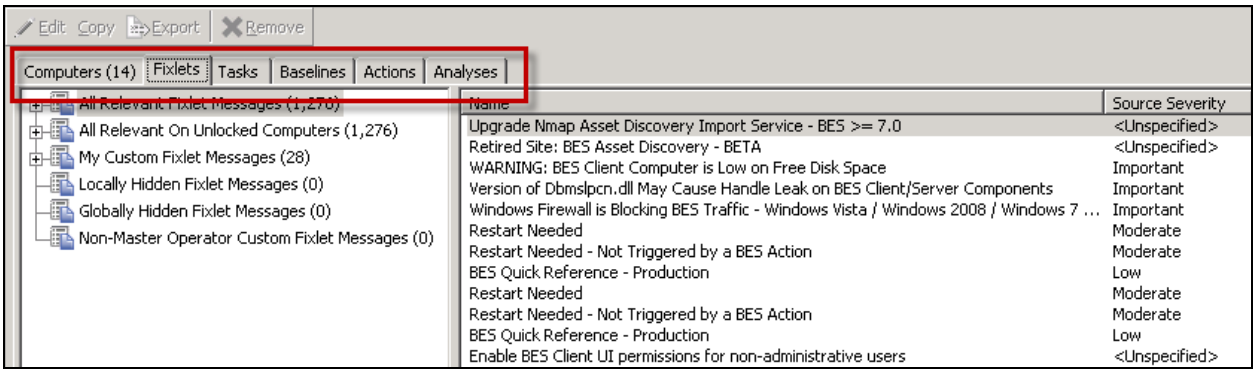
Using the Patches for Windows Overview

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 Severity of Relevant Patches pie chart.



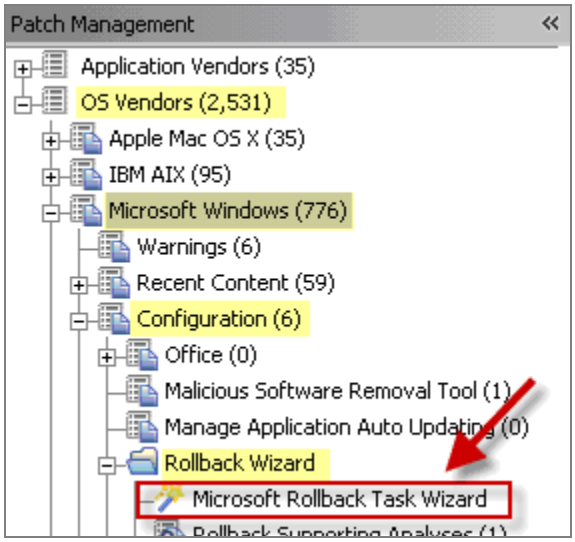
The Overview report provides a quick summary of your Windows remediation, including the number of existing patches, broken down by severity and relevance. It also includes per-computer information, such as average number of patches and critical patches.

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

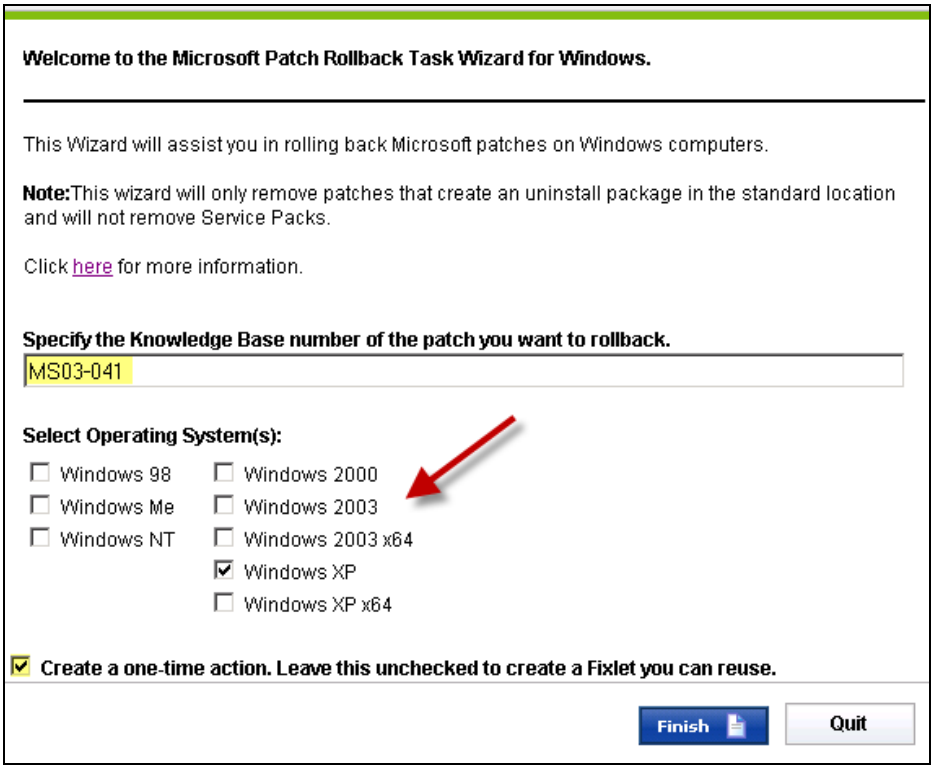


Removing Patches with the Rollback Wizard

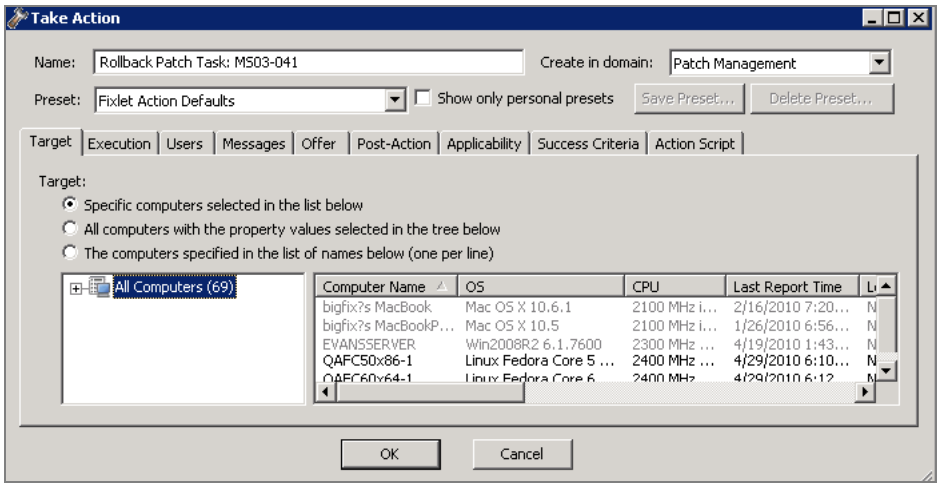
You can remove certain patches using the *Microsoft Patch Rollback Task Wizard*. Access the Wizard by clicking the OS Vendors "site" in the Patch Management navigation tree. Then click Microsoft Windows, Configuration, Rollback Wizard, and *Microsoft Rollback Task Wizard*.



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. Then click *Finish.*



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



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

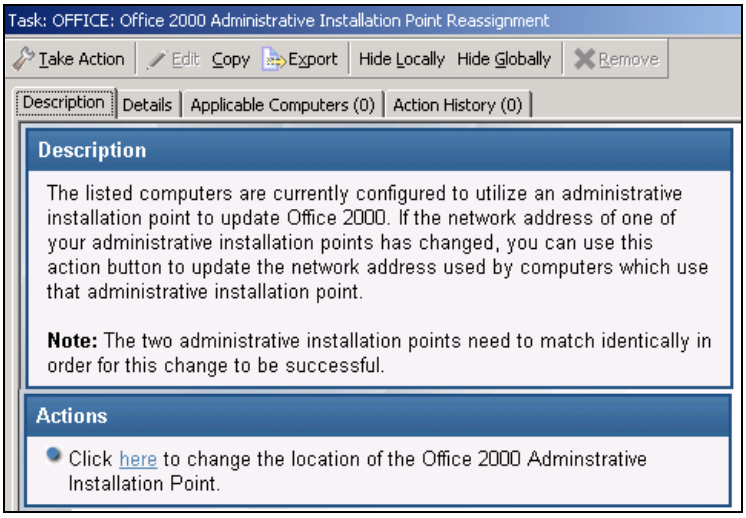
Patching Microsoft Office

Updates to Microsoft Office may require that installation or source files be present in order 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 via the Office Deployment Control Tasks in the BES Support site.

Administrative Installation

The Administrative Installation method utilizes 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 properly 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 utilizes 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 only be one Office product present on the computer, however multiple installations of different Office versions will work (for instance, 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 utilizes source Office install media or source files that are present locally on every computer to be updated. The following caveats apply to this install method:

- Before executing the Action, the proper Office CD must be placed in the local CD-ROM drive of each computer you wish 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 will 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 site.

Part 3

Support

Frequently Asked Questions

The following are a list of Frequently Asked Questions. If you have a question about this product and don't see your question below, see the Global Support section of this document for a list of available resources.

What kind of Microsoft security content does BigFix release for the Patches for Windows site?

Please check the related Knowledge Base article on the BigFix support website.

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, though some content may 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 will successfully apply but the relevance conditions will indicate that it is still needed. Check to see if there are any special circumstances associated with the patch, or contact 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.

Where is the *Software Distribution Wizard* that used to be part of Patch Management *for Windows?*

The Software Distribution Wizard is now located in the System Lifecycle Management domain.

Do I need to use the Microsoft Office Source Configuration Wizard?

Office 2007 and later products are automatically installed with a local source and do not need to be reconfigured.

Why is there no default action?

There are a variety of reasons for this. Sometimes a Fixlet message 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 message before initiating the action.*

What does "*Manual Caching Required*" mean?

For whatever reason, a particular vendor may not be providing a download directly to their link. You will then need to click through a EULA 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 didn't complete. These patches become relevant to indicate that something is wrong with the security patch. To remediate, take the appropriate action that will 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. We provide Microsoft security patches on Patch Tuesdays, as well as some hotfixes associated with Security Packs.

Best Practice "Tips"

- If you have Microsoft Office patches, you should set your deployment options for older patches.
- For Microsoft Windows 7 and Microsoft Server 2008 r2, you need to have the appropriate version of the BigFix Client (7.2.5.22 or above) in order to see patches.

Global Support

BigFix offers a suite of support options to help optimize your user-experience and success with this product. Here's how it works:

- First, check the BigFix website Documentation page:
- Next, search the BigFix Knowledge Base for applicable articles on your topic:
- Then check the User Forum for discussion threads and community-based support:

If you still can't find the answer you need, contact BigFix's support team for technical assistance:

- Phone/US: 866 752-6208 (United States)
- Phone/International: 661 367-2202 (International)
- Email: enterprisesupport@bigfix.com

