IBM Endpoint Manager
Version 9.0

Getting Started

IBM Endpoint Manager
Version 9.0

Getting Started

Note
Before using this information and the product it supports, read the information in "Notices" on page 17.

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

Contents

Getting Started

IBM® Endpoint Manager is a suite of products that provides a fast and intuitive solution for compliance, endpoint, and security management and allows organizations to see and manage physical and virtual endpoints through a single infrastructure, a single console, and a single type of agent.

Specifically, IBM Endpoint Manager provides you with the following capabilities:

- Single intelligent agent for continuous endpoint self-assessment and policy enforcement.
- Real-time visibility and control from a single management console.
- Management of hundreds of thousands of endpoints regardless of location, connection type, or status.
- Targeting of specific actions to an exact type of endpoint configuration or user type.
- Management of complexity and cost reduction, increasing accuracy, and boosting productivity.
- Patch management, software distribution, and OS deployment.
- Support for heterogeneous platforms.
- Mobile device management.
- Automatic endpoint assessment and vulnerability remediation according to the National Institute of Standards and Technology (NIST) standards.
- Real-time protection from malware and other vulnerabilities.
- Server Automation.

Depending on your business and environment needs, you can choose to implement some or all of these capabilities by buying licenses for the specific products belonging to the suite.

Licensing is done through annual subscription, according to the number of endpoints that are managed and the products that are selected in the suite.

All products are compatible with one another, and they are accessible from anywhere in your network by using the IBM Endpoint Manager console.

Typically, an IBM Endpoint Manager installation consists of the following parts:

- "IBM Endpoint Manager platform"
- One or more "IBM Endpoint Manager applications" on page 3

For more details about the product, see:

- "A sample architecture" on page 5
- "Types of content" on page 6
- "How to identify on which targets to apply content" on page 8

IBM Endpoint Manager platform

All the IBM Endpoint Manager applications run on top of the IBM Endpoint Manager platform.

The IBM Endpoint Manager platform is a multi-layered technology platform that acts as the core part of the global IT infrastructure. The platform is a dynamic, content-driven messaging and management system that distributes the work of managing IT infrastructures out to the managed devices themselves, the agents.

The platform can manage up to 250,000 physical and virtual computers, over private or public networks, including servers desktops, roaming laptops, mobile phones, Point-Of-Sale devices, Automated Teller Machines, and self-service kiosks.

The platform supports Microsoft Windows, UNIX, Linux and Mac OS.

If you buy a license for the IBM Endpoint Manager for Mobile Devices Management product the platform coverage is extended also to Microsoft Windows Mobile, Apple iOS, Google Android, and Blackberry OS systems.

In terms of features and benefits, IBM Endpoint Manager platform delivers:

A single intelligent agent
It operates with less than 10 megabytes of RAM and it must be installed on every computer that must be managed. It continuously assesses the state of the endpoint against the stated policy, whether connected to the network or not. As soon as the agent notices that the target out of compliance with a policy or checklist, it informs the server, runs the configured remediation task, and immediately notifies the server of the task status and result. In most cases, the agent operates silently, without any direct intervention from the user. However, if you want to solicit a user response, the program also allows you to provide screen prompts. A computer with the IBM Endpoint Manager agent installed is also referred to as a *client*.

A single console
Whatever specific solution you use, whether it is endpoint protection, systems lifecycle management or security configuration and vulnerability management, it is managed from a single console. If you are an operator with the required privileges, from the console you can quickly and easily distribute a fix to only those computers that need it, with no impact on the rest of the network.

A single server
It coordinates the flow of information to and from individual clients and stores the results in the database. It manages policy-based content and allows the operator to maintain real-time visibility and control over all devices in the environment. The content is delivered in messages that are called *Fixlet* and it is updated continuously using the Content Delivery cloud-based service. Because most of the analysis, processing, and enforcement work is done by the agent rather than the server, one server can support up to 250.000 endpoints. High availability is enabled by employing multiple servers.

Optionally one or more relays
They help manage distributed devices and policy content. A relay is a client, that is enhanced with a relay service. It performs all client actions to protect the host computer, and in addition, delivers content and software downloads to child clients and relays. Instead of requiring every networked computer to directly access the server, relays can be used to offload much of the burden. Hundreds of clients can point to a relay for downloads, which in turn makes only a single request to the server. Relays

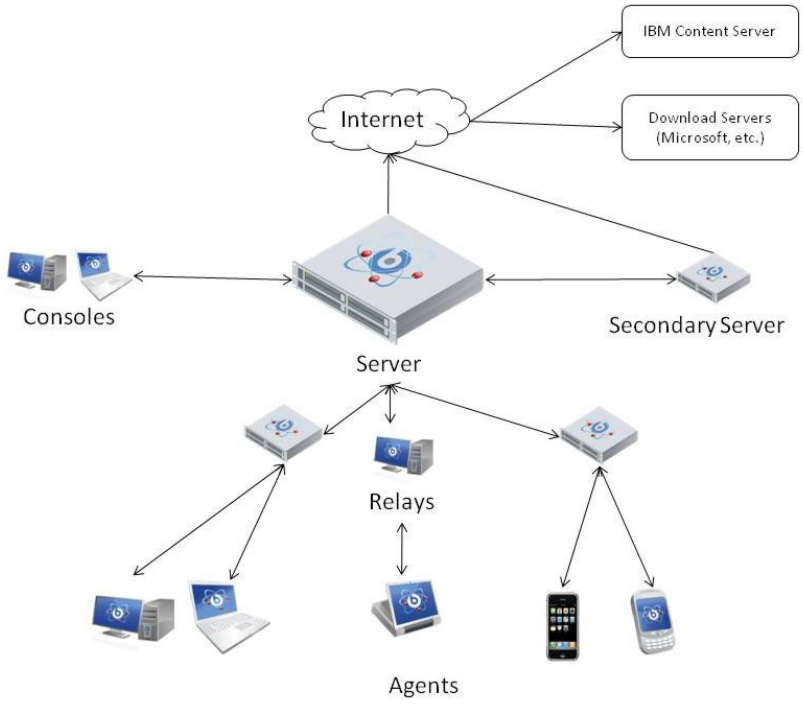
can connect to other relays as well, further increasing efficiency. Promoting an agent to a relay takes minutes and does not require dedicated hardware or network configuration changes.

Optionally a secondary server
A Distributed Server Architecture (DSA) server, which replicates the server information for disaster recovery. If a IBM Endpoint Manager server fails, other IBM Endpoint Manager servers automatically take over as fully functional IBM Endpoint Manager servers.

Web Reports
Using the Web Reports program you can:

- Produce charts and graphs of your data, providing you with hardcopy.
- Help you to maintain an audit trail of all the Fixlet activity in your network.
- Export data for further manipulation in a spreadsheet or database.
- Aggregate information from extra IBM Endpoint Manager servers that are installed at your organization.

The interface runs in a web browser and provides a set of users with visibility into the state of the computers, but no rights to alter those computers.



IBM Endpoint Manager applications

IBM Endpoint Manager includes the following application products:

IBM Endpoint Manager for Lifecycle Management
Use this product to provide administrators with an agent-based tool that delivers accurate visibility into the state of endpoints and automatically

remediates issues. The Remote Control capability allows you the remote takeover and monitor of workstations and servers in your deployment.

IBM Endpoint Manager for Patch Management
Use this product to provide an automated, simplified patching process to all distributed endpoints. It manages both operating system and software application patches.

IBM Endpoint Manager for Power Management
Use this product to manage and monitor the power usage settings on the computers in your network. It manages and applies the company conservation policies that you set with the use of dashboards, wizards, and web reports.

IBM Endpoint Manager for Security and Compliance
Use this product to protect endpoints, to automate remediation, and to assure regulators that you are meeting security compliance standards.

IBM Endpoint Manager for Core Protection
Use this product to have real-time antimalware function against viruses, Trojan horses, worms, spyware, rootkits, web threats, and their new variants. It uses protection methods such as file and web reputation, personal firewall, and behavior monitoring for:

- Network connected endpoints.
- Roaming, Internet-connected endpoints.
- Virtual endpoints.

IBM Endpoint Manager for Software Use Analysis
Use this product to scan monitored computers to:

- Identify what software is installed
- Match the signatures that are discovered by the scan against the software catalog
- Create reports
- Compare the results with the information about costs and entitlement that is provided in the contracts.

IBM Endpoint Manager for Mobile Devices
Use this product to manage security controls, software and hardware inventory, and application management over corporate and employee-owned smartphones and media tablets that access enterprise resources.

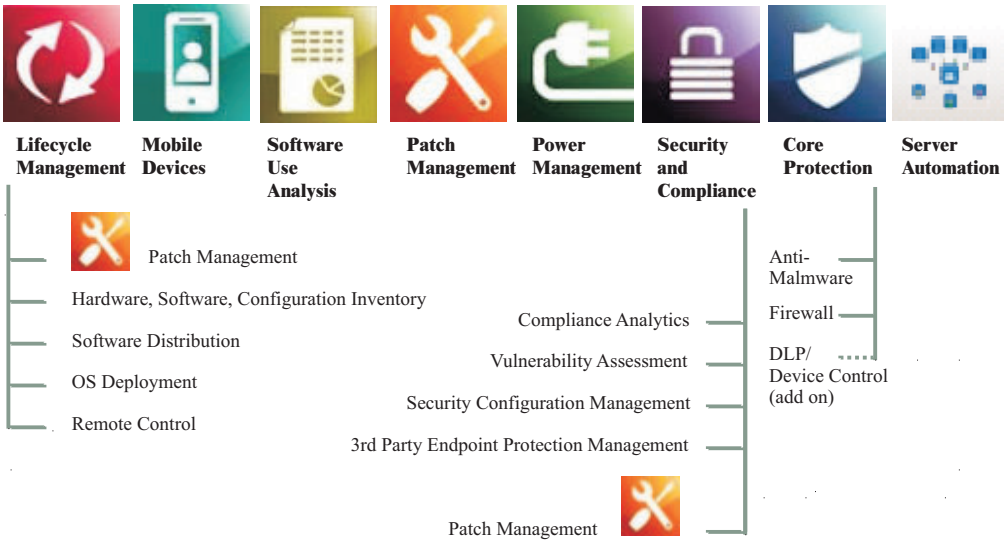
IBM Endpoint Manager for Server Automation
Use this product if you need powerful automation. You can use it to sequence automation actions in steps across multiple endpoints.

You can decide to add products that belong to the suite later by buying extra licenses; they will automatically be available for use on the IBM Endpoint Manager Console. You do not have to install any additional software or buy new hardware when you add products that belong to the suite. Only Asset Discovery and Software Use Analysis require the installation of new components, but the installation is done through IBM Endpoint Manager itself.

Note: Asset Discovery is an IBM Endpoint Manager platform component that allows you to identify unmanaged assets in your network.

Many customers start with one product, such as Patch Management, then they expand the scope of their deployments, buying new licenses, as they come to appreciate the full capabilities of the product suite.

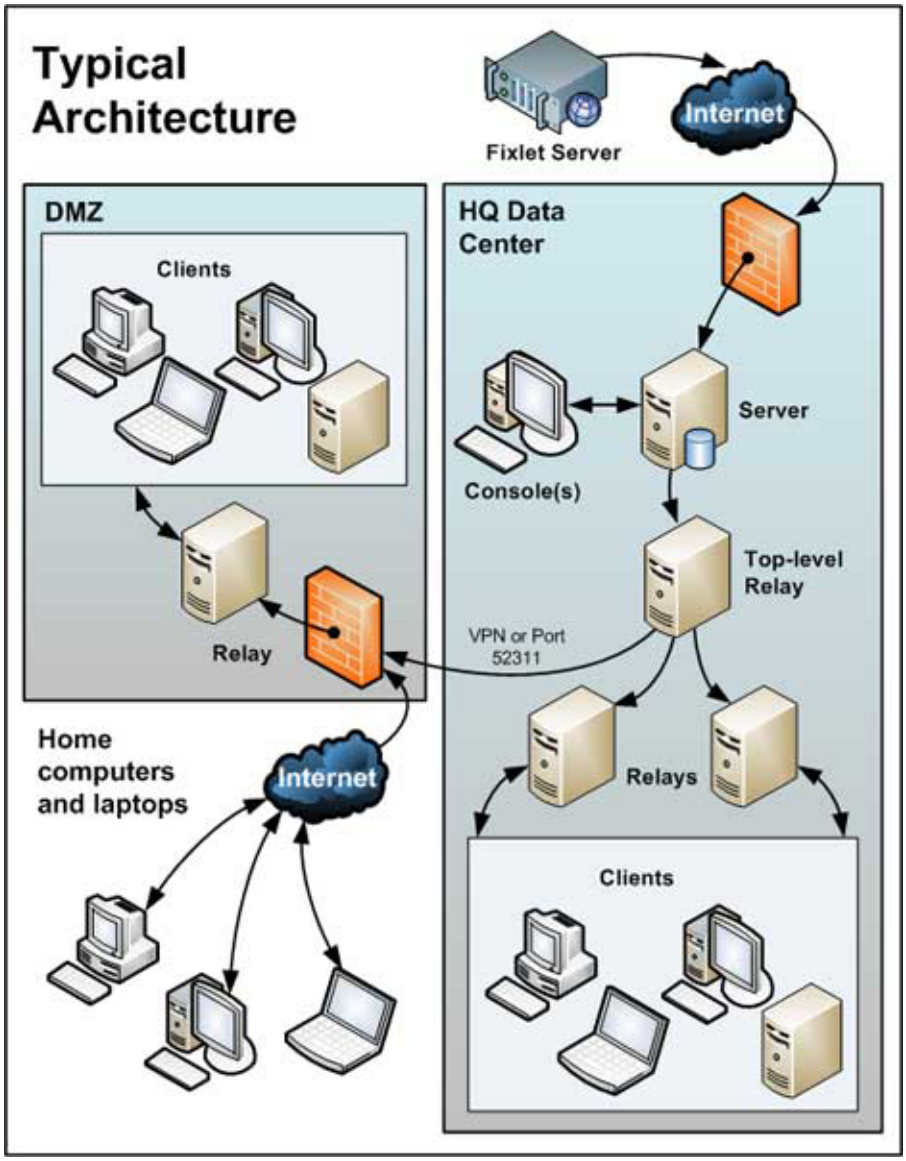
Consider that some capabilities are common to more than one product in the IBM Endpoint Manager product suite. For example, as you can see in the picture, the capability to apply OS and software application patches is available in the Patch Management product, as well as in the Security and Compliance, and Lifecycle Management products. You can buy any of these licenses to manage patches.



All these products take advantage of the continuous evaluation on the agent and of the gathering process to acquire data from repositories and send to the targets.

A sample architecture

A typical installation has at least one IBM Endpoint Manager server that gathers Fixlets from the internet. These messages can be viewed by the console operator and distributed to the relays, which forward the data on to the clients. Each client inspects its local computer and reports any relevant Fixlets back to the relays, which compress the data and pass it back up to the servers.



The console oversees this activity. It connects to the server and periodically updates its views to reflect changes or new information about your network. When vulnerabilities are discovered, the console operator can target patches or other fixes to the appropriate computers. The progress of the fixes can be followed in near real time as they spread to all the relevant computers and, one by one, eliminate bugs and vulnerabilities.

IBM Endpoint Manager is flexible enough to connect to a distant office over a VPN and even allows home-based workers or on-the-road sales staff to connect over the internet to a firewall-protected relay in a DMZ. This simple hierarchy can be extended and deepened to accommodate networks of virtually any size.

Types of content

IBM Endpoint Manager is based on contents. The generic term of content might represent data to distribute to targets, or instructions to run on targets, or queries to run on targets.

IBM Endpoint Manager implementation is based on these different types of content:

Action

An action is a script that runs on selected targets. Actions are used to fix policy violation and security exposures, to run configuration steps or, in general, to run operations or commands on targets. Fixlets, tasks, and baselines contain actions and depend on actions to run their remediation mission.

For more information about actions, see the *Actions* chapter in the *IBM Endpoint Manager Console Operator's Guide*.

Fixlet A Fixlet is a document that contains instructions that the IBM Endpoint Manager agents on target systems use to assess their status, identify issues, such as a vulnerability or a lack of compliance with a policy rule, and take corrective actions to resolve.

For more information about Fixlets, see the *Fixlets and Tasks* chapter in the *IBM Endpoint Manager Console Operator's Guide*.

Task A task is a document that contains instructions that IBM Endpoint Manager agents on target systems use to run locally commands or configuration activities.

For more information about tasks, see the *Fixlets and Tasks* chapter in the *IBM Endpoint Manager Console Operator's Guide*.

Baseline

A baseline is a deployment container of Fixlets and tasks. You can use it to apply a set of contents at the same time to one or more targets. The contents are applied according to the sequence specified in the baseline description. For example, a baseline might contain:

1. A Fixlet to install a product.
2. A Fixlet to upgrade it to a required level.
3. A task to configure the product that is installed.

When the baseline is deployed, the contents are applied respecting the predetermined sequence.

For more information about baselines, see the *Baselines* chapter in the *IBM Endpoint Manager Console Operator's Guide*.

Analysis

An analysis is a collection of property expressions that allows an operator to view and summarize various properties of IBM Endpoint Manager Client computers across a network.

For more information about analyses, see the *Analyses* chapter in the *IBM Endpoint Manager Console Operator's Guide*.

You can access these types of contents from the IBM Endpoint Manager console. Each application that belongs to the IBM Endpoint Manager suite uses these contents to accomplish its activities. You can create your custom content to satisfy your specific needs. For example, you can create custom Fixlets to apply patches to your home-developed applications or to enforce your policy rules. You must have specific authorizations to create your custom content.

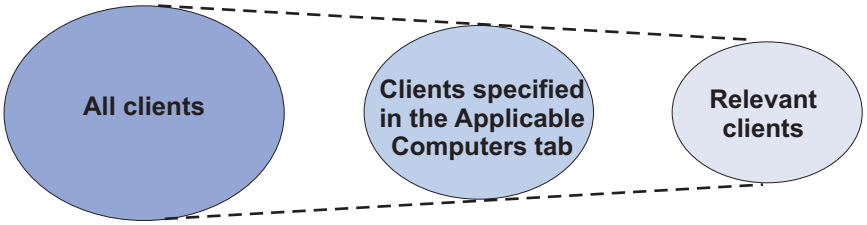
Contents are contained in content sites. These contents are automatically updated on a timely basis. The set of content sites available to you depends on the IBM Endpoint Manager product licenses that you bought. For more information about

accessing content sites, see the *Post installation steps* topic in the *IBM Endpoint Manager Console Administrator's Guide*. If you have the required authorizations, you can create your own custom content site to collect your custom contents.

How to identify on which targets to apply content

One of the main strengths of IBM Endpoint Manager is the ability to determine which targets the content applies to, in other words, which computers need that content. This is accomplished using Relevance expressions. Relevance expressions are part of the content definition and their scope is to interrogate the hardware and software properties of your managed clients to ensure that a patch or a maintenance activity, for example, is applied to only those computers that need it, and to no others.

When you define a content, you specify in the Applicable Computer tab a set of computers that can be targets for that content. Relevance evaluation narrows down this set of computers and selects only those computers that really must apply that content.



Even though relevance expressions are used in the same way for all types of content, depending on the type of content, the relevance triggers different behaviors:

Relevant action
It represents a violation to be remediated by running the instructions stated in the action description using the Action script language. Actions incorporate relevance clauses that can be customized at run time in the Take Action dialog.

Relevant Fixlet
It means that the computer is out-of-compliance with a policy rule. When the Fixlet is relevant, the actions that are contained in the Fixlet definition can be run to remediate the issue. After the actions run, the relevance is evaluated again to check if the vulnerability is fixed.

For example, a Fixlet can be used to install Symantec Endpoint Protection. This Fixlet is relevant for those computers where Symantec Endpoint Protection is not installed. After the Fixlet is installed on all the relevants computers, it is no longer marked as relevant. If, later, Symantec Endpoint Protection is uninstalled on one or more computers specified in the Applicable Computers tab, the Fixlet is marked as relevant again.

Relevant task
It indicates that the computer has a violation of a configuration standard or requirement or it must run maintenance activities.

For example, a task can be used to start Symantec Endpoint Protection. This task is relevant for those computers where Symantec Endpoint Protection is not active.

When the task is relevant, the actions that are contained in the task definition can be run to remediate the issue. After all the steps of the actions have completed, the task is marked as not relevant on the computer. The relevance expression *is not* evaluated again. As a best practice, success criteria can be used to determine whether the actions completed successfully to ensure that the remediation efforts succeeded in solving the problem.

Relevant baseline
It informs that one or more of the Fixlets that it contains is relevant for one or more computers that satisfy the criteria of both relevance expressions, those specified in the Fixlet description and those specified in the baseline's Applicable Computers tab. If nothing is specified in the baseline's Applicable Computers tab, then no restriction applies to the Fixlet or task applicability.

For example, a baseline might contain Fixlets and tasks for both Windows and Linux operating systems, however, if the baseline's Applicability Computers states that only Windows computers are relevant then only the Fixlets and tasks that are applicable for Windows are considered.

Note: Even though the baseline contains tasks, the Fixlet behavior is applied.

Relevant analysis
It runs property queries, according to their query intervals, and sends the results back to the server. The results are then displayed on the IBM Endpoint Manager console.

When a computer evaluates relevance of a newly-gathered document, for example a Fixlet or an analysis, it posts the results, and these results are then displayed on the IBM Endpoint Manager console. After the initial evaluation, the computer only reports changes, because there is no benefit in using network bandwidth to report the same result.

Relevance expressions are written in a human-readable proprietary language called Relevance Language.

For information about the Relevance language, see the *Relevance Language Guide*.

If you have Custom Content authorization, you can write a new relevance expression or modify existing expressions, to tailor content delivery to your needs. For more information about assigning authorizations to operators, see Operators permissions.

A patch management scenario

Follow the steps listed in these topics to learn how to deploy a patch using the Patch Management application on a newly installed IBM Endpoint Manager. All the steps are run from the IBM Endpoint Manager console.

This scenario applies to Windows operating systems. You can follow the same procedure to enable and apply patches also on other operating systems.

The scenario is divided into two parts:

- "Configuring Patch Management for Windows patches" on page 10
- "Applying a Windows patch" on page 12

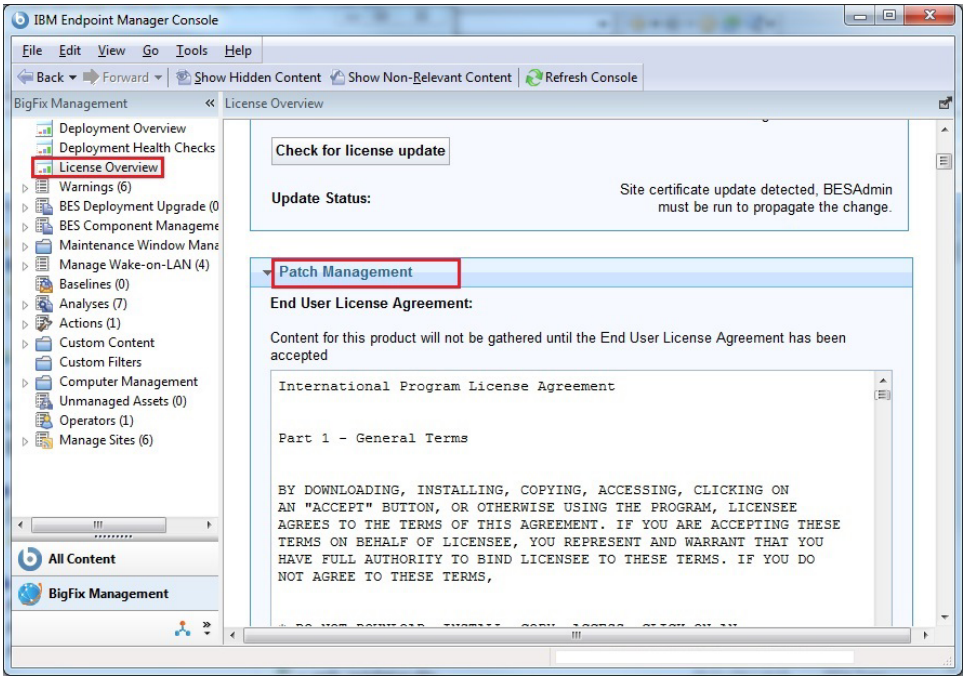
Configuring Patch Management for Windows patches

After installation, the IBM Endpoint Manager product is automatically set up to subscribe to certain management and maintenance sites. In this way content from those sites automatically flows into your enterprise and is evaluated for relevance on all computers running the IBM Endpoint Manager client.

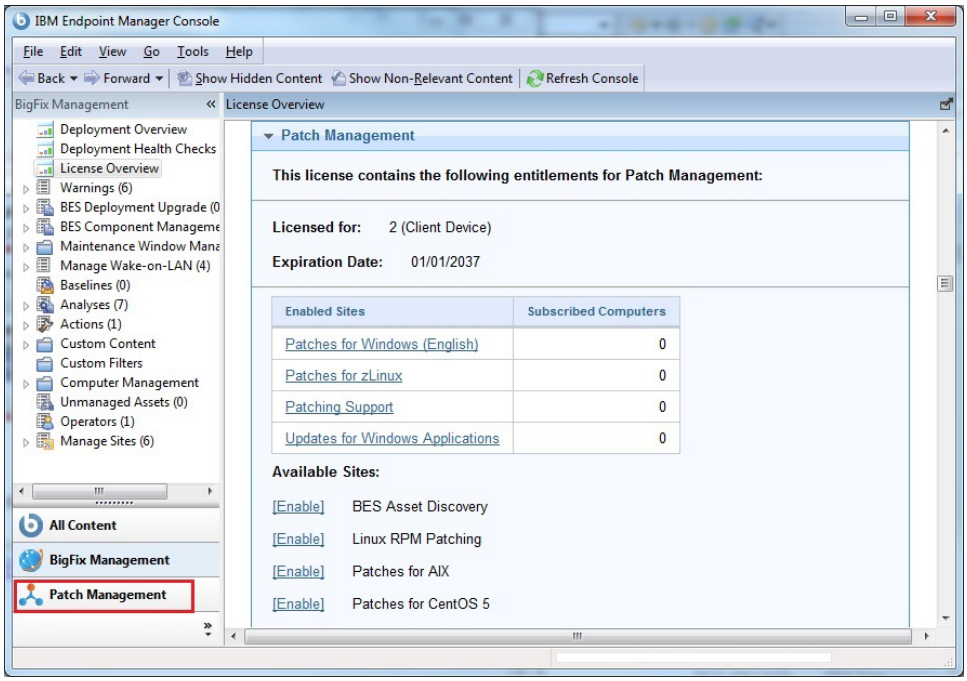
Run these steps to subscribe to the Patch Management site:

1. Open the IBM Endpoint Manager console by double clicking the icon:

2. Click the **License Overview** dashboard.
3. Scroll down to the Patch Management area.

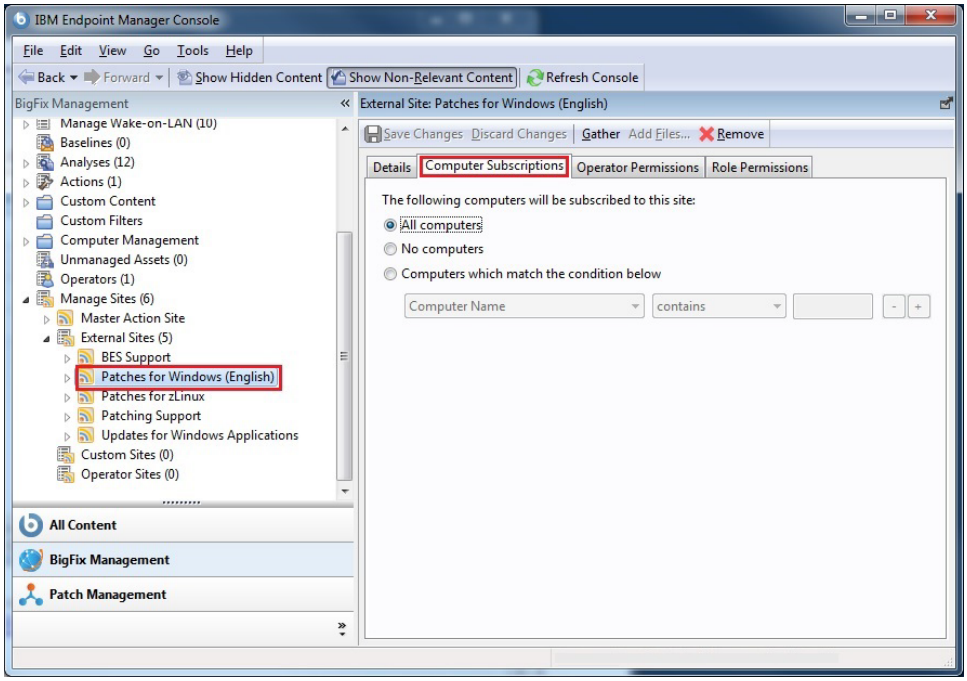


4. Read and accept the Patch Management license agreement.
5. In the **Available sites** click **Enable** beside **BES Asset Discovery**, **Patches for Windows (English)**, **Patching support** and **Updates for Windows Applications** to enable download content from the Patch Management web site.



The Patch Management site is now listed in the **Manage Sites** node of the domain panel.

6. Open the **Manage Sites** node and select **Patches for Windows (English)**.
7. From the site dialog, click the **Computer Subscriptions** tab and then select **All computers**.

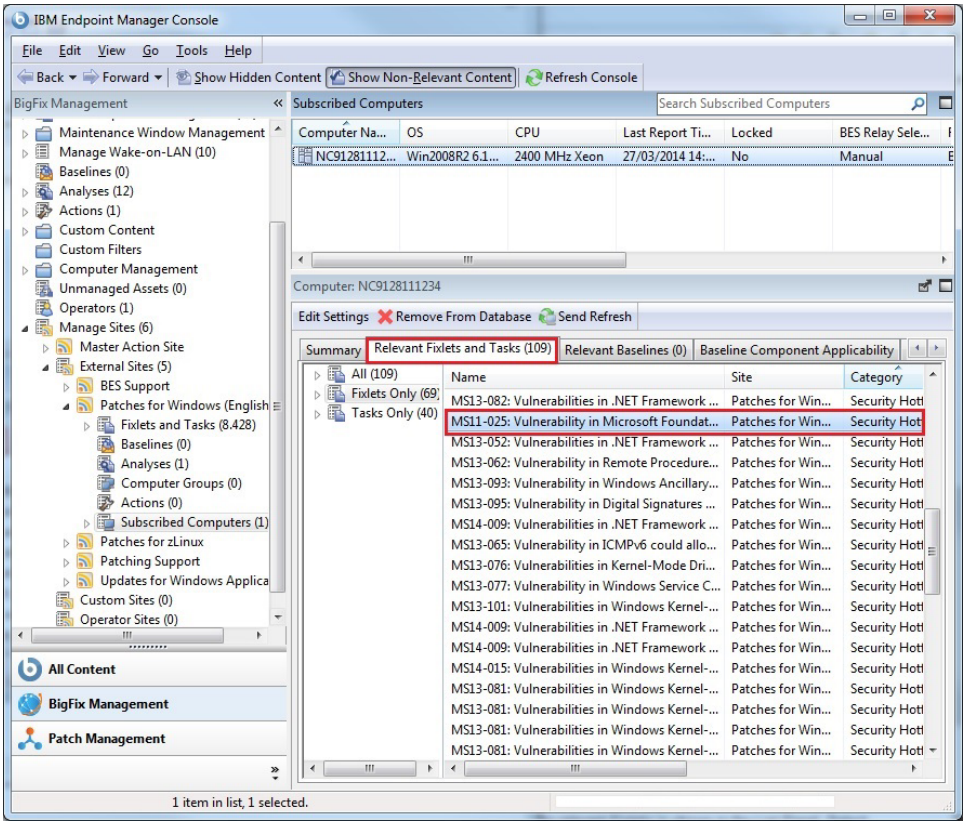


8. You can either wait for the gather process to automatically run or you can click **Gather** to start downloading the available contents from the selected sites.
9. After the gather process completes, the **Patches for Windows (English)** subtree is populated with the new content.

Applying a Windows patch

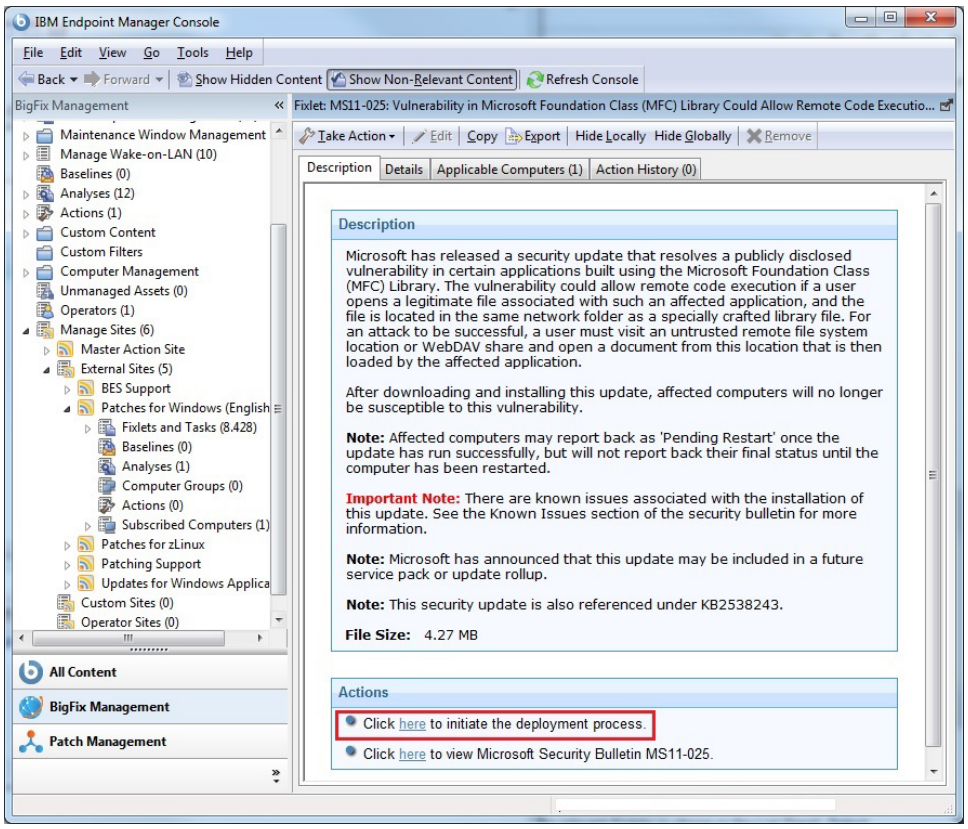
Run the following steps from the console to apply a Windows patch:

1. Expand the **Patches for Windows (English)** subtree and click **Subscribed Computers**. In the **List panel** you see an entry representing the client installed on the server system.
2. Select the **Relevant Fixlets and Tasks** tab to display the list of Fixlets that are relevant for the selected client.

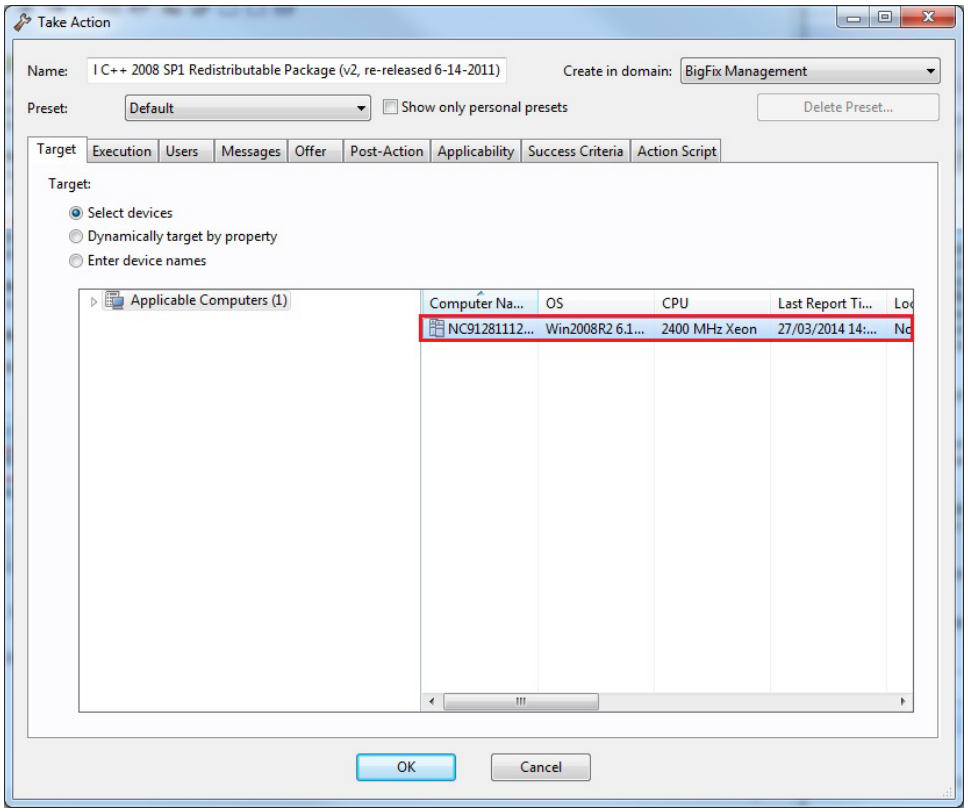


A Fixlet is relevant for a client if the client *needs* to install the content referenced in the Fixlet. The need to install that content is automatically evaluated on the Client using a set of predefined conditions specified in Fixlet.

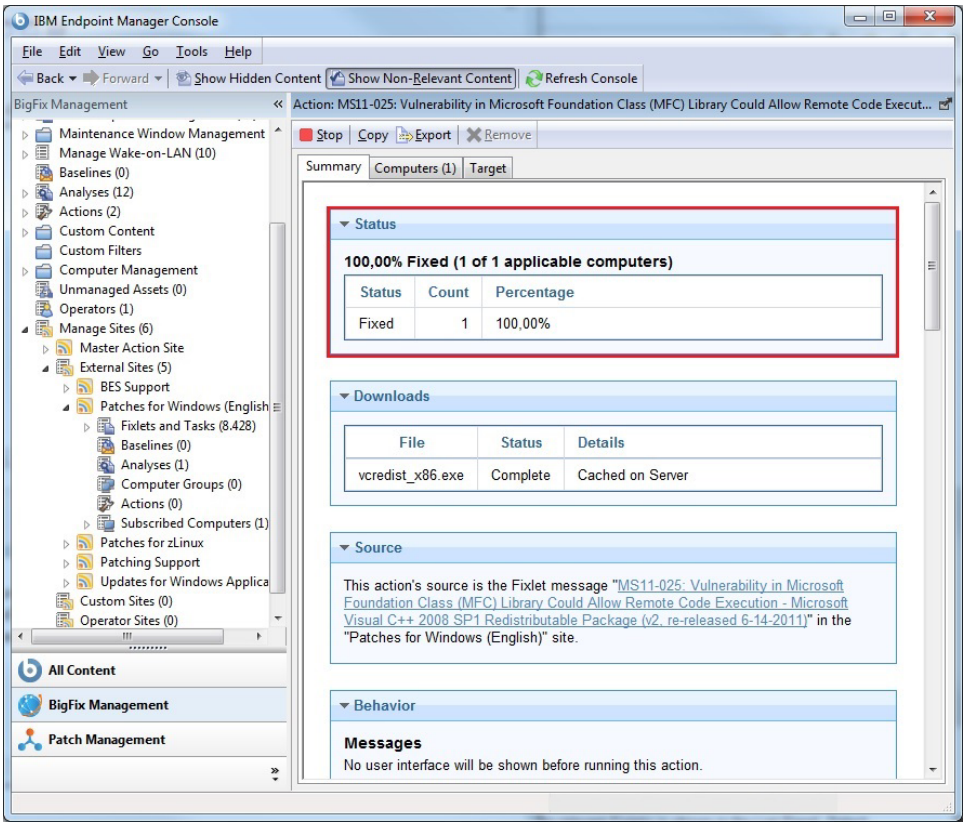
3. Double click a Fixlet to access the Fixlet description.
4. In the **Actions** pane choose to initiate the deployment process.



5. The **Take action** panel opens. In this panel select the client and then click **OK** to start the deployment.



6. You are automatically redirected to the **Action** panel. The status pane shows the progression of the deployment of the Fixlet. The status changes from **Not evaluated** to **Evaluating** to **Fixed** if the vulnerability on the client is successfully fixed. The remove of the vulnerability is automatically evaluated on the Client using a set of predefined conditions specified in the **Success Criteria** tab of the Action.



7. After the vulnerability is removed the client does not need to apply again the Fixlet and the Fixlet is marked as not-relevant for the client.

Appendix. Support

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

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

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

Printed in USA