BigFix
Getting Started

Special notice

Before using this information and the product it supports, read the information in Notices (on page 49).

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..... 2

Edition notice..... 3

Chapter 1. Introduction..... 1

Chapter 2. BigFix Platform..... 3

Chapter 3. BigFix applications..... 6

Chapter 4. A sample architecture..... 9

Chapter 5. Types of content..... 10

Chapter 6. How to identify on which targets to apply content..... 12

Chapter 7. A patch management scenario..... 15

Chapter 8. Security Overview..... 23

Chapter 9. BigFix Relays..... 28

Appendix A. Glossary..... 33

Appendix B. Support..... 48

Notices..... 49

Index.....

Chapter 1. Introduction

BigFix 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.

BigFix 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 are accessible from anywhere in your network by using the BigFix console.

Typically, a BigFix installation consists of the following parts:

- BigFix Platform *(on page 3)*
- One or more BigFix applications *(on page 6)*

For more details about the product, see:

- A sample architecture *(on page 9)*
- Types of content *(on page 10)*
- How to identify on which targets to apply content *(on page 12)*

Chapter 2. BigFix Platform

All the BigFix applications run on top of the BigFix platform.

The BigFix 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. For information about the supported versions, see Server requirements.

In terms of features and benefits, BigFix 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 BigFix 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. For information about Console requirements, see Console requirements.

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

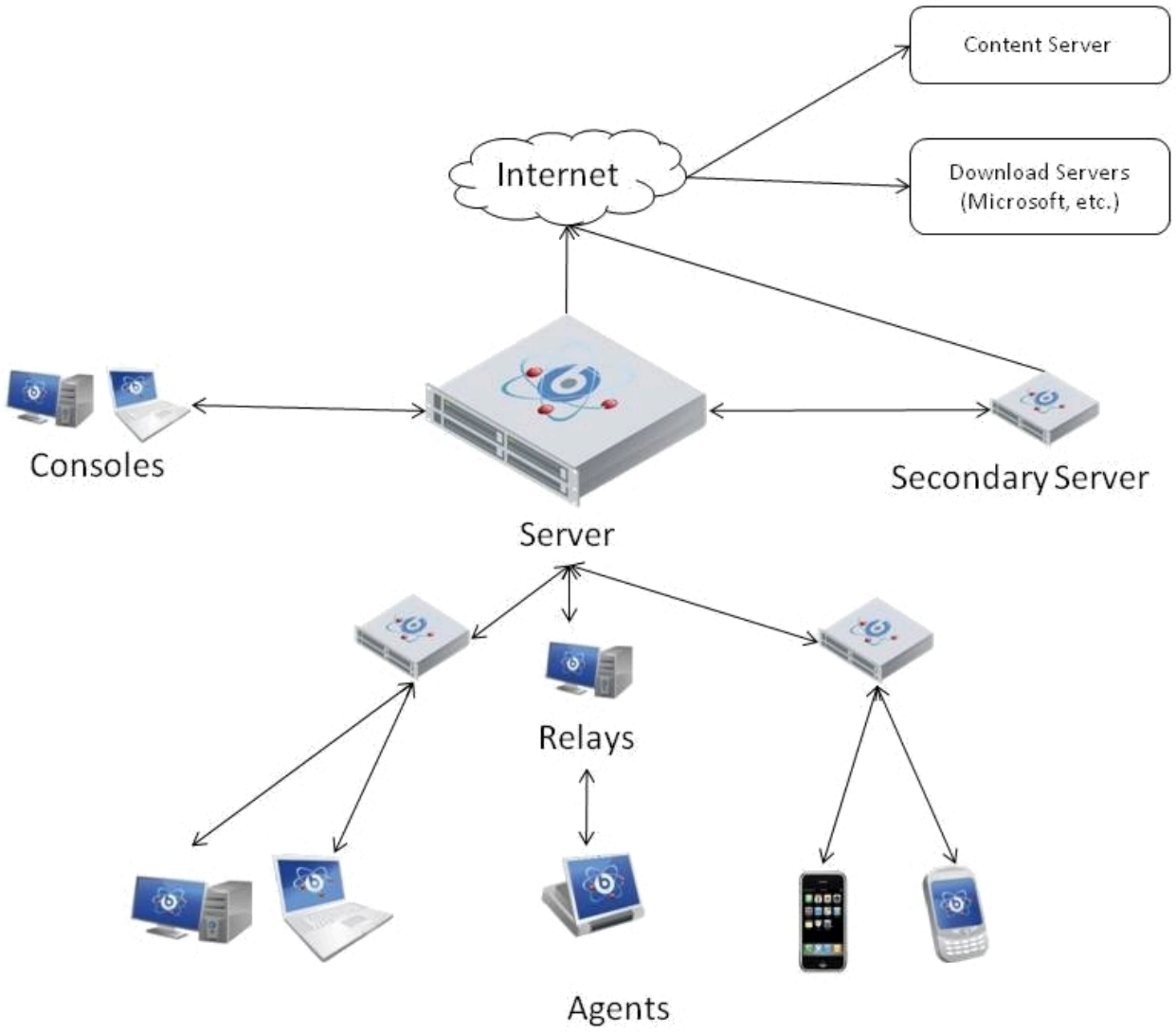
A Disaster Server Architecture (DSA) server, which replicates the server information for disaster recovery. If a BigFix server fails, other BigFix servers automatically take over as fully functional BigFix servers.

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 BigFix 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.



Chapter 3. BigFix applications

The BigFix solution comprises several application products that provide consolidated security and operations management, simplified and streamlined endpoint management, while increasing accuracy and productivity.

BigFix Lifecycle

Use this application to provide administrators with an agent-based tool that delivers accurate visibility into the state of endpoints and automatically remediates issues.

BigFix Lifecycle includes the following applications:

OS Deployment

Provides a consolidated, comprehensive solution to quickly deploy new workstations and servers throughout a network from a single, centralized location.

Power Management

Manages and monitors the power usage settings on the computers in your network. It also manages and applies the company conservation policies that you set with the use of dashboards, wizards, and web reports.

Remote Control

Remotely takes over and monitors workstations and servers in your deployment.

Server Automation

Automates provisioning workflows. You can automate a sequence of Fixlets, tasks, and baselines across different endpoints, such as servers or computers.

Software Distribution

Provides a consolidated, comprehensive solution to quickly deploy software throughout a network from a single, centralized

location. It provides cost-effective operational control and visibility of your software delivery and installation process.

For more information about BigFix Lifecycle, see BigFix Lifecycle Help Center.

BigFix Patch

Use this application to provide an automated, simplified patching process to all distributed endpoints. It manages both operating system and software application patches.

For more information about BigFix Patch, see BigFix Patch Help Center.

BigFix Compliance

Use this application to protect endpoints, automate remediation, and assure regulators that you are meeting security compliance standards.

For more information about BigFix Compliance, see BigFix Compliance Help Center.

BigFix Inventory

Use this application to scan monitored computers to:

- Identify which 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.

For more information about BigFix Inventory, see BigFix Inventory Help Center.

You can decide to add applications that belong to the BigFix solution later by buying extra licenses; they will automatically be available for use on the BigFix Console. You do not have to install any additional software or buy new hardware when you add applications that belong to the solution. Only Asset Discovery and Inventory require the installation of new components, but the installation is done by BigFix itself.

Note: Asset Discovery is a BigFix platform component that allows you to identify unmanaged assets in your network.

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

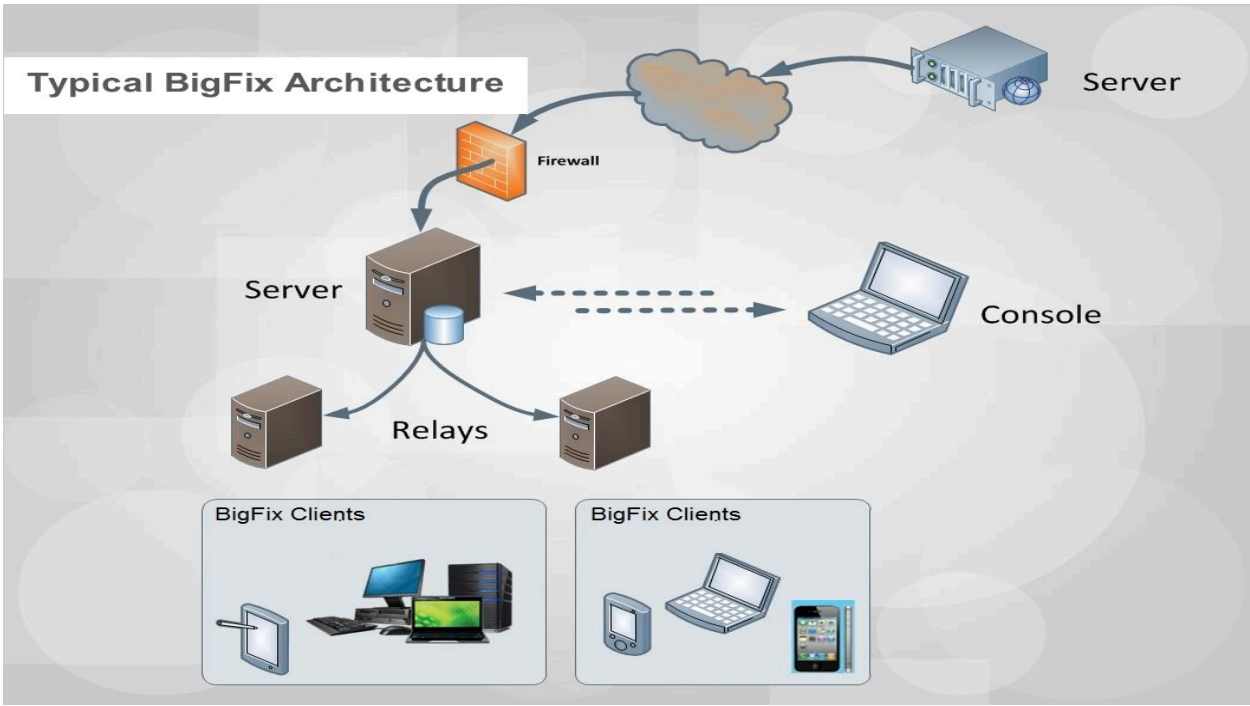
Consider that some capabilities are common to more than one application in the BigFix product solution. For example, as you can see in the picture, the capability to apply OS and software application patches is available in the Patch application, as well as in the Compliance and Lifecycle applications.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

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

Chapter 4. A sample architecture

A sample architecture helps you to plan your environment.

A typical installation has at least one BigFix 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.

BigFix 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.

Chapter 5. Types of content

BigFix 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.

BigFix 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 Actions.

Fixlet

A Fixlet is a document that contains instructions that the BigFix 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 Fixlets and Tasks.

Task

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

For more information about tasks, see Fixlets and Tasks.

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 Baselines.

Analysis

An analysis is a collection of property expressions that allows an operator to view and summarize various properties of BigFix client computers across a network.

For more information about analyses, see Analyses.

You can access these types of contents from the BigFix console. Each application that belongs to the BigFix 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 and are automatically updated on timely basis. The set of content sites available to you depends on the BigFix product licenses that you bought. For more information about accessing content sites, see Post-installation steps. If you have the required authorizations, you can create your own custom content site to collect your custom contents.

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 BigFix product licenses that you bought. If you have the required authorizations, you can create your own custom content site to collect your custom contents.

Chapter 6. How to identify on which targets to apply content

BigFix helps you identify on which targets to apply content.

One of the main strengths of BigFix is its 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 relevant 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 Applicable Computers tab. If nothing is specified in the baseline 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 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 BigFix 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 BigFix 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.

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 Mapping authorized activities with permissions.

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 Mapping authorized activities with permissions.

Chapter 7. 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 BigFix server. All the steps are run from the BigFix 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:

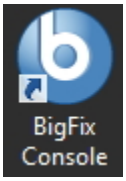
- Configuring Patch Management for Windows patches *(on page 15)*
- Applying a Windows patch *(on page 18)*

Configuring Patch Management for Windows patches

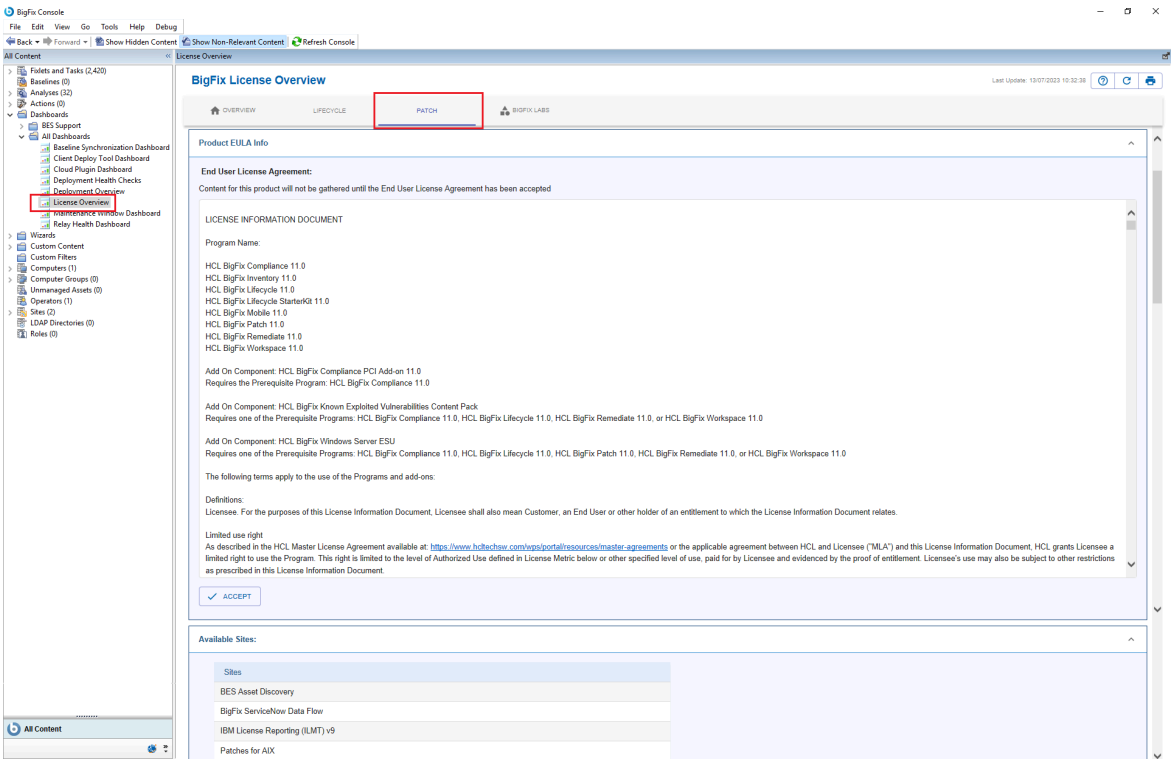
After installation, the BigFix product is automatically set up to subscribe to certain management and maintenance sites. In this way content from those sites automatically flows into your enterprise and is evaluated for relevance on all computers running the BigFix client.

Run these steps to subscribe to the Patch Management site:

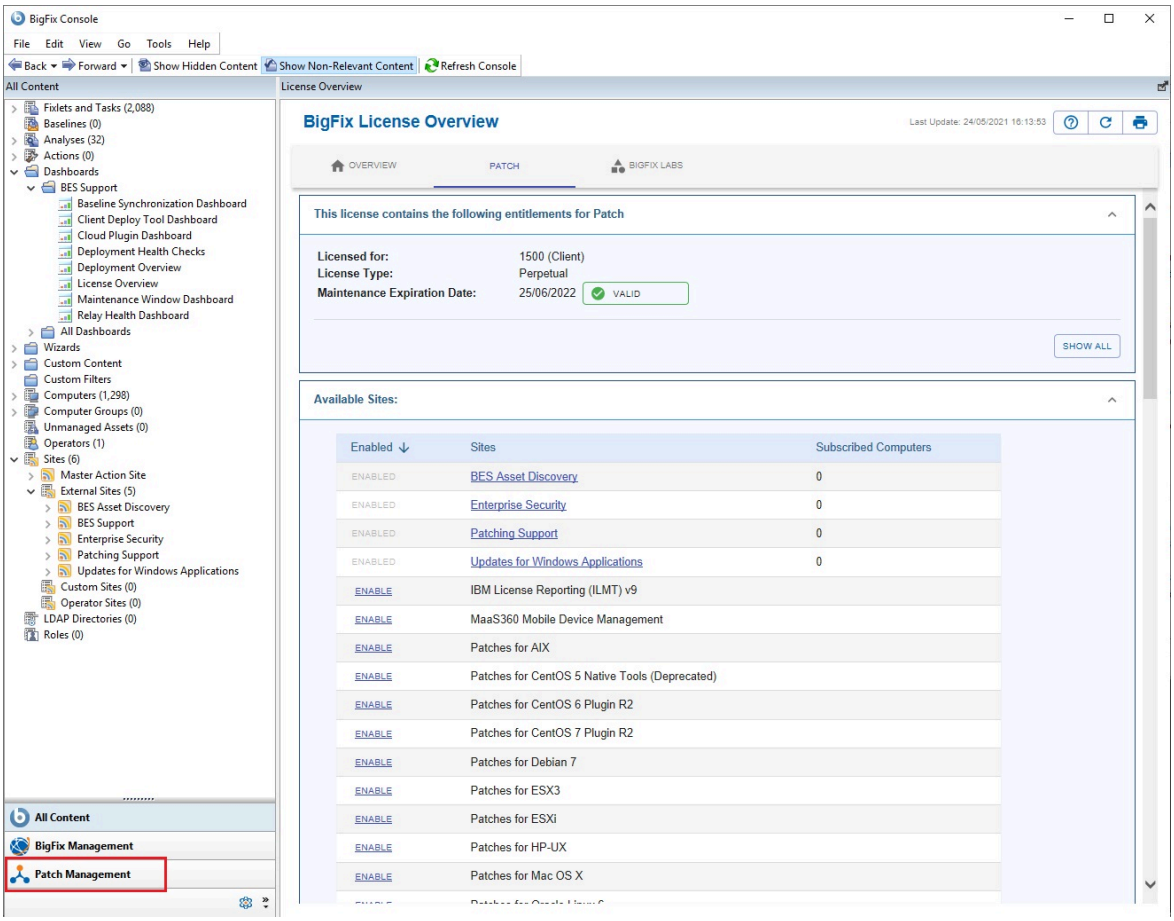
1. Open the BigFix console by double clicking the icon:



2. Click the **License Overview** dashboard.
3. Select the Patch Management tab.

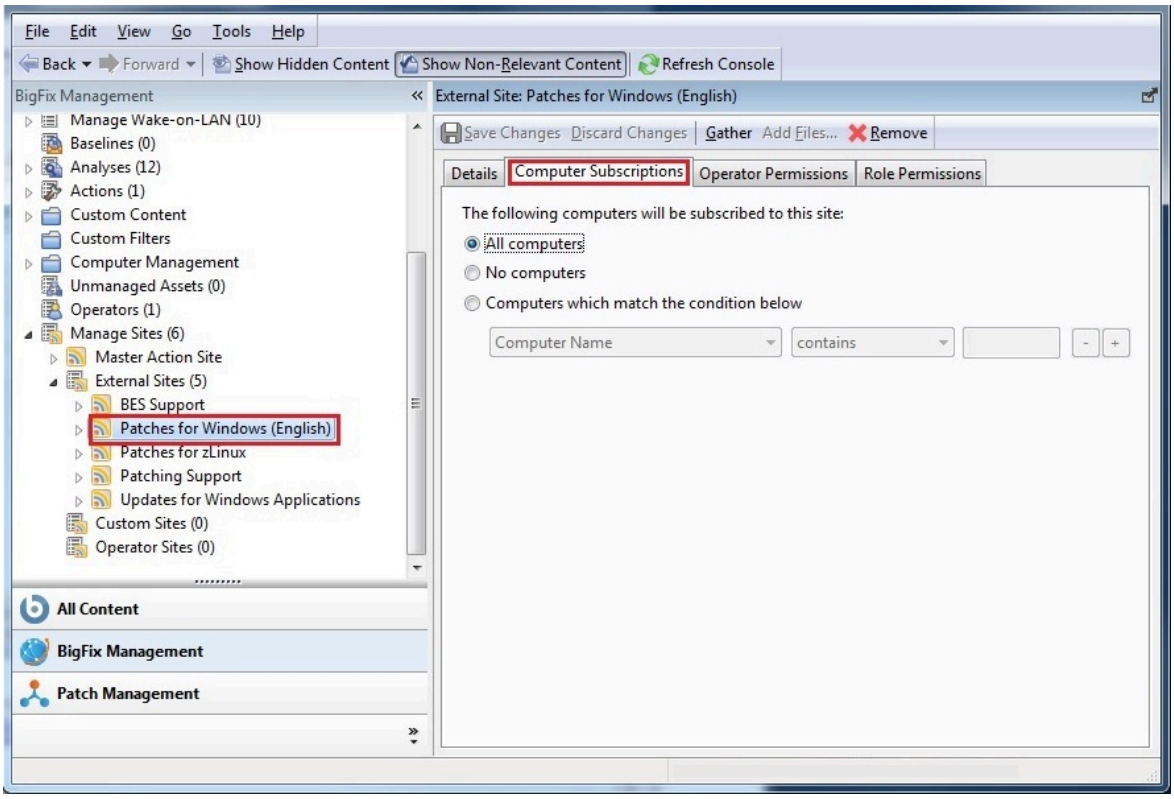


4. Read and accept the Patch Management license agreement.
5. In the **Available sites** click **Enable** beside **BES Asset Discovery**, **Patches for Windows (English)**, **Patching support** and **Updates for Windows Applications** to enable download content from the Patch Management web site.



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**.

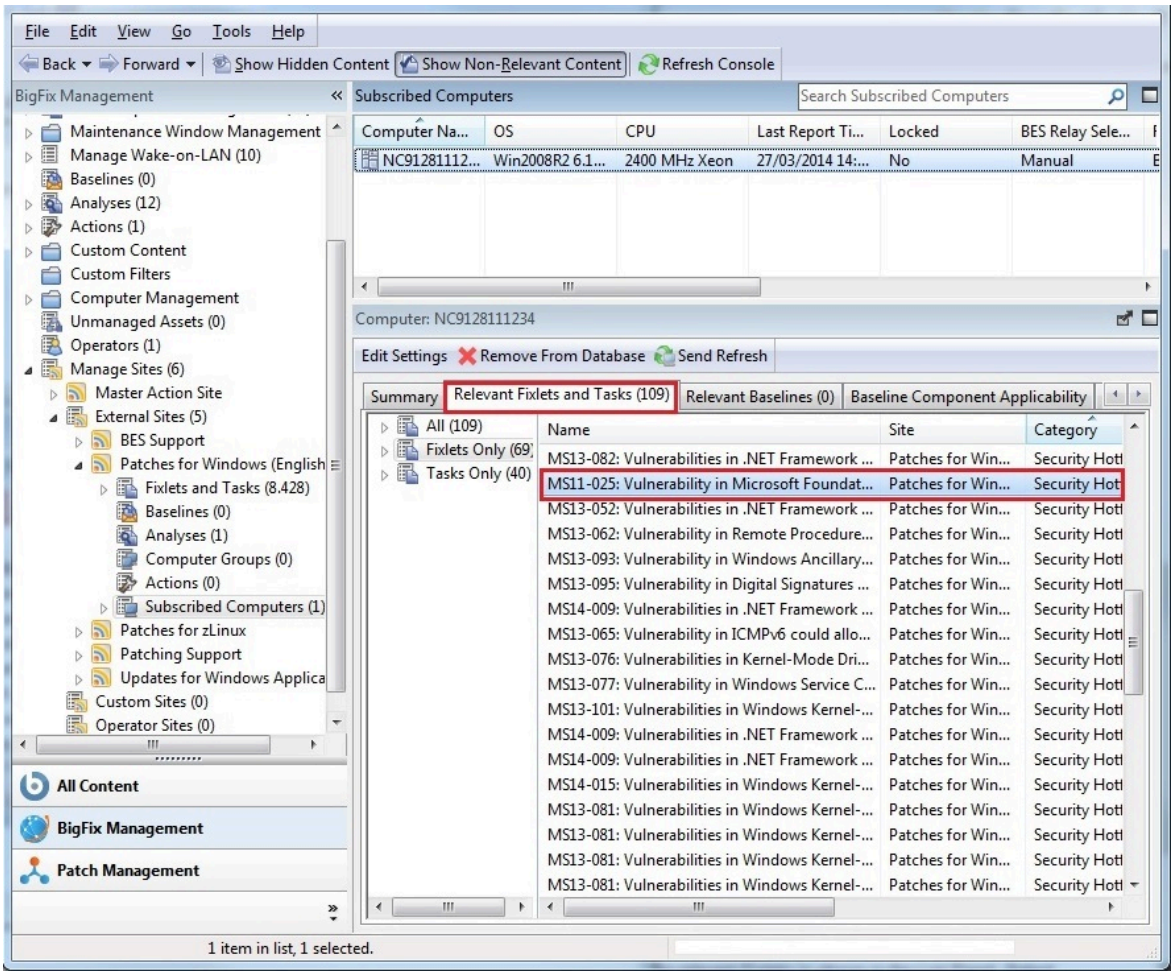


8. You can either wait for the gather process to automatically run or you can click **Gather** to start downloading the available contents from the selected sites.
9. After the gather process completes, the **Patches for Windows (English)** subtree is populated with the new content.

Applying a Windows patch

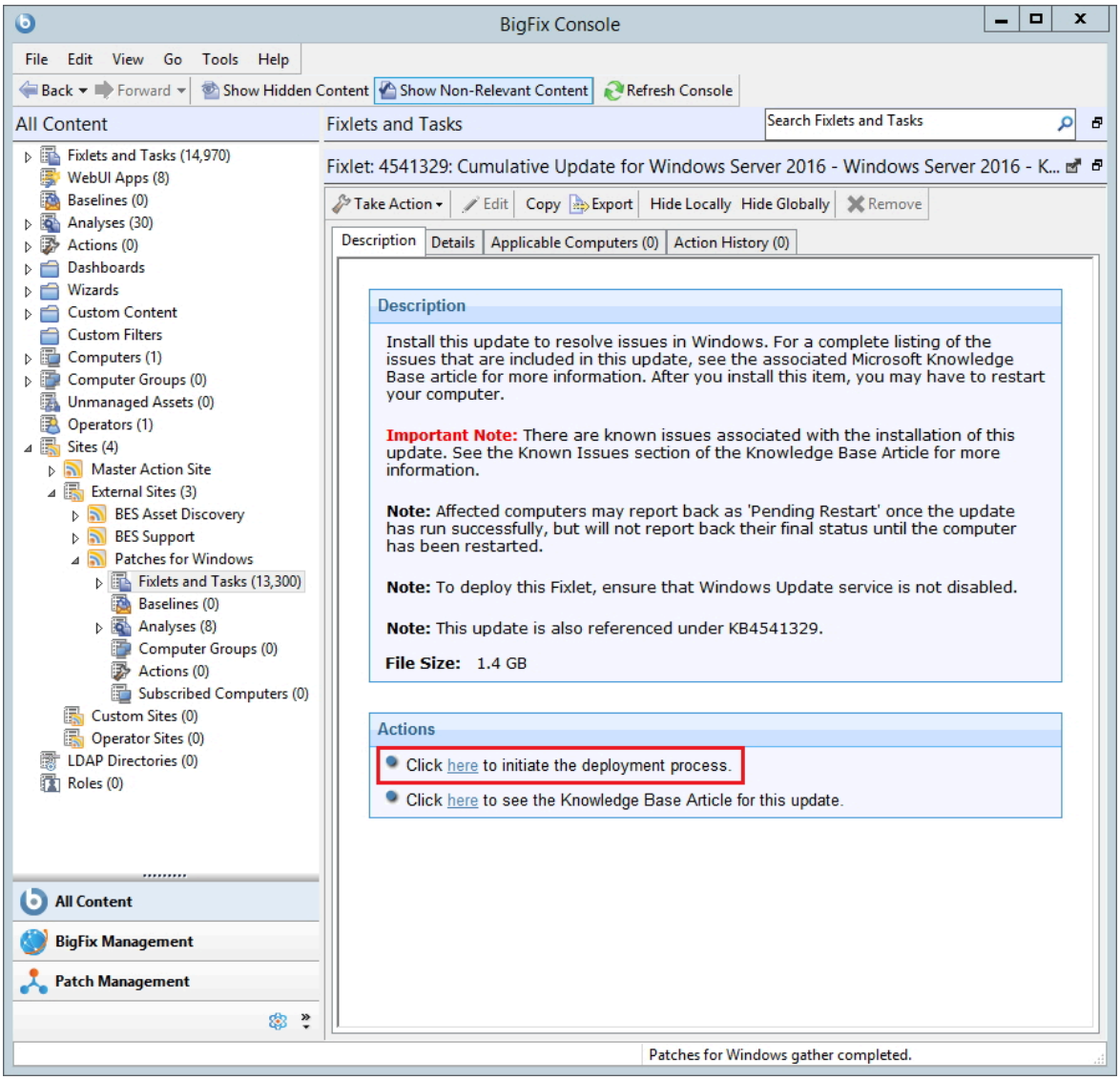
Run the following steps from the console to apply a Windows patch:

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.

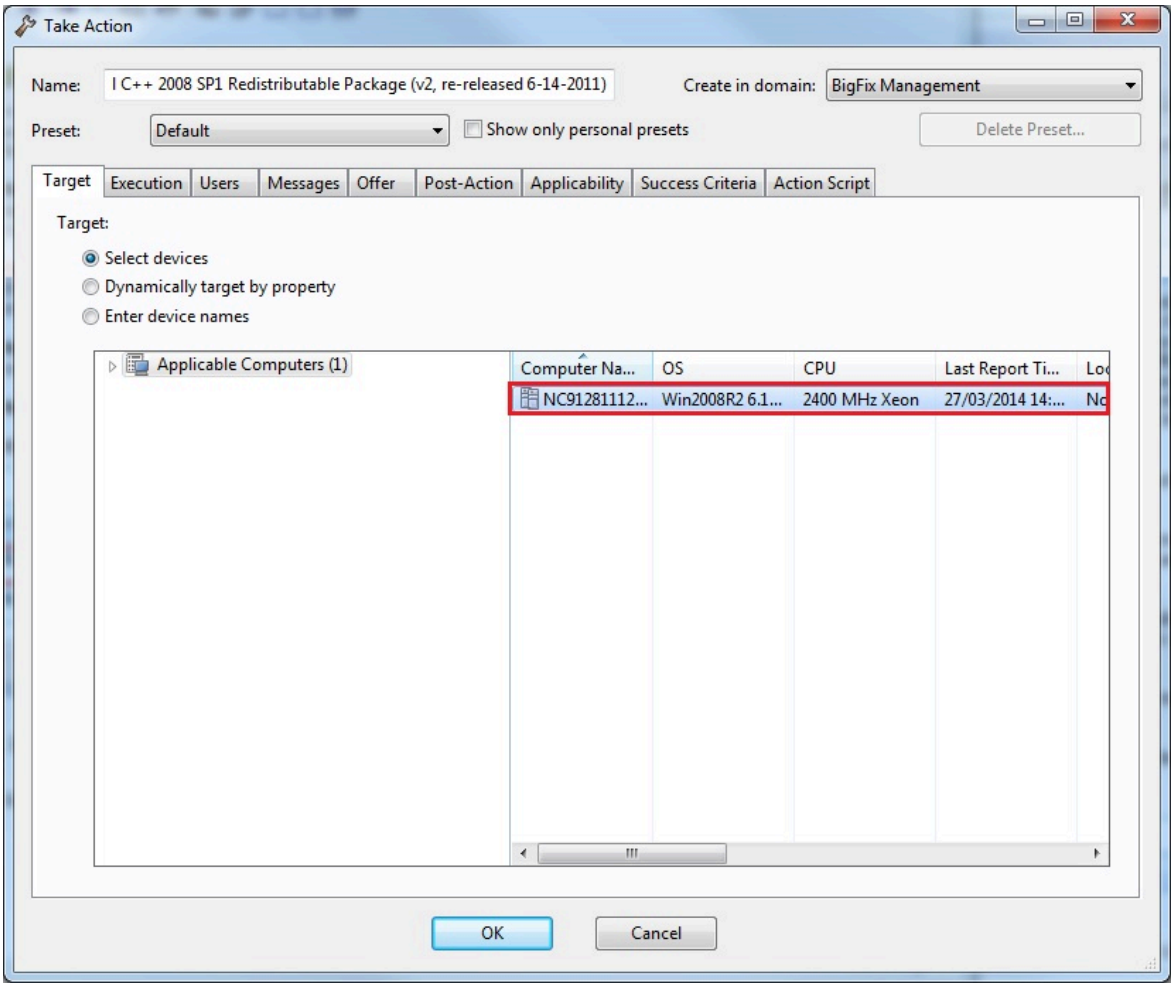


A Fixlet is relevant for a client if the client needs to install the content referenced in the Fixlet. The need to install that content is automatically evaluated on the Client using a set of predefined conditions specified in Fixlet.

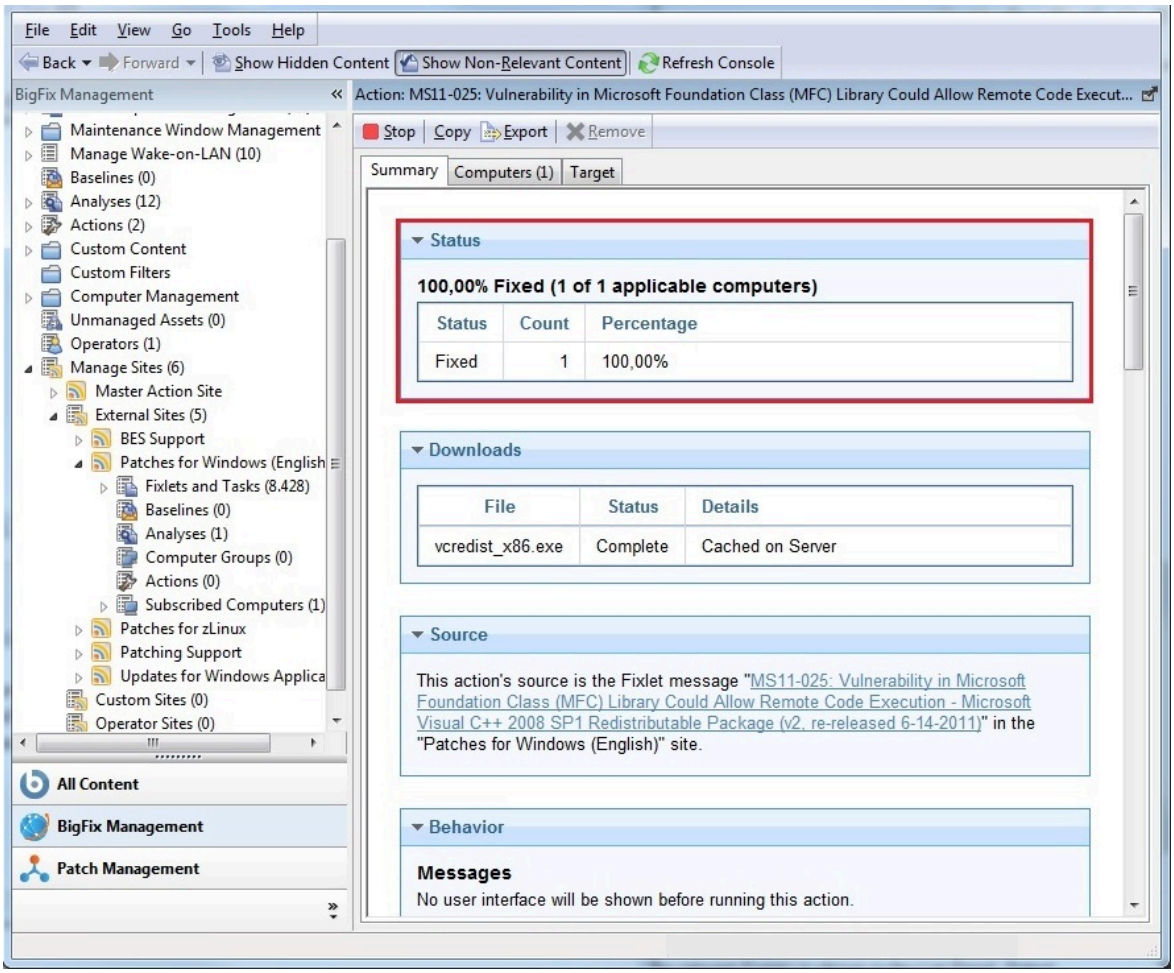
3. Double click a Fixlet to access the Fixlet description.
4. In the **Actions** pane choose to initiate the deployment process.



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.

Chapter 8. Security Overview

Introduction

BigFix is a systems and security management product that allows you to fully control all of the endpoints in your organization. This level of access, and the automation it brings, provides exceptional power and visibility into all of the computing endpoints managed by the system. Logically, one must also ensure that the management system itself be managed securely and audited regularly. BigFix provides strong security out-of-the-box but even a natively secure system still requires proper deployment, oversight, and configuration to ensure that it is protected from outside attackers or malicious operators. This document describes the overall security of the system and the attack vectors that each security feature is designed to counter for BigFix.

Installation: Site Administrator Key

This private key, generated during install is critical to the security of BigFix. This key should be created with a high-complexity password, copied to removable media, and stored in a locked safe. The original system on which the key was generated should have its free space wiped securely after the site key has been deleted from the system. Note that if this key is lost the entire BigFix deployment must be re-deployed, there is no "back door" or key recovery mechanism. HCL recommends a 4096 bit key over a 2048 bit key when creating the Site Administrator key. The latter is still secure but each year there is slow but steady progress in factoring improvements and computing power, each of which slowly chips away at the relative cryptographic strength of RSA asymmetric keys. The Site Administrator Key is used to create an X.509 certificate chain that is the basis for the security of the BigFix system (discussed below). Note that there are no default accounts or passwords created during the BigFix installation; this makes BigFix secure from simplistic attacks that target products that use well-known defaults.

Operation: Fixlets and Actions

All Fixlets and Actions managed by BigFix are protected by digital signatures using strong authentication: all signature hashes are created using SHA-256. Any time a Fixlet is received from HCL in a site update – such as a Windows patch definition or SCM check – the site includes a full directory listing of its contents including the name, size, sha1 and sha256 of

each file. The directory listing is digitally signed and the signature is verified against a public key distributed in the product binaries.

Any time a custom Fixlet is created by the customer it is protected in the same way and the directory listing is signed using the BigFix Server key which is part of the certificate chain created during installation. The BigFix components will reject any Fixlet that is inconsistent with the directory listing. This protects against data corruption and man-in-the-middle attacks. Custom Fixlets are also individually signed when first created and stored in the database, which prevents a database administrator (who is not an BigFix operator) or an attacker from inserting bogus Fixlets into the system.

Actions follow the same rule and are validated against a site's signed directory list. All actions – there are no exceptions to this rule – sent from the BigFix Server to BigFix Agents are also digitally signed. Again, this prevents against data corruption and, more importantly, prevents an attacker from masquerading as the BigFix Server or inserting malicious actions at any point in the Relay network architecture.

Not only will an BigFix Agent reject any content that fails the signature check but it will also reject properly signed messages that were created in another BigFix deployment. If your organization has two deployments (say, test and production) you can not accidentally control BigFix Agents that are from the wrong deployment since those Agents do not share the same certificate chain credentials.

Data in transit, Data at Rest

All communication between Relays and Agents can be encrypted using TLS. This prevents an eavesdropper from performing any analysis on the type of instructions being sent to endpoints or reading the reports sent from an Agent to the Server.

If you choose not to use TLS between Relay and Agent you can still choose to encrypt the report payload that an Agent sends back through the Relays to the Server. These AES-256 encrypted reports ensure that an attacker is unable to read information such as the list of patches or vulnerabilities that exist on an endpoint. This also means that for the brief period of time these reports are "at rest" in a Relay's cache they are secure from anyone who has access to a Relay computer.

Relays can also be configured to only communicate with Agents that can successfully authenticate using TLS based on a previously distributed certificate. This optional behavior ensures that internet-facing Relays will not expose any information – such as a list of available Fixlets – to attackers masquerading as an BigFix Agent trying to innocently gather instructions from your Relay infrastructure.

Notes:

- BigFix uses OpenSSL for all cryptographic operations
- An optional FIPS 140-2 mode is available. Note that in this mode an Agent will refuse to start if the host system does not provide enough entropy for the random number generator (this is an intentional fail-safe design).

Certificate Lifecycle

The site_admin_cert and private key are generated at deployment creation time. The site_admin_cert is signed by the license server, but HCL does not have access to the private key. The site_admin_cert only needs to be used in order to rotate the server_cert or for infrequent system configuration changes (e.g. upgrades), and so it can be kept offline in a protected place.

The server_cert is generated at server installation time and signed by the site_admin_cert certificate. The server_cert is bundled into the agent installer and is included on the endpoint in order to provide a chain of trust back to the root server. The server_cert can be rotated if compromised by using the site_admin private key.

The client_cert is generated on the endpoint at agent installation/registration time. Endpoint certificates are signed by the root server via a certificate signing request (CSR) process. The root server stores all client certificates in its database.

The relay_cert is generated and signed in the same manner as the client_cert.

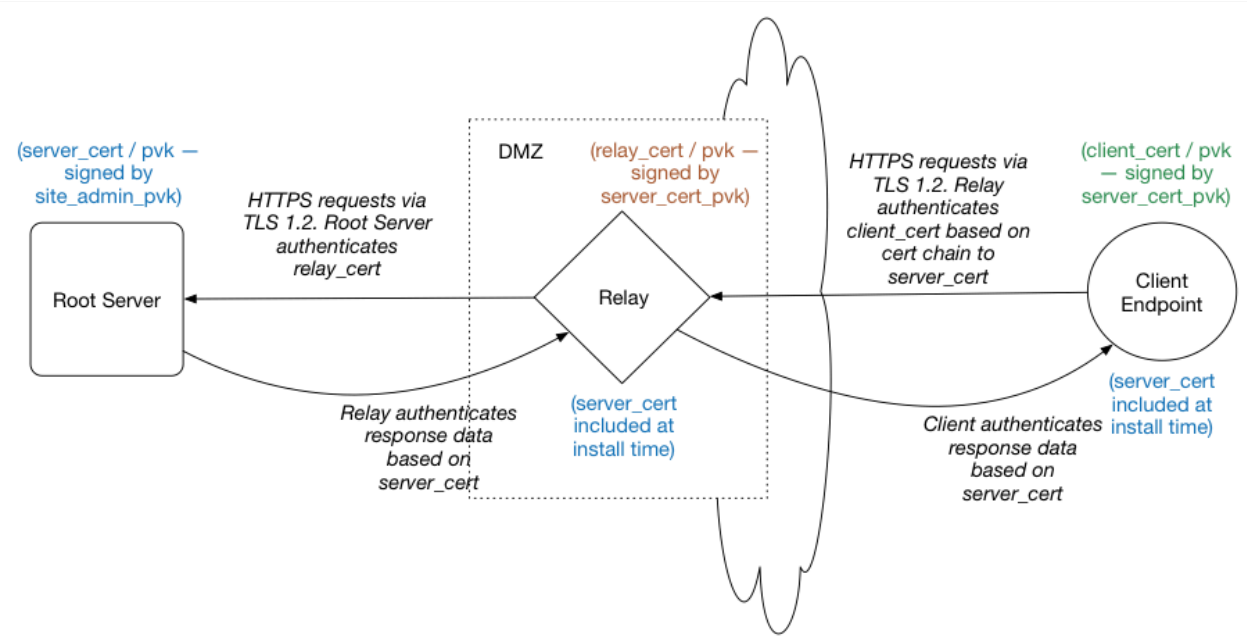
Endpoint certificates can be revoked in order to prevent them from connecting to the deployment.

All certificates used in these various internal operations ultimately derive from an internal BigFix Root CA, and are trusted based on public keys included in the product binaries. As a result, BigFix certificates will appear as self-signed certificates to vulnerability scanners, but

they are not actually self-signed certificates (which could be easily spoofed). The product will only function with valid BigFix certificates generated by our licensing process, and cannot be configured to use 3rd-party certificates signed by external CAs. This allows product security to be seamlessly built-in to its functionality from the start, eliminating external dependencies on certificate management and distribution. It also enables the BigFix Root Server to automatically manage product certificates, so BigFix or Server administrators do not need to manually maintain or renew endpoint certificates.

Note: The above statement only applies to internal communication and digital signature usage between BigFix components. External interfaces (WebUI, Web Reports, BCA, BFI, and the REST API) can be configured to use 3rd-party certificates.

Communication Security and Certificate Trust



Private Key Protection

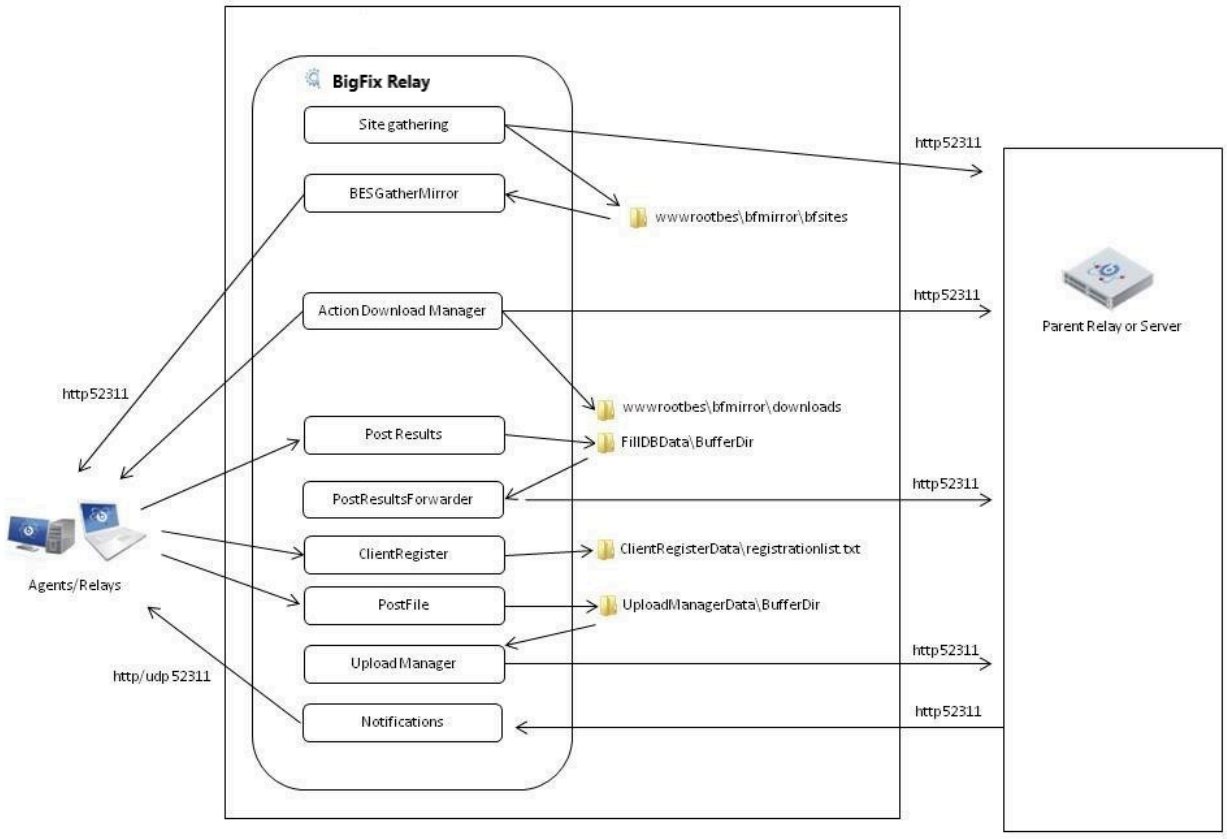
Private keys are protected in the following ways:

- on Windows: limit access to Administrator users via file permissions and use the Windows CryptoAPI to encrypt the private key on disk
- on Mac/Linux/Unix: limit access to root users via file permissions

Implication: the only way to compromise the server_certificate is to be an administrator/root on the root server machine itself.

Chapter 9. BigFix Relays

For more information on Relays, see Managing relays.



BigFix Relays allow an N-tier hierarchy to be created for the transmission of information from the BigFix Clients to the BigFix Server in the BigFix Enterprise. Following are Frequently Asked Questions about BigFix Relays.

What do BigFix Relays do?

- BigFix Relays "relay" information to and from the BigFix Client and another BigFix Relay or the BigFix Server.
- BigFix Relays enable BigFix Clients to gather the latest information about new Fixlet messages, new actions, or new downloads.

- BigFix Relays enable BigFix Clients to pass status messages to the BigFix Server including action results, retrieved properties, and relevant Fixlet messages.
- BigFix Relays enable BigFix Clients to register their last known IP address so they can be "pinged" later if there is new information to gather.
- BigFix Relays enable BigFix Clients to download patches and other files.

Do I need to find/buy a separate dedicated computer to be a BigFix Relay?

- No! BigFix Relays are specially designed to work on shared systems.
- Any BigFix Client (on a supported BigFix Relay OS) can be a BigFix Relay.
- Most customers will deploy BigFix fully without purchasing a single BigFix Relay (even the largest deployments with over 3000 BigFix Relays).
- It is very common to deploy the BigFix Relay on server computers that already exist in the enterprise infrastructure. AV distribution servers, file servers, print servers, Active Directory servers, and more are all commonly used as BigFix Relays. Server computers make a good choice because servers tend to exist in the same places you want to place a BigFix Relay and they are rarely turned off; however, a server class computer is not a requirement of a BigFix Relay.
- A BigFix Relay uses minimal computer resources and is idle most of the time and it is designed to have minimal impact on a computer so there are no conflicts with other applications/services running on the same computer.
- BigFix Relays do *not* need server-class fault-tolerant hardware because the nature of the BigFix architecture makes the system fault-tolerant (because BigFix Clients will automatically fail-over to other near-by BigFix Relays in the event of a problem).
- BigFix Relays can also be deployed on standard desktop computers with no problems. Examples from current customers include BigFix Relays on secretary's computers, kiosk computers in retail stores, IT administrators' computers, and deprecated old desktop hardware that would have been thrown away but instead were used as BigFix Relays.
- BigFix Relays require no additional 3rd party software (e.g., SQL Server, IIS, and other applications are not required for the BigFix Relay).

Why use BigFix Relays?

- Bandwidth Savings - Often the BigFix Clients are not in the same geographic location as the BigFix Server, and often the different locations are connected by thin network pipes. By downloading from a BigFix Relay instead of the main BigFix Server, the information about the action and -- more importantly -- any files associated with the actions only need to be transferred across the thin pipe one time to the BigFix Relay instead of one time per BigFix Client. The BigFix Relay then distributes the information over the LAN to the BigFix Clients. The result is a substantial bandwidth savings. Without BigFix Relays, it would often be impossible to administer remote computers because of the bandwidth limitations.
- BigFix Server Scaling - The BigFix Server has a database and a web server and is the central communication piece of the whole system. A single computer can only accept so many inbound connections from BigFix Clients, BigFix Consoles, etc. Without using BigFix Relays, even a very powerful computer could easily be overwhelmed by only a few thousand BigFix Clients. By using BigFix Relays, you effectively distribute the load from the BigFix Server to the BigFix Relays allowing for the BigFix Server to scale to handle many more BigFix Clients, use less expensive hardware, and be more efficient.

How do BigFix Relays work?

- BigFix Relays are BigFix Clients that are running two extra services (BESGather and BESRelay).
- BigFix Relays act as a mini BigFix-specific webserver.
- BigFix Clients connect using standard HTTP on the specified port number (default 52311).
- BigFix Clients will request downloads, the latest Fixlet sites, and the latest action sites from the BigFix Relay.
- If the BigFix Relay does not have the latest information, it gets the data from another BigFix Relay or from the BigFix Server.
- BigFix Clients will send action results and retrieved property reports to the BigFix Relay, which will bundle and compress them and send them to another BigFix Relay or to the BigFix Server (the bundling and compression also saves network bandwidth).

- BigFix Relays will cache downloaded files so that it will not have to re-download the files if they are needed later. BigFix Relays (default cache size is 1 GB, but is configurable) use a least-recently-used (LRU) cache replacement scheme for when the cache fills up.

How do you administer BigFix Relays?

- Installing BigFix Relays is done by using an "Install BigFix Relay" task in the BigFix Console to designate a BigFix Client as a relay.
- To uninstall the BigFix Relay, you simply run the "Uninstall BigFix Relay" task in the BigFix Console.
- BigFix Clients can be told which BigFix Relay to point to by using the BigFix Console to set a BigFix Client (or groups of BigFix Clients based on properties like subnet, location, etc.) to use a primary and secondary relay.
- BigFix Clients can also be set to automatically find their closest BigFix Relays based upon network hops.
- BigFix Relays can be manually set to create a hierarchy or the BigFix Relays can establish a hierarchy automatically.

How does the BigFix Client/BigFix Relay Auto Selection work?

- BigFix Clients will choose their closest BigFix Relay by periodically "pinging" each BigFix Relay to determine which relay is the closest based upon the number of network hops. The default BigFix Relay selection period is 6 hours and is configurable.
- Each BigFix Client will make a list of their closest BigFix Relays. If they cannot reach their closest BigFix Relay because it is off or down, they will try the second closest, and so on.
- If a BigFix Client cannot find any BigFix Relays or they are all down, the BigFix Client will connect directly with the main BigFix Server.
- If more than one BigFix Relays are the same distance away from a BigFix Client, the BigFix Client will randomly choose amongst them.

What are the system requirements to be a BigFix Relay?

For details about relay capacity planning, see BigFix Capacity Planning

Do you have a "best practices" list for maintaining a healthy BigFix Relay deployment?

Yes. See the Relay Health page for more information.

Appendix A. Glossary

This glossary provides terms and definitions for the BigFix software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

A *(on page 33)* B *(on page 34)* C *(on page 35)* D *(on page 37)* E *(on page 39)* F *(on page 39)* G *(on page 39)* L *(on page 40)* M *(on page 40)* N *(on page 41)* O *(on page 41)* P *(on page 42)* R *(on page 42)* S *(on page 43)* T *(on page 45)* U *(on page 45)* V *(on page 46)* W *(on page 46)*

A

action

1. See Fixlet *(on page 39)*.
2. A set of Action Script commands that perform an operation or administrative task, such as installing a patch or rebooting a device.

Action Script

Language used to perform an action on an endpoint.

agent

See BigFix agent *(on page 34)*.

ambiguous software

Software that has an executable file that looks like another executable file, or that exists in more than one place in a catalog (Microsoft Word as a standalone product or bundled with Microsoft Office).

audit patch

A patch used to detect conditions that cannot be remediated and require the attention of an administrator. Audit patches contain no actions and cannot be deployed.

automatic computer group

A computer group for which membership is determined at run time by comparing the properties of a given device against the criteria set for group membership. The set of devices in an automatic group is dynamic, meaning that the group can and does change. See also computer group *(on page 35)*.

B

baseline

A collection of actions that are deployed together. A baseline is typically used to simplify a deployment or to control the order in which a set of actions are applied. See also deployment group *(on page 37)*.

BigFix agent

The BigFix code on an endpoint that enables management and monitoring by BigFix.

BigFix client

See BigFix agent *(on page 34)*.

BigFix console

The primary BigFix administrative interface. The console provides a full set of capabilities to BigFix administrators.

BYOD

Bring Your Own Device (BYOD) refers to employees using personal devices to connect to their organizational networks and access work-related systems and potentially sensitive or confidential data.

C

client

A software program or computer that requests services from a server. See also server *(on page 44)*.

client time

The local time on a BigFix client device.

Cloud

A set of compute and storage instances or services that are running in containers or on virtual machines.

Common Vulnerabilities and Exposures Identification Number (CVE ID)

A number that identifies a specific entry in the National Vulnerability Database. A vendor's patch document often includes the CVE ID, when it is available. See also National Vulnerability Database *(on page 41)*.

Common Vulnerabilities and Exposures system (CVE)

A reference of officially known network vulnerabilities, which is part of the National Vulnerabilities Database (NVD), maintained by the US National Institute of Standards and Technology (NIST).

component

An individual action within a deployment that has more than one action. See also deployment group *(on page 37)*.

computer group

A group of related computers. An administrator can create computer groups to organize systems into meaningful categories, and to facilitate deployment of content to multiple computers. See also automatic computer group *(on page 34)* and manual computer group *(on page 40)*.

console

See BigFix console *(on page 34)*.

content

Digitally-signed files that contain data, rules, queries, criteria, and other instructions, packaged for deployment across a network. BigFix agents use the detection criteria (Relevance statements) and action instructions (Action Script statements) in content to detect vulnerabilities and enforce network policies.

content relevance

A determination of whether a patch or piece of software is eligible for deployment to one or more devices. See also device relevance *(on page 38)*.

Coordinated Universal Time (UTC)

The international standard of time that is kept by atomic clocks around the world.

corrupt patch

A patch that flags an operator when corrections made by an earlier patch have been changed or compromised. This situation can occur when an earlier service pack or application overwrites later files, which results in patched files that are not current. The corrupt patch flags the situation and can be used to re-apply the later patch.

custom content

BigFix code that is created by a customer for use on their own network, for example, a custom patch or baseline.

CVE

See Common Vulnerabilities and Exposures system *(on page 35)*.

CVE ID

See Common Vulnerabilities and Exposures Identification Number *(on page 35)*.

D

data stream

A string of information that serves as a source of package data.

default action

The action designated to run when a Fixlet is deployed. When no default action is defined, the operator is prompted to choose between several actions or to make an informed decision about a single action.

definitive package

A string of data that serves as the primary method for identifying the presence of software on a computer.

deploy

To dispatch content to one or more endpoints for execution to accomplish an operation or task, for example, to install software or update a patch.

deployment

Information about content that is dispatched to one or more endpoints, a specific instance of dispatched content.

deployment group

The collection of actions created when an operator selects more than one action for a deployment, or a baseline is deployed. See also baseline *(on page 34)*, component *(on page 35)*, deployment window *(on page 38)*, and multiple action group *(on page 41)*.

deployment state

The eligibility of a deployment to run on endpoints. The state includes parameters that the operator sets, such as 'Start at 1AM, end at 3AM.'

deployment status

Cumulative results of all targeted devices, expressed as a percentage of deployment success.

deployment type

An indication of whether a deployment involved one action or multiple actions.

deployment window

The period during which a deployment's actions are eligible to run. For example, if a Fixlet has a deployment window of 3 days and an eligible device that has been offline reports in to BigFix within the 3-day window, it gets the Fixlet. If the device comes back online after the 3-day window expires, it does not get the Fixlet. See also deployment group *(on page 37)*.

device

An endpoint, for example, a laptop, desktop, server, or virtual machine that BigFix manages; an endpoint running the BigFix Agent.

device holder

The person using a BigFix-managed computer.

device property

Information about a device collected by BigFix, including details about its hardware, operating system, network status, settings, and BigFix client. Custom properties can also be assigned to a device.

device relevance

A determination of whether a piece of BigFix content applies to applies to a device, for example, where a patch should be applied, software installed, or a baseline run. See also content relevance *(on page 36)*.

device result

The state of a deployment, including the result, on a particular endpoint.

Disaster Server Architecture (DSA)

An architecture that links multiple servers to provide full redundancy in case of failure.

DSA

See Disaster Server Architecture *(on page 38)*.

dynamically targeted

Pertaining to using a computer group to target a deployment.

E

endpoint

A networked device running the BigFix agent.

F

filter

To reduce a list of items to those that share specific attributes.

Fixlet

A piece of BigFix content that contains Relevance and Action Script statements bundled together to perform an operation or task. Fixlets are the basic building blocks of BigFix content. A Fixlet provides instructions to the BigFix agent to perform a network management or reporting action.

Full Disk Encryption

To reduce a list of items to those that share specific attributes.

G

group deployment

A type of deployment in which multiple actions were deployed to one or more devices.

H

Hybrid cloud

The utilization of distinct sets of cloud services (typically public and private) with integration and/or orchestration across them.

L

locked

An endpoint state that prevents most of the BigFix actions from running until the device is unlocked.

M

MAG

See multiple action group *(on page 41)*.

management rights

The limitation of console operators to a specified group of computers. Only a site administrator or a master operator can assign management rights.

manual computer group

A computer group for which membership is determined through selection by an operator. The set of devices in a manual group is static, meaning they do not change. See also computer group *(on page 35)*.

master operator

A console operator with administrative rights. A master operator can do everything that a site administrator can do, except creating operators.

masthead

A collection of files that contain the parameters of the BigFix process, including URLs to Fixlet content. The BigFix agent brings content into the enterprise based on subscribed mastheads.

MCM and BigFix Mobile

Refers to the offering by Bigfix that is common for both Modern Client Management to manage laptops (Windows and macOS) and BigFix Mobile to manage mobile devices (Android, iOS, and iPadOS).

mirror server

A BigFix server required if the enterprise does not allow direct web access but instead uses a proxy server that requires password-level authentication.

Multicloud

The utilization of distinct sets of cloud services, typically from multiple vendors, where specific applications are confined to a single cloud instance.

multiple action group (MAG)

A BigFix object that is created when multiple actions are deployed together, as in a baseline. A MAG contains multiple Fixlets or tasks. See also deployment group *(on page 37)*.

N

National Vulnerability Database (NVD)

A catalog of officially known information security vulnerabilities and exposures, which is maintained by the National Institute of Standards and Technology (NIST). See also Common Vulnerabilities and Exposures Identification Number *(on page 35)*.

NVD

See National Vulnerability Database *(on page 41)*.

O

offer

A deployment option that allows a device holder to accept or decline a BigFix action and to exercise some control over when it runs. For example, a device

holder can decide whether to install a software application, and whether to run the installation at night or during the day.

open-ended deployment

A deployment with no end or expiration date; one that runs continuously, checking whether the computers on a network comply.

operator

A person who uses the BigFix WebUI, or portions of the BigFix console.

P

patch

A piece of code added to vendor software to fix a problem, as an immediate solution that is provided to users between two releases.

patch category

A description of a patch's type and general area of operation, for example, a bug fix or a service pack.

patch severity

The level of risk imposed by a network threat or vulnerability and, by extension, the importance of applying its patch.

R

relay

A client that is running special server software. Relays spare the server and the network by minimizing direct server-client downloads and by compressing upstream data.

Relevance

BigFix query language that is used to determine the applicability of a piece of content to a specified endpoint. Relevance asks yes or no questions and evaluates the results. The result of a Relevance query determines whether

an action can or should be applied. Relevance is paired with Action Script in Fixlets.

S

SCAP

See Security Content Automation Protocol *(on page 43)*.

SCAP check

A specific configuration check within a Security Content Automation Protocol (SCAP) checklist. Checks are written in XCCDF and are required to include SCAP enumerations and mappings per the SCAP template.

SCAP checklist

A configuration checklist that is written in a machine-readable language (XCCDF). Security Content Automation Protocol (SCAP) checklists have been submitted to and accepted by the NIST National Checklist Program. They also conform to a SCAP template to ensure compatibility with SCAP products and services.

SCAP content

A repository that consists of security checklist data represented in automated XML formats, vulnerability and product name related enumerations, and mappings between the enumerations.

SCAP enumeration

A list of all known security related software flaws (CVEs), known software configuration issues (CCEs), and standard vendor and product names (CPEs).

SCAP mapping

The interrelationship of enumerations that provides standards-based impact measurements for software flaws and configuration issues.

Security Content Automation Protocol (SCAP)

A set of standards that is used to automate, measure, and manage vulnerability and compliance by the National Institute of Standards and Technology (NIST).

server

A software program or a computer that provides services to other software programs or other computers. See also client *(on page 35)*.

signing password

A password that is used by a console operator to sign an action for deployment.

single deployment

A type of deployment where a single action was deployed to one or more devices.

site

A collection of BigFix content. A site organizes similar content together.

site administrator

The person who is in charge of installing BigFix and authorizing and creating new console operators.

software package

A collection of Fixlets that install a software product on a device. Software packages are uploaded to BigFix by an operator for distribution. A BigFix software package includes the installation files, Fixlets to install the files, and information about the package (metadata).

SQL Server

A full-scale database engine from Microsoft that can be acquired and installed into the BigFix system to satisfy more than the basic reporting and data storage needs.

standard deployment

A deployment of BigFix that applies to workgroups and to enterprises with a single administrative domain. It is intended for a setting in which all Client computers have direct access to a single internal server.

statistically targeted

Pertaining to the method used to target a deployment to a device or piece of content. Statically targeted devices are selected manually by an operator.

superseded patch

A type of patch that notifies an operator when an earlier version of a patch has been replaced by a later version. This occurs when a later patch updates the same files as an earlier one. Superseded patches flag vulnerabilities that can be remediated by a later patch. A superseded patch cannot be deployed.

system power state

A definition of the overall power consumption of a system. BigFix Power Management tracks four main power states Active, Idle, Standby or Hibernation, and Power Off.

T

target

To match content with devices in a deployment, either by selecting the content for deployment, or selecting the devices to receive content.

targeting

The method used to specify the endpoints in a deployment.

task

A type of Fixlet designed for re-use, for example, to perform an ongoing maintenance task.

U

UTC

See Coordinated Universal Time *(on page 36)*.

V

virtual private network (VPN)

An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

VPN

See virtual private network *(on page 46)*.

vulnerability

A security exposure in an operating system, system software, or application software component.

W

Wake-from-Standby

A mode that allows an application to turn a computer on from standby mode during predefined times, without the need for Wake on LAN.

Wake on LAN

A technology that enables a user to remotely turn on systems for off-hours maintenance. A result of the Intel-IBM Advanced Manageability Alliance and part of the Wired for Management Baseline Specification, users of this technology can remotely turn on a server and control it across the network, thus saving time on automated software installations, upgrades, disk backups, and virus scans.

WAN

See wide area network *(on page 46)*.

wide area network (WAN)

A network that provides communication services among devices in a geographic area larger than that served by a local area network (LAN) or a metropolitan area network (MAN).

Appendix B. 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

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.