

**BigFix
Patch for Windows - User's Guide**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page lxxxv\)](#).

Edition notice

This edition applies to BigFix version 11 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

- Special notice..... ii
- Edition notice..... iii
- Chapter 1. Patch for Windows User's Guide..... 6**
- Chapter 2. Overview..... 7**
 - System requirements..... 7
 - Other languages supported..... 41
 - Site subscription..... 42
 - Fixlet fields..... 43
- Chapter 3. Patch for Windows..... 45**
 - Patch using Fixlets..... 45
 - Supersedence in Windows..... 46
 - Windows Patch Client settings..... 47
 - Patches for Windows Overview dashboard..... 47
 - Patch Overview dashboard..... 51
 - Uninstalling patches..... 53
 - Using the Rollback Task wizard..... 53
 - Troubleshooting uninstallation of patches..... 55
 - Fixing Corrupt Patches..... 56
 - Using the Corrupt Patch Deployment wizard..... 56
 - Patch Microsoft Office..... 58
 - Administrative Installation..... 58
 - Network Installation..... 59
 - Local Installation..... 60
- Chapter 4. Installing and updating Click-to-Run products..... 61**
 - Installing and updating Click-to-Run products..... 63
 - Understanding how BigFix works with Click-to-Run..... 65
 - Setting up to download updates from a network share location..... 67
 - Setting up the network share..... 67
 - Configuring the Update Path..... 67
 - Maintaining updates..... 68
 - Enabling automatic updates..... 68

Disabling automatic updates.....	69
Removing the Update Path.....	69
Deleting a network share.....	69
Disabling the automatic upgrade of Office 365 – Office 2013 to Office 365 – Office 2016.....	70
Enabling the automatic upgrade of Office 365 – Office 2013 to Office 365 – Office 2016.....	70
Enabling Office 365 previous version Fixlets.....	70
Removing the update source setting.....	71
Checking the Office 365 configuration.....	71
Chapter 5. Navigating Windows Application Update Patches in the BigFix console.....	72
Fixlet Maker dashboard overview.....	73
Creating custom Fixlets from templates.....	75
Chapter 6. Using the custom repository setting feature.....	77
Creating a custom repository setting.....	78
Delete a custom repository setting.....	78
Appendix A. Support.....	80
Appendix B. Frequently asked questions.....	81
Notices.....	lxxxv

Chapter 1. Patch for Windows

BigFix Patch for Windows™ provides Fixlets for Microsoft™ security and non-security patches. Dashboards, wizards, and reports aid you in managing updates for various endpoint devices.

BigFix provides highly scalable, multi-platform, automated patch management solutions. 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, so you can 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 its solution. The solution, which includes deploying a multi-purpose, lightweight BigFix 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

Support for Windows 10 Feature Updates

BigFix Patches for Windows expanded its coverage to include support for Windows 10 Feature Updates of the Education, Enterprise, and Professional editions and their N variants. In this release, BigFix offers the custom repository feature.

- Supported editions: Education, Enterprise, Professional, Education N, Enterprise N, Professional N
- Architecture: x86, x64
- Languages : English and Japanese

Updates in the Custom Repository Settings feature tasks

The Custom Repository Settings feature tasks are now available in the Patching Support site instead of the Updates for Windows Applications site.

The Create or Update Custom Repository (Windows) task was retired and replaced by the Set or Update Custom Repository (Windows) task, which is accessible in the Patching Support site.

Chapter 2. Overview

Patch for Windows™ creates Fixlets for the patches that Microsoft™ issues. The BigFix 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.

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

For each new patch issued by Microsoft™, BigFix releases a Fixlet® that identifies and remediates 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 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.

BigFix 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. BigFix 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 rollout.

System requirements

BigFix supports security and non-security updates for Microsoft and third-party operating systems and applications.

Types of supported updates

BigFix supports the following types of Windows updates.

Security update

Refers to security-related vulnerabilities.

Cumulative update

Refers to updates that contain all the previously released updates up to that update release. If you have installed previous updates, only the new fixes that are contained in this package will be downloaded and installed to your computer.

Non-security update

Refers to all other updates that are not included in the security updates type. There are several types of non-security updates. For more information, see <http://support.microsoft.com/>.

BigFix supports the following non-security updates:

Critical update

Refers to widely released fixes to address bugs that are critical but not related to security.

Service pack

Refers to cumulative set of security, critical, and general updates. Service packs might also contain hot fixes or additional fixes that were found internally since the last release. In some cases, service packs also contain design or feature changes that were requested by customers.

Update

Refers to widely released fixes to address bugs that are not critical or not related to security.



Note: BigFix generally provides support for updates that are found in the Microsoft Update Catalog. In some instances, the updates require users to directly download the links. For more information, see <https://catalog.update.microsoft.com/v7/site/home.aspx>. This link requires the use of Internet Explorer.

Update rollup

Refers to updates that target a specific area, for example security or a product component. Update rollup is a cumulative set of hot fixes, security updates, critical updates, and updates that are packaged for easy deployment.



Note: BigFix generally provides support for updates that are found in the Microsoft Update Catalog. In some instances, the updates require users to directly download the links. For more information, see <https://catalog.update.microsoft.com/v7/site/home.aspx>. This link requires the use of Internet Explorer.

To learn more about the standard terminology that Microsoft uses, see <http://support.microsoft.com/en-us/kb/824684>.

BigFix tries to stay close to the terms that the vendors use, such as the Microsoft patch category terminology. In some instances, Microsoft and BigFix use different category terms. For more information, see <https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/Difference%20in%20category%20terms%20used%20by%20Microsoft%20and%20BigFix>.

Supported operating systems and applications

BigFix provides security and non-security updates for operating systems and applications in the Patch Management for Windows site. Non-security updates include critical updates, service packs, and general updates.

BigFix supports the final release versions of the listed Microsoft products. Microsoft versions other than the final commercial release version, such as alpha, beta, preview, community technology previews (CTP), technical previews, and insider programs, are not supported by BigFix.

The following table lists the supported operating systems, applications, and their corresponding updates types.

Table 1. Supported operating systems and applications with the corresponding update types

Supported OS	Type of Update Supported				
	Security update	Non-security update			
		Critical Update	Service Pack	Update	Update rollout
<i>Antigen</i>					
Antigen for Exchange/SMTP	check	-	-	-	-
<i>Bing</i>					
Bing Bar	check	-	-	-	-
Search Enhancement Pack	check	-	-	-	-
Windows Live	check	-	-	-	-
<i>BizTalk Server</i>					
BizTalk Server 2002	check	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported				
BizTalk Server 2006R2	check	-	-	-	-	
BizTalk Server 2009	check	-	-	-	-	
BizTalk Server 2013	check	-	-	-	-	
Host Integra- tion Server 2000	check	-	-	-	-	
Host Integra- tion Server 2004	check	-	-	-	-	
Host Integra- tion Server 2006	check	-	-	-	-	
Host Integra- tion Server 2009	check	-	-	-	-	
Host Integra- tion Server 2010	check	-	-	-	-	
<i>Developer Tools, Run- times, and Re- distributables</i>						
Report Viewer 2005	check	-	-	-	-	
Report Viewer 2008	check	-	-	-	-	
Report Viewer 2010	check	-	-	-	-	
Visual Studio 2005	check	-	-	-	-	

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
	check	check	check	check	check
Exchange Server 2016	check	check	check	check	check
Exchange Server 2019	check	check	check	check	check
<i>Expression</i>					
Expression Design 1	check	-	-	-	-
Expression Design 2	check	-	-	-	-
Expression Design 3	check	-	-	-	-
Expression Design 4	check	-	-	-	-
Expression Media 2	check	-	-	-	-
Expression Media V1	check	-	-	-	-
Expression Web 3	check	-	-	-	-
Expression Web 4	check	-	-	-	-
<i>Forefront</i>					
Forefront Client Security	check	-	-	-	-
Forefront code named Stirling Beta version	check	-	-	-	-
Forefront Endpoint Protection 2010	check	-	-	-	-
Forefront Identity Manager 2010 R2	check	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported				
Forefront Identity Manager 2010	check	-	-	-	-	
Forefront Protection Category	check	-	-	-	-	
Forefront Server Security Category	check	-	-	-	-	
Forefront Threat Management Gateway, Definition Updates for HTTP Malware Inspection	check	-	-	-	-	
Forefront TMG MBE	check	-	-	-	-	
Forefront TMG Threat Management Gateway Definition Updates for Network Inspection System	check	-	-	-	-	
TMG Firewall Client	check	-	-	-	-	
<i>HPC Pack</i>						
Compute Cluster Pack	check	-	-	-	-	
HPC Pack 2008	check	-	-	-	-	
<i>Internet Security and Acceleration Server</i>						

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported			
Firewall Client for ISA Server	check	-	-	-	-
Internet Security and Acceleration Server 2004	check	-	-	-	-
Internet Security and Acceleration Server 2006	check	-	-	-	-
<i>Microsoft Application Virtualization</i>					
Microsoft Application Virtualization 4.5	check	-	-	-	-
Microsoft Application Virtualization 4.6	check	-	-	-	-
Microsoft Application Virtualization 5.0	check	-	-	-	-
<i>Microsoft BitLocker Administration and Monitoring</i>					
Microsoft BitLocker Administration and Monitoring v1	check	-	-	-	-
<i>Microsoft Dynamics CRM</i>					
Microsoft Dynamics CRM 2011 SHS	check	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported					
Microsoft Dynamics CRM 2011	check	-	-	-	-	-
Microsoft Dynamics CRM 2013	check	-	-	-	-	-
<i>Microsoft HealthVault</i>			-			
HealthVault Connection Center Upgrades	check	-	-	-	-	-
HealthVault Connection Center	check	-	-	-	-	-
<i>Microsoft Lync Server and Microsoft Lync</i>						
Microsoft Lync 2010	check	check	check	check	check	check
Microsoft Lync Server 2010	check	check	check	check	check	check
Microsoft Lync Server 2013	check	check	check	check	check	check
<i>Microsoft Online Services</i>						
Microsoft Online Services Sign-In Assistant	check	-	-	-	-	-
<i>Microsoft Research AutoCollage</i>						

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS			Type of Update Supported			
Microsoft Research Auto-Collage 2008	check	-	-	-	-	-
<i>Microsoft Security Essentials</i>						
MS Security Essentials	check	-	-	-	-	-
Security Essentials	check	-	-	-	-	-
<i>SQL Server PowerPivot for Excel</i>						
Microsoft SQL Server 2008 R2 - PowerPivot for Microsoft Excel 2010	check	-	-	-	-	-
<i>SQL Server PowerPivot for Excel</i>						
Microsoft SQL Server 2008 R2 - PowerPivot for Microsoft Excel 2010	check	-	-	-	-	-
<i>Microsoft StreamInsight</i>						
Microsoft StreamInsight V1.0	check	-	-	-	-	-
<i>System Center Data Protection Manager</i>						
Data Protection Manager 2006	check	-	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported					
Microsoft System Center DPM 2010	check	-	-	-	-	-
<i>Network Monitor</i>						
Network Monitor 3	check	-	-	-	-	-
<i>Office Communications Server And Office Communicator</i>						
Office Communicator 2007 R2	check	check	check	check	check	check
Office Communications Server 2007	check	check	check	check	check	check
Office Communications Server 2007 R2	check	check	check	check	check	check
<i>Office Live</i>						
Office Live Add-in	check	-	-	-	-	-
<i>Office</i>						
Dictionary Updates for Microsoft IMEs	check	check	check	check	check	check
New Dictionaries for Microsoft IMEs	check	check	check	check	check	check
Office 2002/XP	check	check	check	check	check	check
Office 2002/XP	check	check	check	check	check	check
Office 2010	check	check	check	check	check	check

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
Office 2013	check	check	check	check	check
<i>SDK Components</i>					
CAPICOM	check	-	-	-	-
<i>Silverlight</i>					
Silverlight	-	-	-	-	-
<i>Microsoft Sharepoint</i>					
SharePoint Server 2019	check	check	check	check	check
SharePoint Foundation 2016	check	check	check	check	check
SharePoint Foundation 2013	check	check	check	check	check
SharePoint Foundation 2010	check	check	check	check	check
SharePoint Foundation 2010 SP2	check	check	check	check	check
SharePoint Foundation 2013 SP1	check	check	check	check	check
SharePoint Server 2016	check	check	check	check	check

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
	check	check	check	check	check
SharePoint Server 2013 SP1	check	check	check	check	check
SharePoint Server 2010 SP2	check	check	check	check	check
SharePoint Designer 2013	check	check	check	check	check
Skype					
Skype for Windows	check	-	-	-	-
SQL Server					-
Microsoft SQL Server 2019	check	check	check	check	check
Microsoft SQL Server 2017	check	check	check	check	check
Microsoft SQL Server 2016	check	check	check	check	check
Microsoft SQL Server 2014	check	check	check	check	check
Microsoft SQL Server 2012	check	check	check	check	check
Microsoft SQL Server 2012 SP4	check	check	check	check	-
SQL Server 2000	check	check	check	check	check
SQL Server 2005	check	check	check	check	check
SQL Server 2008 R2	check	check	check	check	check

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
SQL Server 2008	check	check	check	check	check
SQL Server 2012 Product Updates for Setup	check	check	check	check	check
<i>System Center Online</i>					
Category for System Center Online Client	check	-	-	-	-
<i>System Center Virtual Machine Manager</i>					
Microsoft System Center Virtual Machine Manager 2007	check	-	-	-	-
Microsoft System Center Virtual Machine Manager 2008	check	-	-	-	-
<i>System Center</i>					
System Center 2012 - App Controller	check	-	-	-	-
System Center 2012 - Data Protection Manager	check	-	-	-	-
System Center 2012 - Operations Manager	check	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported				
System Center 2012 - Orches- trator	check	-	-	-	-	-
System Center 2012 - Virtual Machine Man- ager	check	-	-	-	-	-
System Center 2012 R2 - Da- ta Protection Manager	check	-	-	-	-	-
System Center 2012 R2 - Oper- ations Manager	check	-	-	-	-	-
System Center 2012 R2 - Or- chestrator	check	-	-	-	-	-
System Center 2012 R2 - Vir- tual Machine Manager	check	-	-	-	-	-
System Center 2012 SP1 - App Controller Set- up Self-update	check	-	-	-	-	-
System Center 2012 SP1 - App Controller	check	-	-	-	-	-
System Center 2012 SP1 - Da- ta Protection Manager	check	-	-	-	-	-
System Center 2012 SP1 - Op-	check	-	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported					
eration Manager						
System Center 2012 SP1 - Virtual Machine Manager	check	-	-	-	-	-
System Center Advisor	check	-	-	-	-	-
<i>Systems Management Server</i>						
System Center Configuration Manager 2007	check	-	-	-	-	-
Systems Management Server 2003	check	-	-	-	-	-
<i>Virtual Server</i>						
Virtual PC	check	-	-	-	-	-
Virtual Server	check	-	-	-	-	-
<i>Windows Azure Pack - Web Sites</i>						
Windows Azure Pack: Web Sites	check	-	-	-	-	-
<i>Windows Azure Pack</i>						
Windows Azure Pack: Admin API	check	-	-	-	-	-
Windows Azure Pack: Admin Authentication Site	check	-	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported				
Windows Azure Pack: Admin Site	check	-	-	-	-	
Windows Azure Pack: Configu- ration Site	check	-	-	-	-	
Windows Azure Pack: Mi- crosoft Best Practice Ana- lyzer	check	-	-	-	-	
Windows Azure Pack: Monitor- ing Extension	check	-	-	-	-	
Windows Azure Pack: MySQL Extension	check	-	-	-	-	
Windows Azure Pack: Power- Shell API	check	-	-	-	-	
Windows Azure Pack: SQL Serv- er Extension	check	-	-	-	-	
Windows Azure Pack: Tenant API	check	-	-	-	-	
Windows Azure Pack: Tenant Authentication Site	check	-	-	-	-	
Windows Azure Pack: Tenant Public API	check	-	-	-	-	

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported				
Windows Azure Pack: Tenant Site	check	-	-	-	-	
Windows Azure Pack: Usage Extension	check	-	-	-	-	
Windows Azure Pack: Web App Gallery Extension	check	-	-	-	-	
<i>Windows Embedded</i>						
Windows Embedded Developer Update	check	-	-	-	-	
<i>Windows Essential Business Server</i>						
Windows Essential Business Server 2008 Setup Updates	check	-	-	-	-	
Windows Essential Business Server 2008	check	-	-	-	-	
Windows Essential Business Server Preinstallation Tools	check	-	-	-	-	
<i>Windows Live</i>						

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported			
OneCare Family Safety Installation	check	-	-	-	-
Photo Gallery Installation and Upgrades	check	-	-	-	-
Windows Live Toolbar	check	-	-	-	-
Windows Live Writer Installation and Upgrades	check	-	-	-	-
<i>Windows Small Business Server</i>					
Windows Server Solutions Best Practices Analyzer 1.0	check	-	-	-	-
Windows Small Business Server 2003	check	-	-	-	-
Windows Small Business Server 2008 Migration Preparation Tool	check	-	-	-	-
Windows Small Business Server 2008	check	-	-	-	-
Windows Small Business Server 2011 Standard	check	-	-	-	-
<i>Windows</i>					

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS		Type of Update Supported			
EU Browser Choice Up- date-For Eu- rope Only Graphics Dri- vers for Win- dows 8.1 Up- grade	check	-	-	-	-
OOBE ZDP	check	-	-	-	-
Windows 2000	check	check	check	check	check
Windows 7 Language Packs	check	-	-	-	-
Windows 7	check	check	check	check	check
Windows 8 Language Inter- face Packs	check	-	-	-	-
Windows 8 Language Packs	check	-	-	-	-
Windows 8.1 Drivers	check	-	-	-	-
Windows 8.1 Dynamic Up- date	check	-	-	-	-
Windows 8.1 Language Inter- face Packs	check	-	-	-	-
Windows 8.1 Language Packs	check	-	-	-	-
Windows 8.1	check	check	check	check	check
Windows 8	check	check	check	check	check

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
Windows Consumer Preview Dynamic Update	check	-	-	-	-
Windows Defender	check	-	-	-	-
Windows Security Platform	check	-	-	-	-
Windows Dictionary Updates	check	-	-	-	-
Windows Embedded Standard 7	check	check	check	check	check
Windows POS Ready 7	check	check	check	check	check
Windows GDR-Dynamic Update	check	-	-	-	-
Windows Internet Explorer 7 Dynamic Installer	check	-	-	-	-
Windows Internet Explorer 8 Dynamic Installer	check	-	-	-	-
Windows Media Dynamic Installer	check	-	-	-	-
Windows Server 2003, Datacenter Edition	check	check	check	check	check
Windows Server 2003	check	check	check	check	check

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
	check	check	check	check	check
Windows Server 2008 R2	check	check	check	check	check
Windows Server 2008 Server Manager Dynamic Installer	check	-	-	-	-
Windows Server 2008	check	check	check	check	check
Windows Server 2012 Language Packs	check	-	-	-	-
Windows Server 2012 R2 Language Packs	check	-	-	-	-
Windows Server 2012 R2	check	check	check	check	check
Windows Server 2012	check	check	check	check	check
Windows Server 2016 (support includes feature updates)	check	check	check	check	check
Windows 10 1507 LTSC	check	check	check	check	check
Windows 10 1607 LTSC	check	check	check	check	check
Windows 10 1803(Enterprise and Education edition)	check	check	check	check	check
Windows 10 1809	check	check	check	check	check

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
Windows 10 1903	check	check	check	check	check
Windows 10 1909	check	check	check	check	check
Windows 10 Server 1903	check	check	check	check	check
Windows 10 Server 1909	check	check	check	check	check
Windows 10 2004	check	check	check	check	check
Windows 10 20H2	check	check	check	check	check
Windows Serv- er 2004	check	check	check	check	check
Windows Serv- er 20H2	check	check	check	check	check
Windows 11 ARM 21H2	check	check	check	check	check
Windows 11 ARM 22H2	check	check	check	check	check
Windows 11 ARM 23H2	check	check	check	check	check
Windows Serv- er 2019	check	check	check	check	check
Windows Serv- er Manager - Windows Serv- er Update Ser- vices (WSUS) Dynamic In- staller	check	-	-	-	-
Windows Ulti- mate Extras	check	-	-	-	-

Table 1. Supported operating systems and applications with the corresponding update types (continued)

Supported OS	Type of Update Supported				
Windows Vista Dynamic In- staller	check	-	-	-	-
Windows Vista Ultimate Lan- guage Packs	check	-	-	-	-
Windows Vista	check	check	check	check	check
Windows XP 64-Bit Edition Version 2003	check	check	check	check	check
Windows XP x64 Edition	check	check	check	check	check
Windows XP	check	check	check	check	check



Note: For a complete list of operating systems and applications that have Security updates support, see the following wiki topic: [Supported OS](#)



Note: Microsoft no longer supports and releases updates products that have reached their end of life (EOL). Although, BigFix no longer provides new content for products that reached its end support date, you can use standard support channels to raise concerns and for troubleshooting support for existing content. For a list of end of life products, see the *Products that have reached their end of support date* section.

Support information for Windows 10

BigFix Patches for Windows supports Windows 10 Business edition ISO for the following editions:

- Windows 10 Pro
- Windows 10 Pro N
- Windows 10 Pro for Workstations
- Windows 10 Pro N for Workstations
- Windows 10 Pro Education
- Windows 10 Pro Education N
- Windows 10 Education
- Windows 10 Education N
- Windows 10 Enterprise
- Windows 10 Enterprise N

- Windows 10 IoT Enterprise
- x86 and x64 architectures are supported.



Note: Bigfix Patches for Windows does not support consumer edition ISO.

Support information for Windows 11

BigFix Patches for Windows supports Windows 11 Business edition ISO for the following editions:

- Windows 11 Pro
- Windows 11 Pro N
- Windows 11 Pro for Workstations
- Windows 11 Pro N for Workstations
- Windows 11 Pro Education
- Windows 11 Pro Education N
- Windows 11 Education
- Windows 11 Education N
- Windows 11 Enterprise
- Windows 11 Enterprise N



Note: Bigfix Patches for Windows does not support consumer edition ISO.

Supported Click-to-Run products

BigFix supports Microsoft products that use the Click-to-Run technology.

Table 2. Supported Office 365 - Office 2013 PC applications and channels

Office 365 subscription plan	Office 2013 - PC version
Office 365 ProPlus	<ul style="list-style-type: none"> • Access • Excel • InfoPath • OneNote • Outlook • PowerPoint • Publisher • Skype for Business • Word
Office 365 Enterprise E3	<ul style="list-style-type: none"> • Access • Excel

Table 2. Supported Office 365 - Office 2013 PC applications and channels (continued)

Office 365 subscription plan	Office 2013 - PC version
	<ul style="list-style-type: none"> • InfoPath • OneNote • Outlook • PowerPoint • Publisher • Skype for Business • Word
Office 365 Enterprise E5	<ul style="list-style-type: none"> • Access • Excel • InfoPath • OneNote • Outlook • PowerPoint • Publisher • Skype for Business • Word

Table 3. Supported Office 365 - Office 2016 PC applications and channels

Office 365 subscription plan	Supported PC applications	Supported update channels for clients	Supported types of updates
Office 365 ProPlus	<ul style="list-style-type: none"> • Access • Excel • InfoPath • OneNote • Outlook • PowerPoint • Publisher • Skype for Business • Word 	<ul style="list-style-type: none"> • Current channel • Deferred channel • First release for deferred channel 	<ul style="list-style-type: none"> • Security updates • Non-security updates • Feature updates
Office 365 Enterprise E3	<ul style="list-style-type: none"> • Access • Excel • OneNote • Outlook 		

Table 3. Supported Office 365 - Office 2016 PC applications and channels (continued)

Office 365 sub- scription plan	Supported PC applications	Supported update channels for clients	Supported types of updates
	<ul style="list-style-type: none"> • PowerPoint • Publisher • Skype for Business • Word 		
Office 365 Enterprise E5	<ul style="list-style-type: none"> • Access • Excel • OneNote • Outlook • PowerPoint • Publisher • Skype for Business • Word 		

Table 4. Supported Office 365 - Office 2016 PC applications and channels

Office 365 subscription	Supported products	Supported update channels for clients	Supported types of updates
Microsoft Office 365 apps	<ul style="list-style-type: none"> • Access • Excel • OneNote • Outlook • PowerPoint • Publisher • Skype for Business • Word 	<ul style="list-style-type: none"> • Current channel • Monthly enterprise channel • Semi-annual enterprise channel (pre-view) • Semi-annual enterprise channel 	<ul style="list-style-type: none"> • Security updates • Non-security updates • Feature updates

Supported Windows Management Framework (WMF) and .NET Framework versions**Supported Windows Management Framework versions**

Table 5. Supported Windows Management Framework versions

Windows Management Framework version	Supported products
Windows Management Framework 5.1	<ul style="list-style-type: none"> • Windows 8.1 (x86) • Windows 8.1 (x64) • Windows 7 SP1 (x86) • Windows 7 SP1 (x64) • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2008 R2 SP1

Supported .NET Framework versions**Table 6. Supported .NET Framework versions**

.NET Framework versions	Supported products
4.8	Windows 10, Windows Server 2016, Windows 8.1, Windows 7 Embedded, Windows Server 2012, Windows Server 2012 R2
4.7	Windows 10, Windows 8.1, Windows 7 Service Pack 1, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2 SP1
4.6.2	Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 7, Windows Server 2008 R2
4.6.1	Windows 8.1, Windows Server 2012, Windows Server 2012 R2,
4.6	Windows 8.1, Windows 7, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server 2008
4.5.2	Windows 8.1, Windows 7, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server 2008
4.0	WES09 and POSReady 2009
3.5.1	Windows 7, Windows Server 2008 R2

Table 6. Supported .NET Framework versions (continued)

.NET Framework versions	Supported products
3.5	Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
2.0	Windows Server 2008
2.0 SP2	WES09 and POSReady 2009

Supported third party applications

Third party applications are found in the Updates for Windows Applications site. Some applications are supported with audit Fixlets. Audit Fixlets will only indicate that the application is outdated. Users must manually apply the update.

Use the Fixlet Maker dashboard to create the necessary Fixlets to patch the applications. For more information, see the following topics:

- [Fixlet Maker dashboard overview \(on page 73\)](#)
- [Creating custom Fixlets from templates \(on page 75\)](#)

Table 7. Applications that are supported in the Updates for Windows Applications site

Application	Version	Type of update	
		Standard application support date	Audit Fixlet support date
Adobe Reader	9.5, 11.x, 2015.xx.xxxxx, 2017.xx.xxxxx, 2018.xx.xxxxx, 2019.xx.xxxxx, 2020.xx.xxxxx, 2021.xx.xxxxx, 2022.xx.xxxxx, 2023.xx.xxxxx, 2024.xx.xxxxx	✓	-
Apple iTunes	12.7, 12.8, 12.9, 12.10, 12.11, 12.12, 12.13	✓	-
Skype	8.x	✓	-
Oracle Java™ Runtime Environment	8U1xx, 8U2xx, 8U3xx	✓	-

Table 7. Applications that are supported in the Updates for Windows Applications site (continued)

Appli- cation	Version	Type of update
Google Chrome	79.x, 80.x, 81.x, 83.x, 84.x, 85.x, 86.x, 87.x, 88.x, 89.x, 90.x, 91.x, 92.x, 93.x, 94.x, 95.x, 96.x, 97.x, 98.x, 99.x, 100.x, 101.x, 102.x, 103.x, 104.x, 105.x, 106.x, 107.x, 108.x, 109.x, 110.x, 111.x, 112.x, 113.x, 114.x, 115.x, 116.x, 117.x, 118.x, 119.x, 120.x, 121.x, 122.x	✓ -
Mozilla Firefox	68.x, 69.x, 70.x, 71.x, 72.x, 73.x, 74.x, 75.x, 76.x, 77.x, 78.x, 79.x, 80.x, 81.x, 82.x, 83.x, 84.x, 85.x, 86.x, 87.x, 88.x, 89.x, 90.x, 91.x, 92.x, 93.x, 94.x, 95.x, 96.x, 97.x, 98.x, 99.x, 100.x, 111.x, 112.x, 113.x, 114.x, 115.x, 116.x, 117.x, 118.x, 119.x, 120.x, 121.x, 122.x 123.x	✓ -
Mozilla Firefox ESR	60.x, 68.x, 78.x, 91.x, 102.x, 115.x	✓ -
Mozil- la Thun- derbird	60.x, 68.x, 78.x, 91.x, 102.x, 115.x	✓ -
Notepad ++	7.x.x, 8.x.x	✓ -
Zoom	5.1.xxxx.xxxx, 5.2.xxxx.xxxx, 5.3.xxxx.xxxx, 5.4.xxxx.xxxx, 5.5.xxxx.xxxx, 5.6.x.xxxx, 5.7.x.xxxx, 5.8.x.xxxx, 5.9.x.xxxx, 5.10.x.xxxx, 5.11.x.xxxx, 5.12.x.xxxx, 5.13.x.xxxx, 5.14.x.xxxx, 5.15.x.xxxx, 5.16.x.xxxx, 5.17.x.xxxx	✓ -
Webex	40.x.x.xx, 41.x.x.xx, 42.x.x.xx, 43.x.x.xx, 44.x.x.xx	✓ -
GoTo- Meeting	10.11.1.18068, 10.12.0.18425, 10.13.1.18705, 10.14.0.18962, 10.15.0.19228, 10.16.0.19598, 10.17.0.19796, 10.18.0.19932, 10.19.0.19950	✓ -
Mi- crosoft Edge	84.x.xxx.xx, 86.x.xxx.xx, 87.x.xxx.xx, 88.x.xxx.xx, 89.x.xxx.xx, 90.x.xxx.xx, 91.x.xxx.xx, 92.x.xxx.xx, 93.x.xxx.xx, 94.x.xxx.xx, 95.x.xxx.xx, 96.x.xxx.xx, 96.x.xxx.xx, 97.x.xxx.xx, 98.x.xxx.xx, 99.x.xxx.xx, 100.x.xxx.xx, 101.x.xxx.xx, 102.x.xxx.xx, 103.x.xxx.xx, 104.x.xxx.xx, 105.x.xxx.xx, 106.x.xxx.xx, 107.x.xxx.xx, 108.x.xxx.xx, 109.x.xxx.xx, 110.x.xxx.xx, 111.x.xxx.xx, 112.x.xxx.xx	✓ -
ASP.NET Core Runtime	3.x.xx, 5.x.xx, 6.x.xx, 7.x.xx, 8.x.xx	✓ -
.NET Desktop Runtime	3.x.xx, 5.x.xx, 6.x.xx, 7.x.xx, 8.x.xx	✓ -
.NET Runtime	3.x.xx, 5.x.xx, 6.x.xx, 7.x.xx, 8.x.xx	✓ -

Table 8. Applications that are not supported currently in the Updates for Windows Applications site

Application	Version
Adobe Reader X	10.1.16
Adobe AIR	18.0, 29.0, 30.0, 31.0, 32.0
Adobe Acrobat X	10.1.16
Adobe Digital Editions	4.5.8, 4.5.9, 4.5.10, 4.5.11
Adobe Shockwave Player	12.3.5.205
Apple QuickTime	7.1.6, 7.2, 7.7.9
ImgBurn	2.5.8.0
RealPlayer	11, 16.0.3.51
Winamp	5.6.6.3512
WinZip	11.2, 12.1, 14.0, 14.5, 15.0, 15.5, 16.5, 16.5 (x64), 18.0, 18.0 (x64), 18.5, 18.5 (x64), 20.0 (x64), 20.5, 20.5 (x64), 21.0, 21.0 (x64), 22.0, 22.0 (x64)

Table 9. Adobe Document Cloud

Adobe Product	Track	Version
Adobe Acrobat DC	Classic	2015, 2017, 2020
	Continuous	2020, 2021, 2022
Adobe Acrobat Reader DC	Classic, Continuous	2015, 2017, 2020
	Continuous	2020, 2021, 2022

Table 10. Websphere Application Server

WAS Product	Series	Version
Interim Fix	8.0.0	8.0.0.11, 8.0.0.12, 8.0.0.13, 8.0.0.14, 8.0.0.15
	8.5.5	8.5.5.7, 8.5.5.8, 8.5.5.9, 8.5.5.10, 8.5.5.11, 8.5.5.12, 8.5.5.13,

Table 10. Websphere Application Server (continued)

		8.5.5.14, 8.5.5.15, 8.5.5.16, 8.5.5.17, 8.5.5.18
FixPack	V8.0	V8.0 (Base & ND) Fix Pack 15
	V8.5	V8.5.5 (Base & ND) Fix Pack 16,
		V8.5.5 (Base & ND) Fix Pack 17,
		V8.5.5 (Base & ND) Fix Pack 18

**Note:**

- HCL BigFix does not support beta versions of these listed applications.
- BigFix provides Fixlets that are categorized as "Upgrade" to accommodate upgrades to newer major versions of Oracle Java™ Runtime Environment.
- BigFix provides support for 86-bit of windows applications compatible with x64 machines.
- BigFix does not support the use of 32-bit and 64-bit versions of Oracle Java™ Runtime Environment in the same machine.
- Currently, BigFix supports only the MSI version of zoom, Google Chrome, GoToMeeting, Microsoft Edge, and Webex Apps which are the IT admin installer. BigFix does not support .exe based installation of zoom, Google Chrome, GoToMeeting, Microsoft Edge, and Webex Apps.
- The versions mentioned are in order of initial version to latest version supported.
- Only the current version is available for deployment and all the earlier versions are superseded.
- Other than the mentioned versions, no future updates are supported currently for Adobe Shockwave Player, Apple QuickTime Player, Winamp, ImgBurn, WinZip, and Real Player.
- To check if any update released is supported or not, look for term *-WS-WAS-* in the update name. If the term contains *-WS-WASJAVASDK-* or *-WS-WAS*.* then those updates are not supported. The examples are as follows:
 - 9.x - Not supported
 - 8.5.5.9-WS-WAS-IFPI73197 - Supported
 - 8.0.0.0-WS-WASJavaSDK8-OS390-IFPI93093 - Not Supported
 - 8.5.5.11-WS-WASBundledSDK8-OS390-IFPI93094 - Not Supported
 - 8.0.0.0-WS-WASJavaSDK8-WinX64-IFPI93093 - Not Supported
 - 8.0.0.0-WS-WASJavaSDK8-WinX32-IFPI93093 - Not Supported
 - 8.5.5.11-WS-WASBundledSDK8-WinX32-IFPI93094 - Not Supported
 - 8.0.0.0-WS-WASJavaSDK8-WinX32-IFPI93093 - Not Supported

For supported languages, see https://help.hcl-software.com/bigfix/10.0/patch/Patch/Patch_Windows/c_other_languages.html

Products that have reached their end of support date

Microsoft products have a lifecycle that ends when the product is no longer supported. When a product reaches end of life (EOL) or its end of support date, Microsoft no longer supports and releases updates for the product, including automatic fixes, updates, and online technical assistance.

BigFix, in turn, no longer provides security and non-security content and support for products that reached its end of support date. However, users of existing Windows content can use the standard HCL support channels to raise concerns and for troubleshooting support.

Microsoft provides extended support for some products that have reached their end of life. If you signed for extended support with Microsoft, it is suggested that you contact your HCL account representative. To see information about product offerings, see <https://support.hcltechsw.com/csm>.

Table 11. .NET Framework products that reached their end of support date

.NET Framework

.NET Framework 1.1 Gold and earlier
 .NET Framework 2.0 SP1 and Earlier
 .NET Framework 3.5 Gold and Earlier

Table 12. Microsoft Exchange Server products that reached their end of support date

Microsoft Exchange Server

Microsoft Exchange Server 5.0
 Microsoft Exchange Server 5.5
 Microsoft Exchange Server 2003 Enterprise Edition
 Microsoft Exchange Server 4.0 Service Pack 1

Table 13. Office products that have reached their end of life

Office

Office 2000 and Earlier

Office 2003 SP2 and Earlier

Office 2007

Office 2007 SP1 and Earlier

Office 97

Office XP SP2 and Earlier

Table 14. Office Communicator product that has reached its end of life

Office Communicator

Office Communicator
2007

Table 15. SQL Server products that have reached their end of life

SQL Server

SQL Server 2000 SP3a and Earlier

SQL Server 2000 SP3a and Earlier (Analysis Services)

SQL Server 2000 SP3a and Earlier (BES MSDE)

SQL Server 2000 SP3a and Earlier (Client Tools Only)

SQL Server 2005 SP3 and Earlier

SQL Server 2008 SP1 and Earlier

SQL Server 7.0 SP3 and Earlier

Table 16. Windows products that have reached their end of life

Windows
Windows 2000 and all its editions
Windows 2000 SP4 and Earlier
Windows 7 Gold
Windows 98
Windows NT 4.0
Windows Server 2003 SP1 and Earlier
Windows Server 2008 Gold
Windows Server 2008 R2 Gold
Windows Vista
Windows Vista SP1 and Earlier
Windows XP
Windows XP Gold (x64)

Other languages supported

BigFix 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 17. Other languages supported by the Patch Management for Windows and Patch Management for Windows Application site

Other languages supported

Other languages supported by the Patches for Windows site	Other languages supported by the Windows Application Updates site
Brazilian Portuguese	Brazilian Portuguese
Czech	British English (Only for Mozilla Firefox)
Chinese (Simplified)	Chinese (Simplified)
Chinese (Traditional)	Chinese (Traditional)

Table 17. Other languages supported by the Patch Management for Windows and Patch Management for Windows Application site

Other languages supported

(continued)

Danish	Czech
Dutch	French
Finnish	German
French	Hungarian
German	Italian
Greek	Japanese
Hebrew	Korean
Hungarian	Polish
Italian	Russian
Japanese	Spanish
Korean	-
Norwegian	-
Polish	-
Russian	-
Spanish	-
Swedish	-
Turkish	-

When you purchase 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 from the HCL support website at [BigFix Support Portal](#).



Note: It is highly suggested that users install applications that have the same language version as their operating system.

Site subscription

Sites are collections of Fixlet messages that are created internally by you, by HCL, or by vendors.

Subscribe to a site to access the Fixlet messages to patch systems in your deployment.

You can add a site subscription by acquiring a Masthead file from a vendor or from HCL or by using the Licensing Dashboard. For more information about subscribing to Fixlet sites, see the *BigFix Installation Guide*.

For more information about sites, see the *BigFix Console Operator's Guide*.

Fixlet fields

Fixlet fields provide essential information about Fixlets, helping them assess the importance, relevance, and impact of deploying a particular Fixlet to their systems.

Fixlets contain fields of metadata that provide specific details. Some Fixlet fields are common across all domains, that is, categories of BigFix sites. Other fields are common to only one domain or product, such as Patch Management.

The following table lists the Fixlet fields and their descriptions.

Table 18. Fixlet fields and descriptions

Fixlet fields	Description	BigFix domain
ID	A numerical ID assigned to the Fixlet by the author.	All
Name	The name assigned to the Fixlet by the author.	All
Applicable Computer Count	The number of BigFix clients in the network currently affected by the Fixlet.	All
Category	The type of Fixlet, such as a Security Patch or Update.	All
Download Size	The size of the remedial file or patch that the action downloads.	All
Source	The name of the source vendor that provides the Fixlet information.	All
Source ID	A numerical ID assigned to the Fixlet to relate it back to its source.	All
Source Release Date	The date when an upstream vendor releases the patch.	All
Source Severity	A measure of how critical a Fixlet is, assigned by the Fixlet author. Typical values are Critical, Important, Moderate, or Low.	All
Site	The name of the site that is generating the relevant Fixlet.	All
Unlocked Computer Count	The number of unlocked computers that are affected by the Fixlet.	All

Table 18. Fixlet fields and descriptions**(continued)**

Fixlet fields	Description	BigFix domain
Open Action Count	The number of distinct actions that are open for the given Fixlet.	All
X-Fixlet-product-family	The product family that the patch belongs to.	Windows Patching (Relates to BigFix Patch Management)
X-Fixlet-product	The product that the patch belongs to under a certain product family.	Windows Patching (Relates to BigFix Patch Management)
X-Fixlet-component	A component that the patch targets under a certain product family.	Windows Patching (Relates to BigFix Patch Management)
Modification Time	The time when a given Fixlet was last modified.	All
X-Fixlet-first-propagation	The Fixlet release date.	All

Chapter 3. Patch for Windows

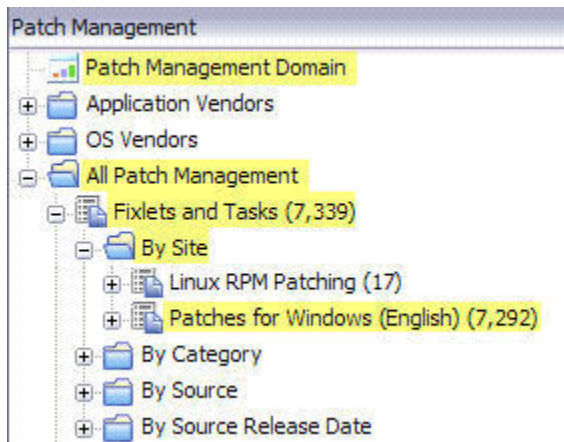
You can manage Fixlets using dashboards, reports, and wizards. You can deploy, fix, and uninstall Fixlets. You can also view the breakdown of Fixlets available or needed in your deployment.

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 BigFix 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.

All Fixlets and Tasks		Search All Fixlets and Tasks			
Name	Source Severity	Site	Applicable Computer Count	Open Acti	
UPDATE: Windows Server 2003 Service Pack 2 Available - Windows XP/2003 (x64)	Critical	Patches for Wind...	1 / 67	0	
UPDATE: Windows Server 2003 Service Pack 2 Available - Pending Restart - Windows ...	Critical	Patches for Wind...	1 / 67	0	
UPDATE: Windows Server 2003 Service Pack 2 Available	Critical	Patches for Wind...	2 / 67	0	
UPDATE: Windows Server 2003 Service Pack 2 Available - Pending Restart	Critical	Patches for Wind...	2 / 67	0	
MS01-056: "Unchecked Buffer" in Windows Media Player .ASF Processor	Critical	Patches for Wind...	1 / 67	0	
MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution - Windows...	Critical	Patches for Wind...	2 / 67	0	

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. You can set more parameters in the Take Action dialog.

For detailed information about setting parameters with the Take Action dialog, see the [BigFix 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.

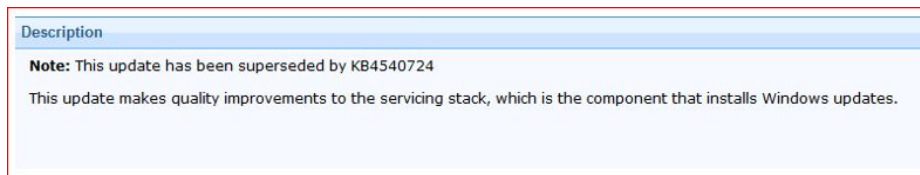
Supersedence in Windows

Windows supersedence refers to the process by which a newer version of a software or update replaces and makes the previous version obsolete.

Supersedence is a property of Fixlets used in BigFix that provides multiple packages.

Superseded Fixlets are Fixlets that contain outdated packages. When a Fixlet is superseded, a newer Fixlet is created to replace it with the newer version of the packages. The description of the Superseded Fixlet contains the new Fixlet ID.

Figure 1. Superseded Fixlets



Understanding how Supersedence works in Patch

1. Superseded patches with *FALSE* Statement.

When the Windows application patches are superseded, BigFix does not allow you to install them by adding a relevance statement set to *FALSE*. These Fixlets will no longer become relevant for endpoints and you can use the latest Fixlet to patch your endpoints.

2. Superseded Controlled Patches.

In the latest version of BigFix Patch, there is an option to continually evaluate the applicability of the superseded patches.

- Superseded Windows OS patches maintain their current applicability relevance and introduces an option to continue reporting relevant to endpoints that have not yet installed a patch (or a Superseding Patch).
- This change allows you to continue reporting on older OS vulnerabilities because Superseded Patches can continue to report applicability when the vulnerability has not been patched.

To deploy a Superseded Patch on an endpoint, set the client configuration parameter **`_BESClient_WindowsOS_EnableSupersededEval`** to 1.

For details on client configuration settings, see [BigFix Configuration Settings](#).



Note: BigFix does not supersede security updates with non-security updates because the security information (CVE-Values) is tied to a specific security update as well as the classification ("security update" vs "update"). Superseding them results in false security report.

For example, if you do not patch the latest updates on endpoints and you supersede the security updates, then you see only the non-security updates relevant, since it is not a security update. The report says that you do not have to do anything because endpoint is secure which is incorrect.



Note: Fixlets that are in a superseded state for more than a year will be removed and moved into an archive site. If any customer wants the masthead for an archived site, they should reach out to their BigFix Point of Contact.

Windows Patch Client settings

Windows patch client settings refer to the configurations and preferences established within the Windows operating system for managing and applying software patches, updates, and fixes.

BigFix Patch introduces the following Client settings which are used in Windows patching module:

- **_BESClient_WindowsOS_BypassPendingRestartRelevance**

All Windows Fixlets that include *not pending restart* relevance recognizes the **_BESClient_WindowsOS_BypassPendingRestartRelevance** Client setting.

When the **_BESClient_WindowsOS_BypassPendingRestartRelevance** is set to **1**, the Client computer ignores the *not pending restart* relevance Fixlets that are checking for Client setting. This helps in generating an accurate patching report or compliance report.

If the setting does not exist or if **_BESClient_WindowsOS_BypassPendingRestartRelevance** is set to 0, the *not pending restart* relevance statement takes into effect.

- **_BESClient_WindowsOS_EnableSupersededEval**

The latest version of the BigFix Patch supports evaluating the applicability of the superseded patches. This provides you with an option to continue reporting relevance to endpoints that do not have patch installed (or a superseding patch).

Setting the client configuration parameter **_BESClient_WindowsOS_EnableSupersededEval** to **1** deploys the Superseded Patch on an endpoint.

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.

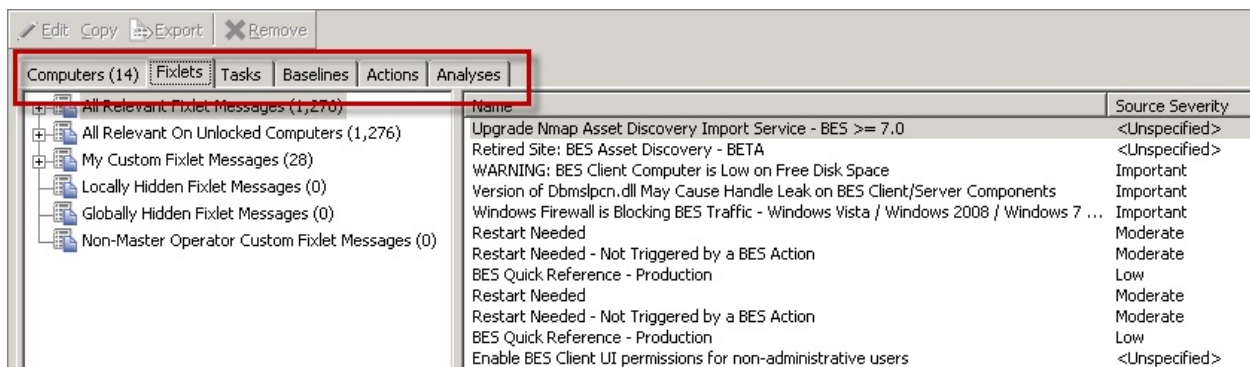
The Patches for Windows Overview dashboard displays a summary of patch information in your deployment using tables, graphs, and pie charts. From the **Patch Management** domain, click **OS Vendors > Microsoft Windows > Reports > Patches for Windows Overview**.

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.

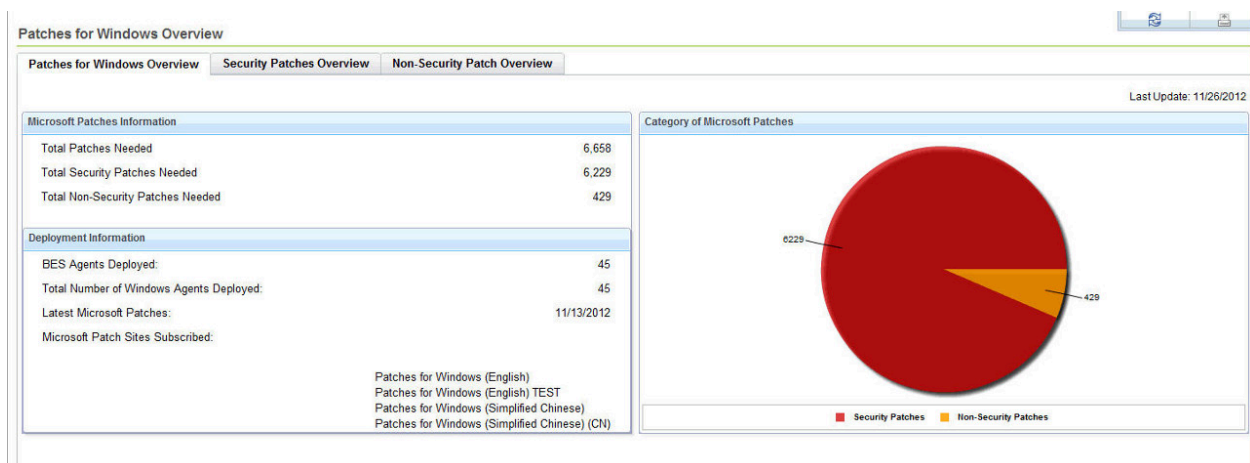
The Security Patches Overview and Non-Security Patch Overview tabs have a different link for computers that need at least one patch. The Security Patches Overview tab has the *Computers Needing at least one Critical Patch*; the Non-Security Patches Overview tab has the *Computers Needing at least one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



Computers (14) Fixlets Tasks Baselines Actions Analyses		Name	Source Severity
All Relevant Fixlet Messages (1,270)		Upgrade Nmap Asset Discovery Import Service - BES >= 7.0	<Unspecified>
All Relevant On Unlocked Computers (1,276)		Retired Site: BES Asset Discovery - BETA	<Unspecified>
My Custom Fixlet Messages (28)		WARNING: BES Client Computer is Low on Free Disk Space	Important
Locally Hidden Fixlet Messages (0)		Version of Dbmslpncn.dll May Cause Handle Leak on BES Client/Server Components	Important
Globally Hidden Fixlet Messages (0)		Windows Firewall is Blocking BES Traffic - Windows Vista / Windows 2008 / Windows 7 ...	Important
Non-Master Operator Custom Fixlet Messages (0)		Restart Needed	Moderate
		Restart Needed - Not Triggered by a BES Action	Moderate
		BES Quick Reference - Production	Low
		Restart Needed	Moderate
		Restart Needed - Not Triggered by a BES Action	Moderate
		BES Quick Reference - Production	Low
		Enable BES Client UI permissions for non-administrative users	<Unspecified>

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 BigFix 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.

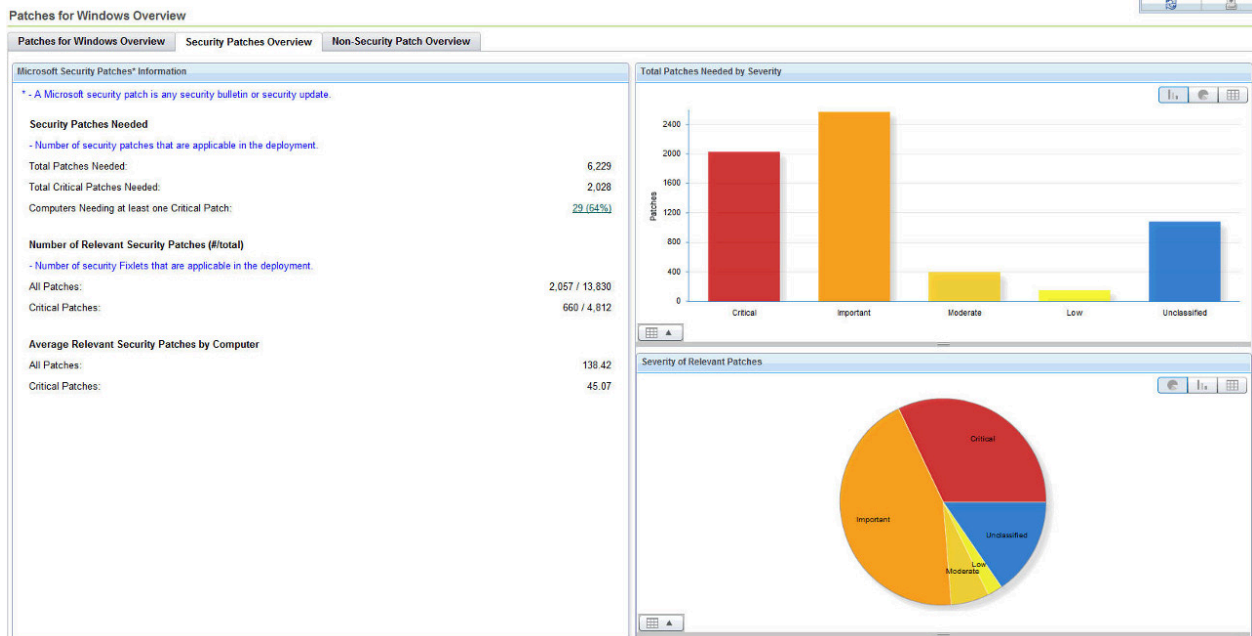
Number of Relevant Security Patches

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.

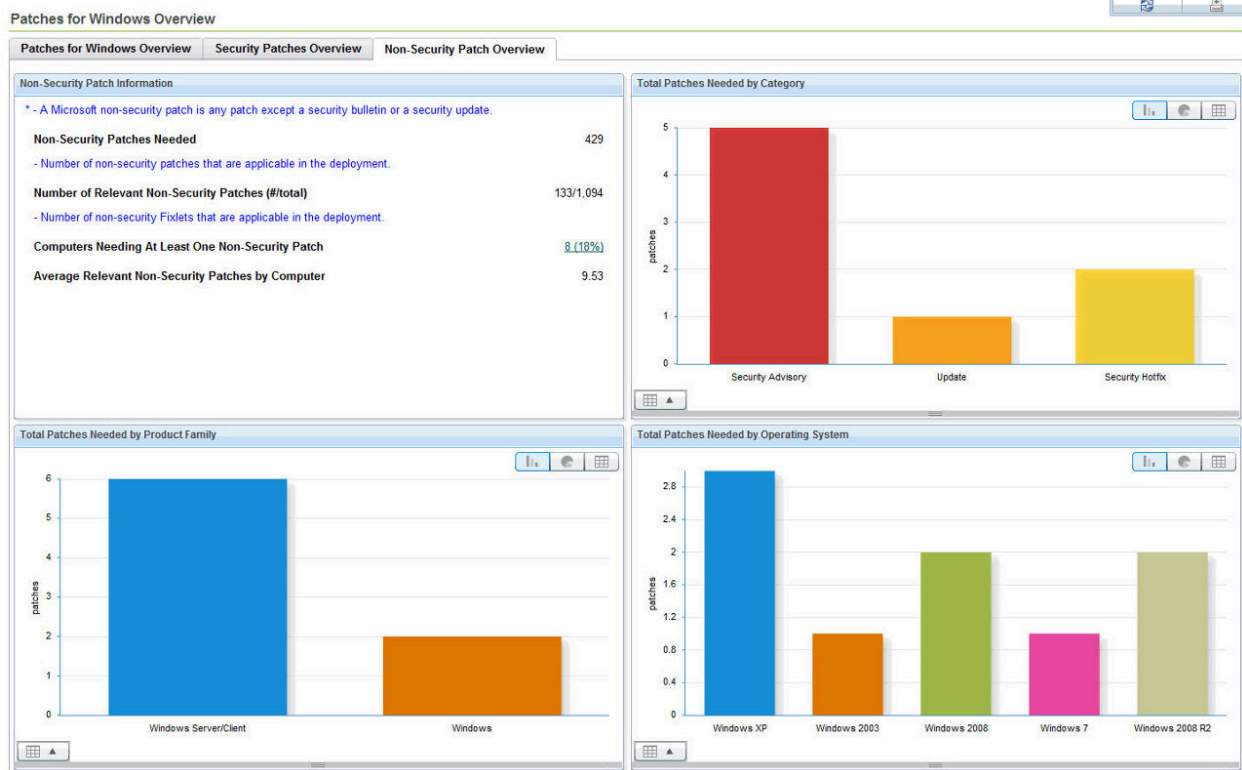


Non-Security Patches Overview tab

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*

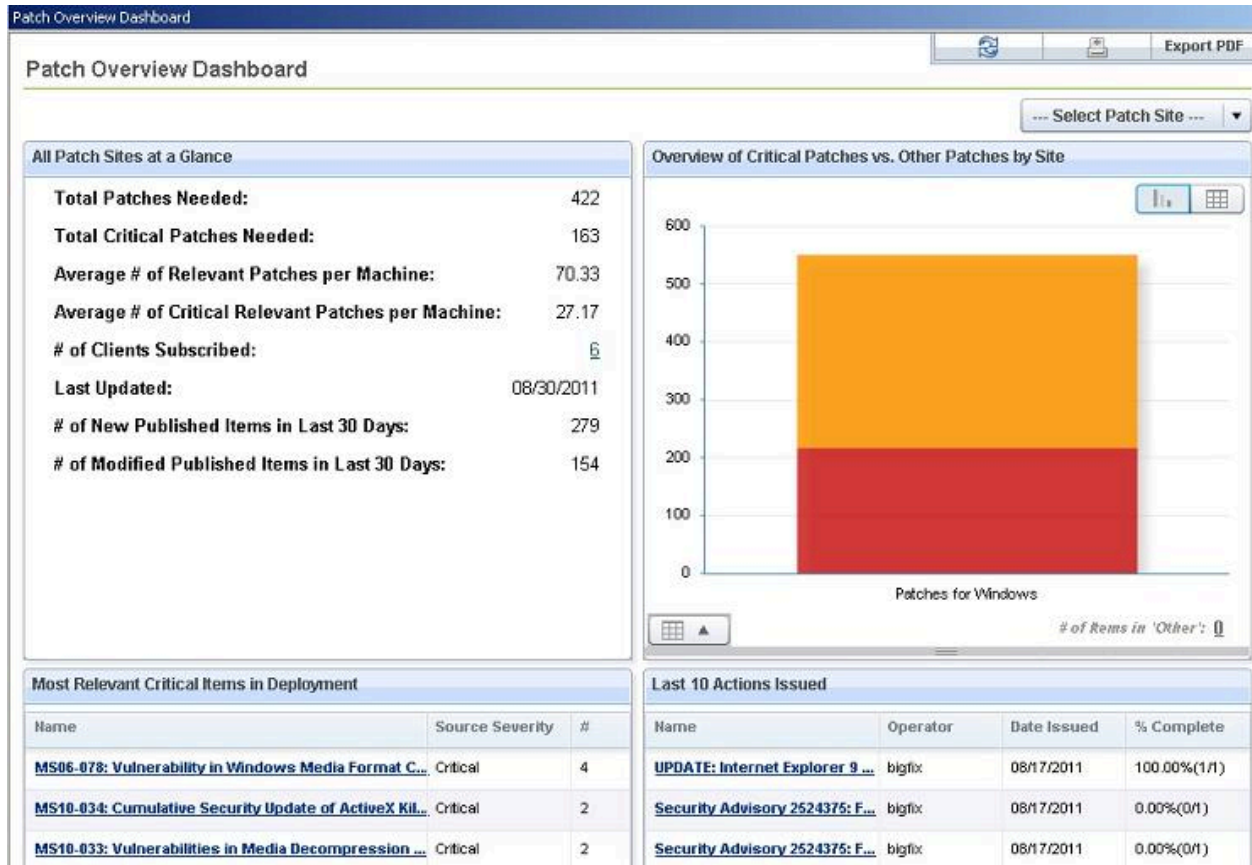
The tab also has a chart that categorizes the total patches that are needed according to product family, category, and operating system.



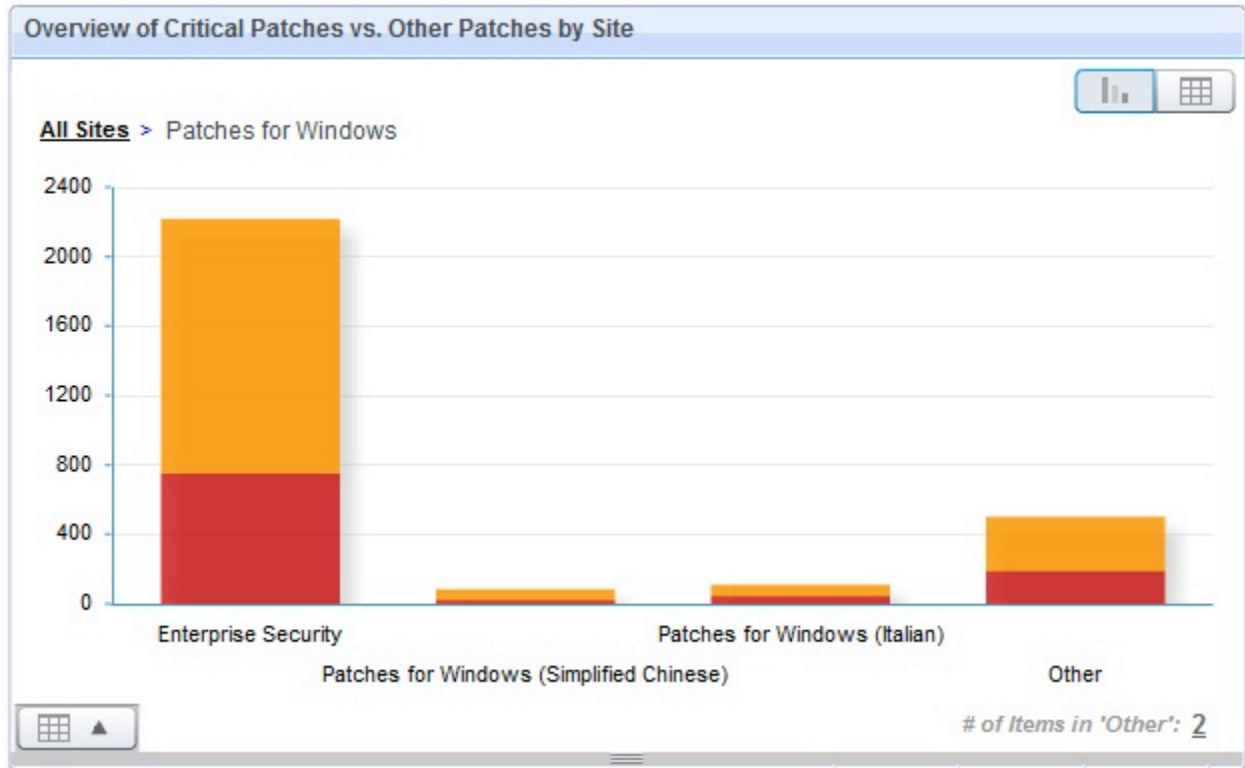
Patch Overview dashboard

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 BigFix 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*.

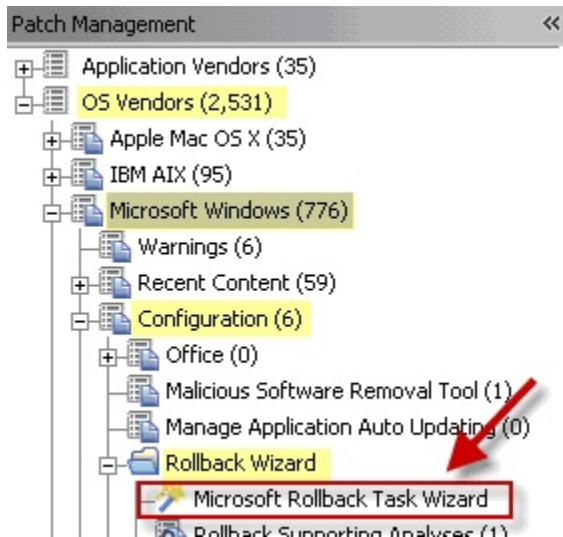
Using the Rollback Task wizard

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

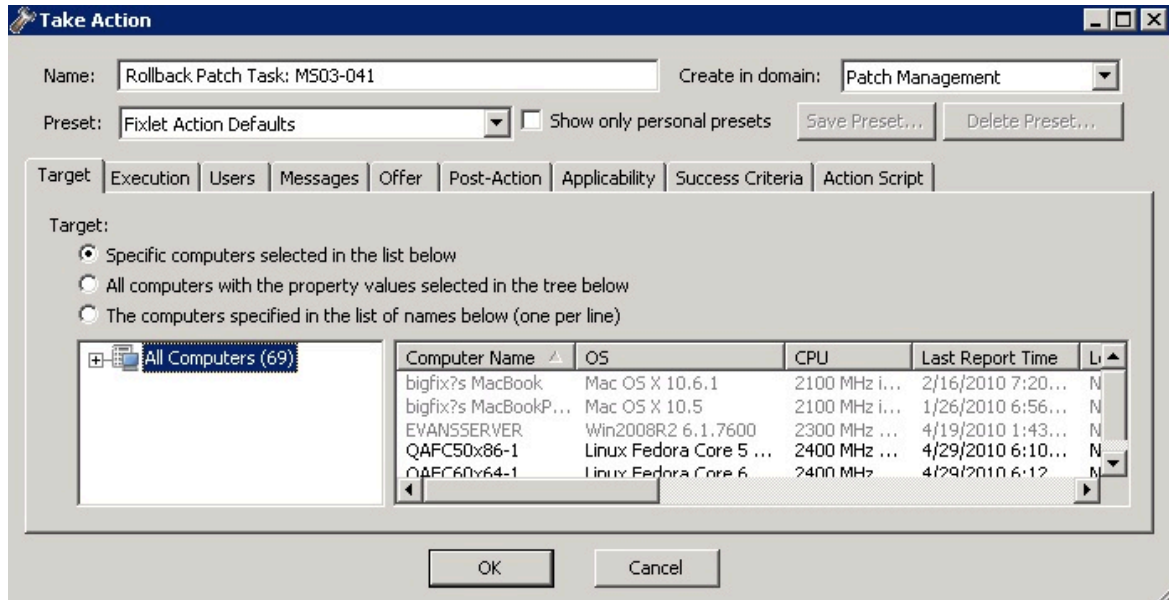
in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\key`. The key must be the KB number for the patch you want to roll back.

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 [Overview \(on page 7\)](#).

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 BigFix 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 BigFix 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.

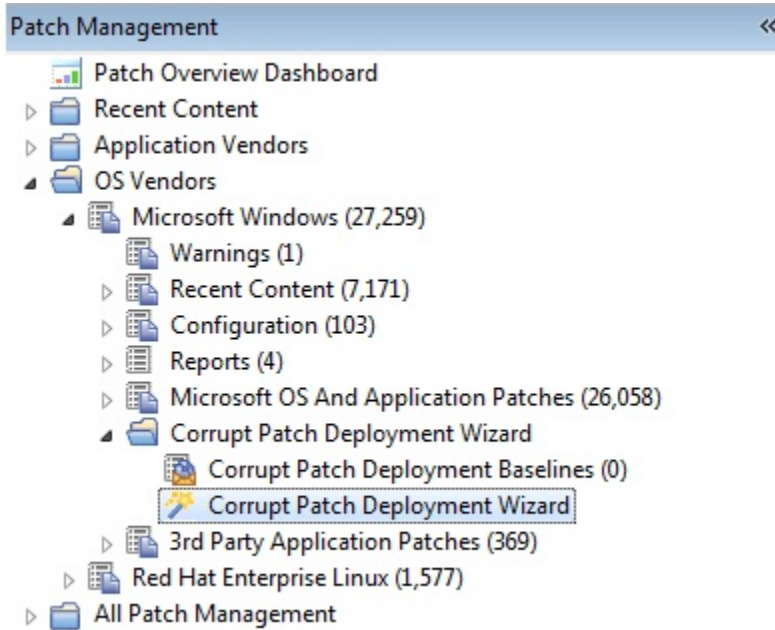
If a machine has multiple corrupt Fixlets that are applicable, you can apply them all at the same time by using the Corrupt Fixlet Deployment Wizard.

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.

Corrupt Patch Deployment Wizard

Welcome to the Corrupt Patch Deployment Wizard! This wizard helps you deploy corrupt patch Fixlets and generates a corrupt patches baseline. You can either pick and choose among Patches for Windows corrupt patches, or you can choose from baselines you have already created, or just copy and paste Fixlets from the Console (ID field has to be the first field and the Site field must be present). For more information about corrupt patches, see BigFix KB #166.

Option 1: Deploy corrupt patch Fixlets or create a new baseline of corrupt patches:

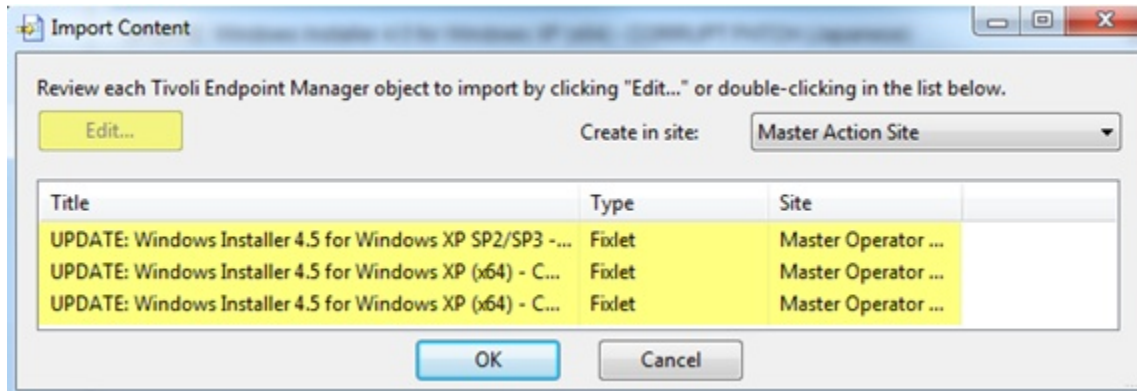
Fixlet Name	Fixlet ID	Site	Applicable ...
UPDATE: Windows Installer 4.5 for Windows XP SP2/SP3 - CORRUPT PATCH (Japanese)	25216	Patches for Windows (Japanese) Test	?
UPDATE: Windows Installer 4.5 for Windows XP SP2/SP3 - CORRUPT PATCH (Simplified Chinese)	25216	Patches for Windows (Simplified Chinese)	?
UPDATE: Windows Installer 4.5 for Windows XP (x64) - CORRUPT PATCH	25218	Patches for Windows (English)	?
UPDATE: Windows Installer 4.5 for Windows XP (x64) - CORRUPT PATCH (Italian)	25218	Patches for Windows (Italian)	?
UPDATE: Windows Installer 4.5 for Windows XP (x64) - CORRUPT PATCH (Spanish)	25218	Patches for Windows (Spanish)	?
UPDATE: Windows Installer 4.5 for Windows XP (x64) - CORRUPT PATCH (Japanese)	25218	Patches for Windows (Japanese)	?

Create Baseline
 Create Modified Fixlets

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, BigFix provides different ways to deploy Microsoft Office updates and patches:

- Administrative
- Network
- Local

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



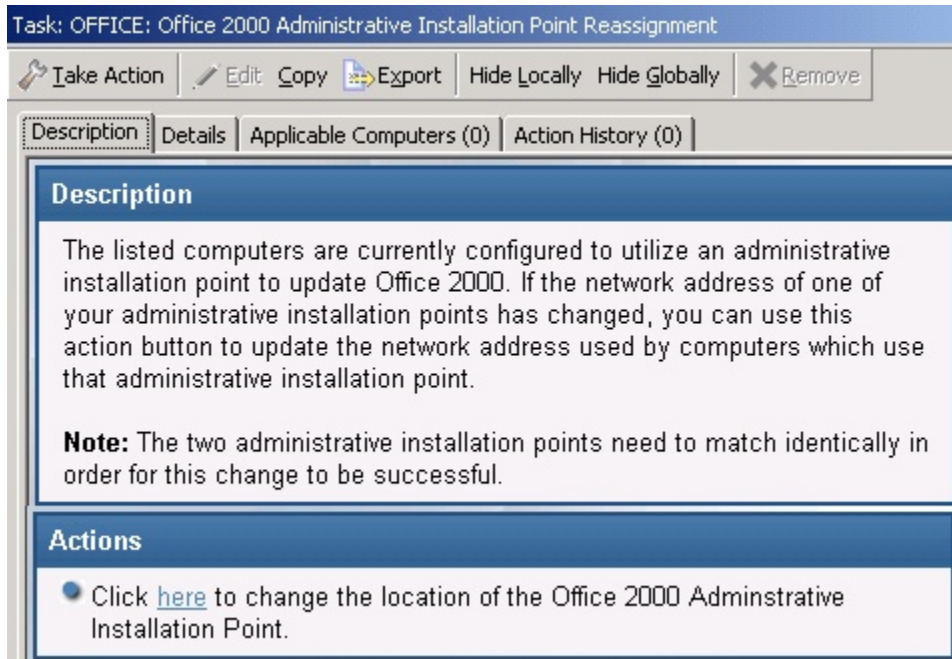
Note: The deployment of updates and patches using *Administrative*, *Network*, and *Local* ways apply to Microsoft Office versions earlier than Microsoft Office 2007.

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.

Chapter 4. Installing and updating Click-to-Run products

Install and update content for Microsoft Click-to-Run products through BigFix Patches for Windows.

BigFix Patches for Windows provides support for Microsoft updates that are installed through Click-to-Run, instead of the Windows installer-based method (MSI). Click-to-Run is a streaming and virtualization Microsoft technology that install and update Microsoft products, including Office 365 and Office 2016. BigFix Patches for Windows helps users with the following features:

- Detect outdated Office 365 and Office 2016 products
- Configure the update source settings of Office 365 Click-to-Run updates to come from the web, a network share location, or from a client cache folder through the BigFix architecture
- Remove the update source settings for Office 365 Click-to-Run updates
- Maintain an updated network share
- Enable and disable automatic updates
- Check the Office 365 configuration of machines

Microsoft Click-to-Run technology

Click-to-Run is a streaming and virtualization Microsoft technology that installs Office products such as Office 365 and the single purchase version of Office 2016. Click-to-Run updates do not use MSI, MSP, and Windows Server Update Services (WSUS). Office products that use Click-to-Run can receive automatic updates from Microsoft through the web or download from an on-premises location. The Office Deployment tool is used to manage Click-to-Run installations.

The Office Deployment Tool supports the following operating systems:

Table 19. Operating systems that are supported by the Office Deployment Tool

Office products	Operating systems
Office 2013	<ul style="list-style-type: none">• Windows 7• Windows 8• Windows Server 2008 R2• Windows Server 2012
Office 2016	<ul style="list-style-type: none">• Windows 10• Windows 7• Windows 8• Windows 8.1

Table 19. Operating systems that are supported by the Office Deployment Tool (continued)

Office products	Operating systems
	<ul style="list-style-type: none"> • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2

For more information about Click-to-Run, see <https://docs.microsoft.com/en-us/office/troubleshoot/office-suite-issues/office-click-to-run-installation>.

For more information about Office Deployment Tool, see the following links:

- Office 2013 Deployment Tool: <https://www.microsoft.com/en-sg/download/details.aspx?id=36778>
- Office 2016 Deployment Tool : <https://www.microsoft.com/en-us/download/details.aspx?id=49117>

Supported applications

BigFix Patches for Windows supports applications and, if applicable, subscription plans for the following Microsoft products that use Click-to-Run.

- Office 365 – Office 2013 PC applications
- Office 365 – Office 2016 PC applications
- Office 2016 (single purchase version)

For more detailed information about the supported application, see [Supported operating systems, products, and updates \(on page 7\)](#).

Supported product IDs for Office 365

For Current, Monthly Enterprise, Semi-Annual, and Semi-Annual Preview Channels, BigFix offers support for the following product IDs in Office 365 which are O365ProPlusRetail, O365BusinessRetail, ProPlus2019Retail, and ProPlus2021Retail.

Additionally, for perpetual channel, BigFix extends support to ProPlus2019Volume and ProPlus2021Volume

The following product IDs for office 365 are supported by BigFix:

- O365ProPlusRetail
- O365BusinessRetail
- ProPlus2019Retail
- ProPlus2021Retail
- ProPlus2019Volume
- ProPlus2021Volume

Installing and updating Click-to-Run products

Install and update content for Microsoft Click-to-Run products through BigFix Patches for Windows.

BigFix Patches for Windows provides support for Microsoft updates that are installed through Click-to-Run, instead of the Windows installer-based method (MSI). Click-to-Run is a streaming and virtualization Microsoft technology that install and update Microsoft products, including Office 365 and Office 2016. BigFix Patches for Windows helps users with the following features:

- Detect outdated Office 365 and Office 2016 products
- Configure the update source settings of Office 365 Click-to-Run updates to come from the web, a network share location, or from a client cache folder through the BigFix architecture
- Remove the update source settings for Office 365 Click-to-Run updates
- Maintain an updated network share
- Enable and disable automatic updates
- Check the Office 365 configuration of machines

Microsoft Click-to-Run technology

Click-to-Run is a streaming and virtualization Microsoft technology that installs Office products such as Office 365 and the single purchase version of Office 2016. Click-to-Run updates do not use MSI, MSP, and Windows Server Update Services (WSUS). Office products that use Click-to-Run can receive automatic updates from Microsoft through the web or download from an on-premises location. The Office Deployment tool is used to manage Click-to-Run installations.

The Office Deployment Tool supports the following operating systems:

Table 20. Operating systems that are supported by the Office Deployment Tool

Office products	Operating systems
Office 2013	<ul style="list-style-type: none"> • Windows 7 • Windows 8 • Windows Server 2008 R2 • Windows Server 2012
Office 2016	<ul style="list-style-type: none"> • Windows 10 • Windows 7 • Windows 8 • Windows 8.1

Table 20. Operating systems that are supported by the Office Deployment Tool (continued)

Office products	Operating systems
	<ul style="list-style-type: none"> • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2

For more information about Click-to-Run, see <https://docs.microsoft.com/en-us/office/troubleshoot/office-suite-issues/office-click-to-run-installation>.

For more information about Office Deployment Tool, see the following links:

- Office 2013 Deployment Tool: <https://www.microsoft.com/en-sg/download/details.aspx?id=36778>
- Office 2016 Deployment Tool : <https://www.microsoft.com/en-us/download/details.aspx?id=49117>

Supported applications

BigFix Patches for Windows supports applications and, if applicable, subscription plans for the following Microsoft products that use Click-to-Run.

- Office 365 – Office 2013 PC applications
- Office 365 – Office 2016 PC applications
- Office 2016 (single purchase version)

For more detailed information about the supported application, see [Supported operating systems, products, and updates \(on page 7\)](#).

Supported product IDs for Office 365

For Current, Monthly Enterprise, Semi-Annual, and Semi-Annual Preview Channels, BigFix offers support for the following product IDs in Office 365 which are O365ProPlusRetail, O365BusinessRetail, ProPlus2019Retail, and ProPlus2021Retail.

Additionally, for perpetual channel, BigFix extends support to ProPlus2019Volume and ProPlus2021Volume

The following product IDs for office 365 are supported by BigFix:

- O365ProPlusRetail
- O365BusinessRetail
- ProPlus2019Retail
- ProPlus2021Retail
- ProPlus2019Volume
- ProPlus2021Volume

Understanding how BigFix works with Click-to-Run

Understanding the integration of BigFix with Click-to-Run involves grasping how BigFix interacts and coordinates with the deployment and management processes of Click-to-Run software installations.

BigFix Patches for Windows uses Fixlets and analyses to do the following set up and maintenance tasks for Office products that use Click-to-Run.

Set up

- Configure the update source settings
- Set up the network share folder
- Configure the Update Path

Maintain

- Detect outdated versions
- Enable automatic updates
- Disable automatic updates
- Remove the Update Path
- Delete network share
- Trigger updates
- Check the Office 365 configuration of machines

BigFix users can use the task "Configure the Update Source of Office 365 - Office 2016" to choose the update source of Office Click-to-Run product updates.

- Through the web [from the Microsoft Content Delivery Network (CDN)]
- From an on-premises location. This method requires setting up a network share location from which updates can be downloaded. Throughout this document, 'network share' or 'network share location' refers to this method.
- Through the use of the BigFix architecture, wherein the entire binary is downloaded to the client cache folder.



Note: Microsoft CDN is the default update source.

Updating from the web

According to Microsoft, Click-to-Run versions of Office products are up to date from the start and automatically updated.

Users who choose to update from the web can use BigFix content to disable the automatic updates from Microsoft. Users can then use a Fixlet to trigger the updates to load and install from the Microsoft CDN.

Updating from a network share location

You can choose for your Office products that use Click-to-Run to receive updates through a network share location, instead of the Microsoft CDN.

Setup up the network share location

You must set up a network share location that will receive the updates. BigFix provides content to set up network share but it is not a requirement. You can choose to use your own network share location.

Configure the client

Once you have set up the network share, you need to configure the update path so it will point to the network share location. BigFix Patch uses an analysis to identify the update path and the data location.

Trigger the client update

You might want to disable the automatic updates from Office so that you have more control of when to update and which version you want to upgrade to.

When the automatic updates are disabled, you can apply the BigFix content to maintain and trigger the updates. An example of this BigFix content is Fixlet 365007: Office 365 Version 15.0.4805.1003 Available - Office 2013. Instead of directly downloading from the Microsoft CDN, the updates are downloaded from the pre-configured network share location.

Maintain network share

As Microsoft releases updates, BigFix provides content so that the network share always has the latest versions. For example, Fixlet 365021: Office 365 Version 15.0.4805.1003 Available for Network Share for Office 365 - Office 2013.

The network share location uses the following ports for TCP and UDP connections.

- TCP: 139, 445
- UDP: 137, 138

For more information about network share and the ports used, see <https://technet.microsoft.com/en-us/library/cc731402.aspx>.

Updating from a client cache folder through the BigFix architecture

You can also choose for your Office products that use Click-to-Run to receive updates through the BigFix architecture, wherein the entire binary is downloaded to the client cache folder. BigFix handles the update download and the Office 365 Client installs the update from the local machine.

If you use this update source, you must consider the download and relay cache sizes.

- Server: 4GB or more
- Client: 4GB or more

Office 365 Channel Change through GPO/ODT

BigFix does not support channel changes, as they can lead to discrepancies between CDNBaseUrl and UpdateChannel (via GPO).

During the period until a Channel Change is successfully completed, there may be false positive evaluation results for Office 365 patching fixlets.

As a result, we do not recommend implementing Channel Change, and we do not provide support if Office 365 Fixlets are not applicable for machines on which Channel Change has been performed.

Setting up to download updates from a network share location

Configure systems to download updates from a network share location.

If you prefer, you can set Office clients to download updates from a network share instead of downloading directly from the Microsoft CDN. To do this, you must assign a network share location and configure the update path. Ensure that the updates have been downloaded to the network share.

Setting up the network share

Network share involves in creating a shared folder on a server and configuring permissions to allow access to authorized users or devices within the network.

Use the Fixlet for the corresponding Office version to set up your network share location.

1. From the Patch Management domain, go to the **Patches for Windows (English) site > Fixlets and Tasks**.
2. Select the Fixlet for the Office version whose network share you prefer to set up. For example, Fixlet 361015: Setup Network Share for Office 365 – Office 2013.
3. Click **Take Action**.
4. From the Action Parameter window, enter the the language of the applications in your deployment. To refer to the list of available language IDs, click the link in the Actions panel. Use a semi-colon to separate the language IDs. For example, 'en-us;zh-cn'.
5. Select the devices and click **OK**. After the action completes, configure the network share folder privileges to grant Office machines access to the update files. The network share folder will be created at the root of the system drive.

You have set up a network share location.

Configuring the Update Path

Setting up the Update Path involves specifying the network location where the system will retrieve updates.

Use a task to configure the update path of Office 365 and Office 2016 applications in selected computers. The endpoints will download updates from this location instead of Microsoft CDN.

1. From the Patch Management domain, go to the Patches for Windows (English) site > Fixlets and Tasks. Select the Configure the Update Path Fixlet for the Office version that you wish to set up. For example, Fixlet 365009: Configure the Update Path of Office 365 - Office 2013.
2. Click **Take Action**.
3. From the Action Parameter window, enter the update URL. For example, `\\NetworkShare\Office2013`. The link can be obtained from the analysis Network Share Information for <Office version>. The analysis returns the result on the network share after it is set up successfully. Click **Ok**.
4. Select the devices and click **OK**.

Maintaining updates

Maintaining updates involves overseeing the process of consistently applying patches, fixes, and upgrades to ensure systems remain up-to-date and secure.

When updates become available from Microsoft, BigFix Patches for Windows releases Fixlets accordingly. BigFix provides content that triggers the update that is required for both Microsoft CDN and network share.

For example:

- For the network update: Fixlet ID 365021: Office 365 Version 15.0.4797.1003 Available for Network Share for Office 365 – Office 2013
- For triggering the client update: Fixlet ID 365007: Office 365 Version 15.0.4805.1003 Available - Office 2013

You can also use Fixlets to remove the update path settings, delete the network share, or disable automatic updates.

Enabling automatic updates

Activating automatic updates entails configuring systems to automatically download and install updates without manual intervention, ensuring continuous maintenance, and security enhancement.

Use the applicable Fixlet to enable automatic updates through the Click-to-Run installation.



Note: The enable and disable automatic update Fixlets are not required to trigger the the update Fixlets such as Fixlet 365007: Office 365 Version 15.0.4805.1003 Available - Office 2013.

1. From the Patch Management domain, go to **Patches for Windows (English) site > Fixlets and Tasks**. Select the applicable Enable Automatic Updates Fixlet. For example, Fixlet ID 365003: Enable Office 365 Automatic Update - Office 2013.
2. Click **Take Action** and click **OK**.
3. Select the applicable device and click **OK**.

Disabling automatic updates

Disabling automatic updates involves turning off the setting that allows systems to automatically download and install updates, thereby requiring manual intervention for updates to be applied.

Use the applicable Fixlet to stop automatic update through the Click-to-Run installation. To provide better control of the updates, you can disable the automatic update and use BigFix content to trigger the updates instead.

1. From the Patch Management domain, go to **Patches for Windows (English) site > Fixlets and Tasks**. Select the applicable Disable Automatic Updates Fixlet. For example, Fixlet ID 365001: Disable Office 365 Automatic Update - Office 2013.
2. Click **Take Action** and click **OK**.
3. Select the applicable device and click **OK**.

Removing the Update Path

Removing the Update Path involves deleting or deactivating the network location previously designated for retrieving updates, effectively discontinuing the use of that specific location for updates.

You can use a task to remove the update path and revert to downloading updates from the Microsoft CDN.

1. From the Patch Management domain, go to **Patches for Windows (English) site > Fixlets and Tasks**. Select the applicable Remove Update Path Fixlet. For example, Fixlet ID 365013: Remove the Update Path of Office 365 - Office 2013.
2. Click **Take Action** and click **OK**.
3. Select the applicable device and click **OK**.

You removed the update path and the updates will revert to downloading from the Microsoft CDN.

Deleting a network share

Deleting a network share involves removing the shared folder or directory from the network, effectively revoking access to its contents for other users or devices.

Deploy the applicable Fixlet task to delete the network share settings.

1. From the Patch Management domain, go to **Patches for Windows (English) site > Fixlets and Tasks**. Select the applicable Delete Network Share Fixlet. For example, Fixlet ID 365017: Delete Network Share for Office 365 - Office 2013.
2. Click **Take Action** and click **OK**.
3. Select the applicable device and click **OK**.

You have removed the network share settings.

Disabling the automatic upgrade of Office 365 – Office 2013 to Office 365 – Office 2016

This involves in configuring settings to prevent the automatic installation of the newer version, thereby maintaining the current version of Office 365 - Office 2013 without upgrading to Office 365 - Office 2016.

Automatic upgrades are set to ON by default. BigFix provides content for users who prefer to disable the automatic upgrade. This would benefit users who might want to delay upgrades, such as users who have Office 2013 applications.

Office 2016 cannot exist on the same computer that have Office 2013 applications. Users who try to install Office 2016 on computers that have Office 2013 applications will receive an error message stating that the Office 2013 will have to be removed. Users have until before February 2017 to defer the upgrade.

For more information, see the following articles:

- <https://support.office.com/en-us/article/Error-Stop-you-should-wait-to-install-Office-2016-We-ll-have-to-remove-the-following-if-you-continue-a225347f-e102-4ea6-9796-5d1ac5220c3b?ui=en-US&rs=en-US&ad=US>
- https://technet.microsoft.com/en-sg/library/7198c31f-2d68-44b4-bc63-e3630cf0c936#BKMK_Key

To disable the upgrade from Office 2013 to Office 2016, use the Fixlet called Disable Office 365 Automatic Upgrade of Office 2013 to Office 2016 applications - Office 2013.

1. From the Patch Management domain, go to **Patches for Windows (English) site > Fixlets and Tasks**. Select the Disable Office 365 Automatic Upgrade of Office 2013 to Office 2016 applications - Office 2013 Fixlet.
2. Click **Take Action** and click **OK**.
3. Select the applicable device and click **OK**.

Enabling the automatic upgrade of Office 365 – Office 2013 to Office 365 – Office 2016

This involves in configuring settings to allow the automatic installation of the newer version, facilitating the transition from Office 365 - Office 2013 to Office 365 - Office 2016 without manual intervention.

To revert to the default automatic upgrade of Office versions in your deployment from Office 2013 to Office 2016, use the Fixlet called Enable Office 365 Automatic Upgrade of Office 2013 to Office 2016 applications - Office 2013.

1. From the Patch Management domain, go to **Patches for Windows (English) site > Fixlets and Tasks**. Select the Enable Office 365 Automatic Upgrade of Office 2013 to Office 2016 applications - Office 2013 Fixlet.
2. Click **Take Action** and click **OK**.
3. Select the applicable device and click **OK**.

Enabling Office 365 previous version Fixlets

This topic describes users how to enable the Office 365 previous version Fixlets.

Microsoft releases multiple versions of updates for the few supported channels of Office 365.

Previously BigFix supported only the latest version of the updates. Starting from December 14, 2021, BigFix Patch provides support for the previous versions of Office 365, but the endpoints require an additional preparation before deploying Fixlets. To enable the previous version of Fixlets, set the client configuration parameter **_BESClient_Office365_EnablePreviousVersion** to **1**. For Client configuration settings details, see [BigFix Configuration Settings](#).

Removing the update source setting

This involves in removing or resetting the designated location from which updates are retrieved.

To remove the Update Source setting, deploy the **Remove Office 365 Click-to-Run Update Source Setting** task.

Checking the Office 365 configuration

This involves in reviewing and examining the settings and parameters within the Office 365 environment to ensure that they are properly configured and aligned with the desired setup and requirements.

To get an overview of the Office 365 configurations of your test machines, you can check the **Results** tab of **Analysis: Application Information for Office 365 - Office 2016**.

Chapter 5. Navigating Windows Application Update Patches in the BigFix console

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

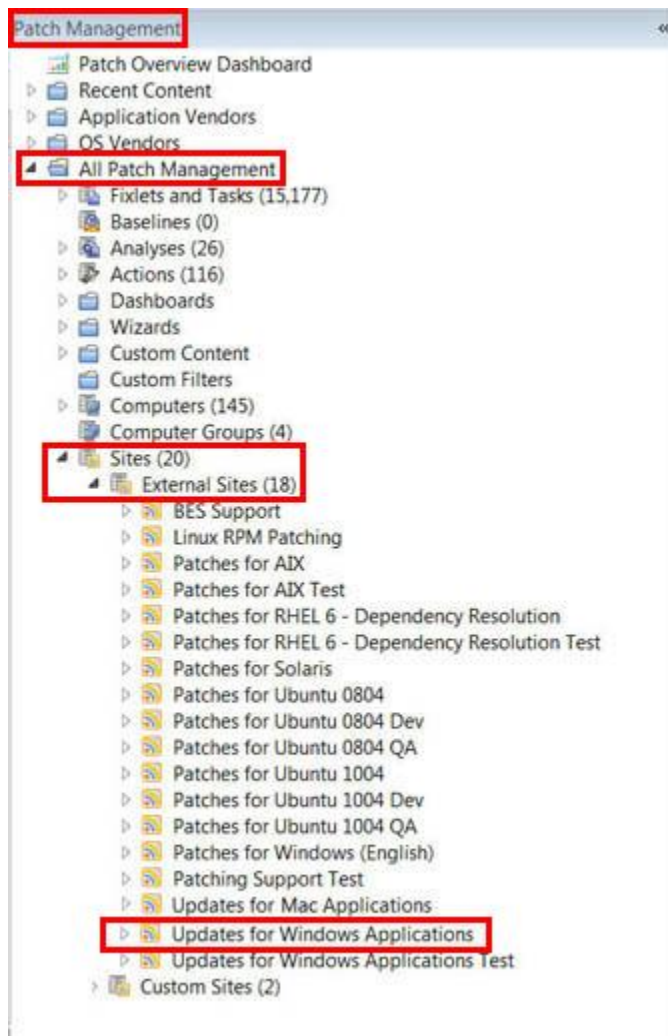
You can deploy the Windows Updates Fixlets from the BigFix console.

From the *Patch Management* domain, in the navigation tree, click **All Patch Management > Sites > External Sites > Updates for Windows Applications**.

Select from among the following options:

- Fixlets and Tasks
- Baselines
- Analyses
- Computer Groups
- Actions
- Subscribed Computers

Figure 2. Updates for Windows Applications site - Navigation tree view



The list panel on the right updates to show what you selected. Double-click the Fixlet that you want to deploy. The Fixlet opens in the work area.

Click the tabs at the top of the window to review details of the selected Fixlet.

Select the link in the Actions box to start deployment.

Click **OK**. The action propagates across your network, installing the designated patch on the computers that you specified and to the schedule that you selected. You can monitor and graph the results of this action to see exactly which computers are remediated to ensure compliance. For more information about navigating the Endpoint Console and deploying patches, see the *Console Operator's Guide* in the [HCL Knowledge Base](#).

Fixlet Maker dashboard overview

The Fixlet Maker dashboard provides an interface where you can create application update Fixlets by using templates.

The dashboard currently supports templates for the following applications:

- Google Chrome (Enterprise Edition)
- Mozilla Firefox
- RealPlayer
- WinZip
- Winamp

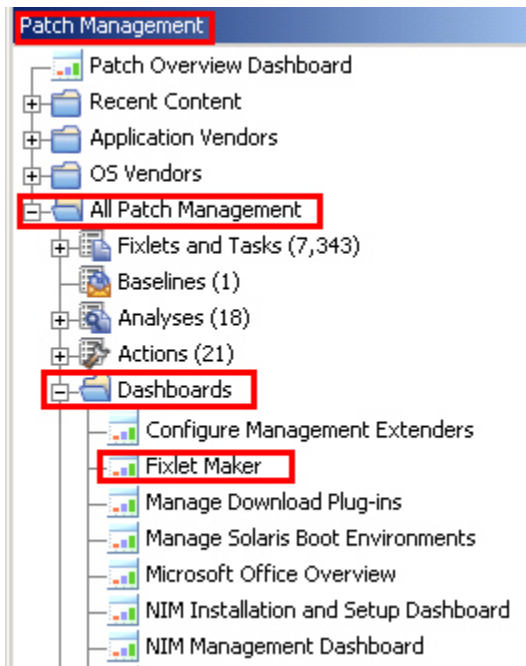
Audit Fixlets for these applications are available to inform you when a new version of the application becomes available.



Note: You can create your own template to generate Fixlets in the Fixlet Maker dashboard. For more information, see the [BigFix wiki](#) and search for "Creating a Fixlet template".

You can access the Fixlet Maker dashboard from the Patch Management domain. Click **All Patch Management > Dashboards > Fixlet Maker**.

Figure 3. Fixlet Maker dashboard from the navigation tree



The dashboard displays all the previously created Fixlets for each template.

Figure 4. Fixlet Maker dashboard

The screenshot shows the Fixlet Maker dashboard. At the top, it says "Fixlet Maker" and "Last Refresh Time: Fri, 12 Jul 2013 21:31:26 +0800". Below this, a text block states: "The Fixlet Maker wizard provides an interface where you can create application update Fixlets with the use of templates. To create a Fixlet, select a template from the table and click Create Fixlet."

The dashboard is divided into two main sections:

Fixlet Templates

At the top of this section is a "+ Create Fixlet" button and a search box. Below is a table with the following data:

Application	Vendor	Operating System	Additional Details
WinZip	WinZip	Windows	Only supports the Winzip ".msi" installer.
Chrome (Enterprise Edition)	Google	Windows	Only supports the Chrome Enterprise Edition ".msi" stand-alone installer.
RealPlayer	Real Networks	Windows	Only supports the RealPlayer ".exe" installer. The generated action upgrades RealPlayer without setting the configuration options.
Winamp	Nullsoft	Windows	Only supports the Winamp ".exe" installer. You might need extra relevance to check the language version of the installed Winamp on the client.
Firefox	Mozilla	Windows	Only supports the Firefox ".exe" installer.

Fixlets

At the top of this section is a "Delete (0)" button and a search box. Below is a table with the following data:

<input type="checkbox"/>	Fixlet Title	Site Name	Source Release Date
<input type="checkbox"/>	RealPlayer 3 Available	ActionSite	Mon, 10 Jun 2013
<input type="checkbox"/>	RealPlayer 1.8 Available	ActionSite	Mon, 14 Jan 2013
<input type="checkbox"/>	RealPlayer 2 Available	ActionSite	Tue, 05 Feb 2013
<input type="checkbox"/>	RealPlayer 2.2 Available	ActionSite	Thu, 28 Feb 2013

Creating custom Fixlets from templates

You can use the Fixlet Maker dashboard to create your own Fixlets for Windows applications that are not supported by the Patching Support site.

You can either create a dedicated custom site or use the Master Action site to store and manage the created Fixlets.

Use the templates from the Fixlet Maker dashboard to create Fixlets for the following applications:

- Google Chrome (Enterprise Edition)
- Mozilla Firefox
- RealPlayer
- WinZip
- Winamp

1. Click **Patch Management > All Patch Management > Dashboards > Fixlet Maker**.
2. Select a template from the list of available templates.
3. Click **Create Fixlet**.
4. Specify the installation file of the application.



Note: The installation files must be downloaded from official vendor sites.

For this release, you can either select the installation file from your local drive or download the file from the internet. An example of the URL download link is `http://download.nullsoft.com/winamp/client/winamp563_lite_en-us.exe`.

The installation file is uploaded in the `BESRootServerDir/Uploads` directory of the BigFix server. For example:

On a 32-bit operating system

```
C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\Uploads
```

On a 64-bit operating system

```
C:\Program Files (x86)\BigFix Enterprise\BES Server\wwwrootbes\Uploads
```

5. Enter the software version. Ensure that you specify the software version of the installation file.
6. Enter the source release date of the updates.
7. **Optional:** Enter the Common Vulnerabilities and Exposures (CVE) ID number.
For example, cve-1234567.
8. **Optional:** Enter the Source ID. This ID is associated with the source of the update.
For example, Microsoft uses MS11-02 and Adobe uses APSB-12.
9. **Optional:** Enter the severity of the Fixlet.
For example, Low, Moderate, Important, and Critical.
10. **Optional:** Select the operating system architecture that you want the updates to be relevant for. You can select either 32-bit or 64-bit.
11. Click **Create Fixlet**. A creation dialog opens with blank fields that you can complete.
12. Enter a user-readable title as the name of the Fixlet.
13. Select the site and domain to host it from.
14. From the **Description** tab, create a description for the Fixlet that you want to deploy.



Note: The **Actions**, **Relevance**, and **Properties** tabs are automatically populated with the information that you entered in the Fixlet template.

15. Click **OK**. The created Fixlet displays in the second table of the dashboard.

Chapter 6. Using the custom repository setting feature

Utilizing the custom repository setting feature involves configuring a specific repository or source from which software or updates can be retrieved, allowing for greater flexibility and control over the update process.

Use the custom repository setting feature to create, update, or delete custom repository settings.



Note: The Custom repository setting feature is applicable only when the public download link is not available for the Fixlets.

- The Windows 10 Feature Upgrade fixlets (Fixlet ID - 1110004 for example) in the Patches for Windows site.
- The Java fixlets in the Updates for Windows Application site.

The custom repository setting feature provides an alternative to manual caching. Installers that are cached in the HCL BigFix server expire and are removed automatically. Use the feature to avoid downloading and manually caching the installers again when deploying Fixlets in the future. Instead, you can set installers to be cached to custom repositories. Another advantage to the feature is that it eliminates the need to rename files to sha1, which must be done in manual caching.

The feature uses the Custom Repository Setting (Windows) analysis to display the custom repositories that are used in your deployment. The following tasks are used to create, update, and delete the repository setting:

- Create or Update Custom Repository Setting (Windows)
- Delete Custom Repository Setting (Windows)



Note: It is not mandatory to enable the Custom Repository Setting (Windows) analysis to create or delete the custom repository setting.

Requirements

To use the custom repository setting feature, ensure that you meet the following requirements.

- Use BigFix version 9.0 and later.
- Subscribe to the Patching Support site.
- Enable the following tasks:
 - Create or Update Custom Repository Setting (Windows)
 - Delete Custom Repository Setting (Windows)
- Add the custom repository directory to the whitelist on the BigFix server. The whitelist is located at `<BES Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt`. When the directory of the custom repository is not set in the whitelist, a download error indicates that the requested URL does not pass the deployment of the download whitelist.

You can host the Windows Custom Repository, which is a web server, on the BES Server or another server. To reduce limitations on server performance and disk size, it is highly suggested that users use a separate server.

Creating a custom repository setting

This topic describes how to create a custom repository setting.



Note: The Custom repository setting feature is applicable only when the public download link is not available for the Fixlets.

- The Windows 10 Feature Upgrade fixlets (Fixlet ID - 1110004 for example) in the Patches for Windows site.
- The Java fixlets in the Updates for Windows Application site.

Ensure that the custom repository directory is added to the whitelist on the HCL Manager Server, which is located at `<BES Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt`. When the directory of the custom repository is not set in the whitelist, a download error indicates that the requested URL does not pass the deployment of the download whitelist.

1. From the console, go to **Sites > External Sites > Patching Support > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** panel, select the **Set or Update Custom Repository (Windows)** task.
3. Click **Take Action**.
4. In the **Action Parameter** window, enter the custom repository directory. For example, `http://10.1.11.11/software`. Click **Ok**.
5. The **Take Action** window opens. Select the target computer and click **Ok**.

You can check if the setting was applied to the custom repository.

Go to the registry key `_BESClient_AllowCustomRepoDownloads`, which you can find at the following locations, depending on the operating system version that you are using.

- For x64: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432\BigFix\EnterpriseClient\Settings\Client_BESClient_AllowCustomRepoDownloads`
- For x86: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\EnterpriseClient\Settings\Client_BESClient_AllowCustomRepoDownloads`

The value must contain the custom repository directory.

Delete a custom repository setting

This entails deleting or removing the configured repository from which software or updates were being retrieved, thereby discontinuing its use for future updates or installations.

1. From the console, go to **Sites > External Sites > Patching Support > Fixlets and Tasks**.
2. From the **Fixlets and Tasks** panel, select the **Delete Custom Repository (Windows)** task.
3. Click **Take Action**. The **Take Action** window opens.
4. Select the target computer and click **Ok**.

Check the registry key `_BESClient_AllowCustomRepoDownloads` to confirm that the setting is deleted.

You can find the `_BESClient_AllowCustomRepoDownloads` registry at the following locations.

- For x64: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432\BigFix\EnterpriseClient\Settings\Client_BESClient_AllowCustomRepoDownloads`
- For x86: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\EnterpriseClient\Settings\Client_BESClient_AllowCustomRepoDownloads`

The setting is deleted if the Value key is removed.

Appendix A. Support

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

- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Playlist on YouTube](#)
- [BigFix Tech Advisors channel on YouTube](#)
- [BigFix Forum](#)

Appendix B. Frequently asked questions

Learn the answers to frequently asked questions.

The Manage Download Plug-ins dashboard is not reflecting any data. What do I do?

Here are some steps you can do to troubleshoot the issue:

- Gather the latest **Patching Support** site.
- Activate the **Download Plug-in Versions** analysis, available from the **Patching Support** site.
- Clear the BigFix console cache.

Where are my dashboards located in the BigFix Console?

The updated BigFix 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 [HCL 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 HCL 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.



Note: 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 BigFix 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?

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

How do I deal with missing patches?

BigFix 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 BigFix. You can also contact HCL 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. BigFix supports critical updates and service packs. For more information about the types of updates that are supported by BigFix, see the wiki article on [Supported OS](#).

What types of patches are supported by BigFix?

BigFix 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 BigFix, 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 BigFix?

Hotfixes are not supported. Customers are advised to contact [HCL Software Support](#) for critical hot fix requests. The BigFix Patch team will thoroughly assess each request and provide content on a case by case basis.

What is an audit Fixlet?

An BigFix 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.

Does Patch Management for Windows support cross-language installation?

Cross-language patch application is currently not supported. For example, a user cannot deploy a Fixlet from the Patches for Windows (English) site to an operating system in a different language. Users can either change the setup or, alternatively, work around the issue by making a custom copy of the Fixlet and removing the relevance checking for OS language. Users are strongly encouraged to perform tests before applying the workaround.

The Custom Repository Setting feature requires adding the custom repository directory in a whitelist. What happens if this is not done?

When the custom repository directory is not added to the whitelist, a download error indicates that the requested URL does not pass the deployment of the download whitelist. The whitelist text is located at `<BES Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt`.

The modification time got changed in the Fixlet. Why can't I see any difference?

There are a number of reasons why the modification time in a Fixlet might change, such as content modifications, localization changes, and MIME field updates. Localization changes and MIME field updates are usually not visible to users. No action needs to be taken and no patches need to be re-deployed because of these changes.

Why is the Source Release Date after the First Release Date in BigFix?

When a source vendor updates their software, the source release date may be after the first release date. For example, virus update Fixlets may show daily changes to their source release date but show an older BigFix first release date.

How can I make better use of the MIME for product name and component?

See the 'Filtering by product family and added Fixlet MIME fields' wiki here: <https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/Filtering%20by%20product%20family%20and%20added%20Fixlet%20MIME%20fields>.

What is the correlation between the Microsoft and BigFix categories?

The article 'Difference in category terms used by Microsoft and BigFix' provides the category terms that Microsoft and BigFix use. <https://bigfix-wiki.hcltechsw.com/wikis/home?lang=en-us#!/wiki/BigFix%20Wiki/page/Difference%20in%20category%20terms%20used%20by%20Microsoft%20and%20BigFix>.

Where does BigFix base the value of the Source Severity field?

Source Severity is a field that is shared by all Fixlets. BigFix bases the source severity on the Windows and non-Windows vendors. For Microsoft security content, Patch Management for Windows follows the severity rating system of the Microsoft Security Response Center (MSRC).

What is the 'MIME_no-relevance-health-check' Fixlet field used for?

This MIME field is used to skip the Action Size check for content that contains lengthy relevance. This Fixlet field is for internal use only.

Can BigFix break down large cumulative updates?

BigFix cannot break down large cumulative updates by taking note of the difference. By design, Microsoft should already be covering that function. According to Microsoft: "Only the files that are different are copied down to a Download folder on the local computer, and they're downloaded in a compressed form. This helps reduce the size of the download.."

For more information, see <https://technet.microsoft.com/en-us/library/dn761709.aspx>.

Which ports does the network share location use when updating Microsoft Click-to-Run products?

The Network Share location uses the following ports for TCP and UDP connections:

- TCP: 139, 445
- UDP: 137, 138

For more information, see <https://technet.microsoft.com/en-us/library/cc731402.aspx>.

What cache and server sizes should I consider when my update source is the client's cache folder?

The direct download method pushes the entire binary through the BigFix architecture. You must consider the download and relay cache sizes.

- Server: 4GB or more
- Client: 4GB or more

I'm having trouble uninstalling Java Runtime Environment Fixlets from my deployment. What could be the cause of this issue?

The uninstall issue might be a result of having 32-bit and 64-bit JRE versions on the same machine. BigFix does not support multiple JRE versions in the same machine.

For example, if you have JRE 8u91 32bit, JRE 8u91 64bit, and JRE 8u121 32bit, the uninstall Fixlet would not be able to uninstall 8u91 32bit, because there is a mix of 32-bit and 64-bit JRE versions.

You can refer to <https://bigfix.me/uninstall> for sample Fixlets to uninstall Java. Bigfix.me is a community website that has user-generated content.

Notices

This information was developed for products and services offered in the US.

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

HCL 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:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. 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 jurisdictions 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. HCL 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-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide 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:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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 HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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

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

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 actual people or business enterprises 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 HCL, 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. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

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.

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

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

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

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.