BigFix® Enterprise Suite (BES™)

Administrator's Guide

BigFix, Inc.

Emeryville, CA

Last Modified: 11/14/2008

Version 7.2

Contents

Preface

Audience

This guide is meant for Administrators and IT managers who want to install and administer the BigFix Enterprise Suite (BES). It details the system requirements for each of the BES components and provides licensing and installation instructions that will enable you to deploy BigFix in your environment. It also includes information on configuring and maintaining BES. Please refer to the ***BES Console Operator's Guide*** for operating instructions and further information related to optimizing the performance of the various suite components, including BES Servers, Relays and Clients.

Conventions Used in this manual

This document makes use of the following conventions and nomenclature:

Convention	Use
Bold Sans	A bold sans-serif font is used for chapter headers.
bold text	Bold text typically refers to a program interface.
`Mono-space`	A mono-spaced font is used to indicate scripts or code snippets.
bold italics	A bold-italic font is used to indicate the titles of BigFix Guides.

Versions

The document includes the functionality introduced in the BigFix Enterprise Suite Version 7.2.

Introduction

The **BigFix Enterprise Suite (BES)** aims to solve the increasingly complex problem of keeping your critical systems updated, compatible, and free of security leaks. It uses patented Fixlet® technology to identify vulnerable computers in your enterprise and allows you to remediate them across your entire network with a few simple mouse-clicks.

Fixlet messages are highly flexible. Utilizing Fixlet technology, you can:

- Analyze the vulnerability status (patched or insecure configurations).

- Easily and automatically remediate all your networked endpoints.

- Establish and enforce configuration policies across your entire network.

- Distribute and update software packages.

- Manage your entire network system from a central Console.

- View, modify and audit properties and configurations of your networked client computers.

- Maintain a robust redundancy to minimize data loss even in severe conditions.

- Depend on encrypted communication to protect sensitive information

Fixlet technology allows you to analyze the status of configurations, vulnerabilities, and inventories across your entire enterprise and then enforce policies automatically in near real-time. With Fixlet subscriptions, the work of detecting and solving issues is done for you, allowing you to quickly authorize fixes without wasting time on the implementation details. In addition, administrators can create or customize their own Fixlet solutions and Tasks to suit their specific network needs.

BES is easy to install and has built-in public/private-key encryption technology to ensure the authenticity of Fixlet messages and actions. BES is designed to grant maximum power to you as the administrator, with a minimal impact on network traffic and computer resources. BES is capable of handling hundreds of thousands of computers in networks spanning the globe.

Once BES is installed, you will find it easy to keep your networked computers properly configured, updated, and patched, all from a central BES Console. Rolling out a package such as a software application or a patch to a large enterprise can be accomplished in minutes instead of weeks, allowing you to stay ahead of potential virus and hacker attacks. Computers that are not afflicted by a given issue are never bothered – and for those that do need updates, the users will not even know they are being updated (unless you specifically want them to know).

You will be able to track the progress of each computer as updates or configuration policies are applied, making it simple to gauge the level of compliance across your entire enterprise. In addition to downloads and security patches, you can also look directly at all your managed computers by specific attributes, allowing you to group them for action deployments, ongoing policies or asset management. You can log the results to keep an audit trail and chart your overall activity with a convenient web-based reporting program.

You can also use BigFix to gather a wealth of information about your computers such as installed applications, hardware devices, networking information, and more. If there is information specific to your deployment that you want to retrieve, you can instruct BigFix to collect that information as well.

Because BigFix lets you author your own content, you will find it to be an invaluable tool for maintaining your network, from a small installation to a large, globally dispersed enterprise.

Overview of the BES System

The BES system has the following main components:

- **BES Clients**, also called Agents, are installed on every computer you wish to manage under BigFix. They access a collection of Fixlet messages that detects security holes, improper configurations and other vulnerabilities. The BES Client is then capable of implementing corrective actions received from the BES Console through the BES Server. The BES Client is designed to run undetected by end users using a minimum of system resources. However, BigFix also allows the administrator to provide screen prompts for those actions that require user input. Starting with version 7.1, BES Clients are capable of encrypting their upstream communications, protecting sensitive information. BES Client software can run under Windows, Linux, Solaris, HPUX, AIX and Macintosh operating systems.

- **BES Servers** offer a collection of interacting services, including application services, a web server and a database server, forming the heart of the BigFix system. It coordinates the flow of information to and from individual computers and stores the results in the BigFix database. The BES Server components operate quietly in the background, without any direct intervention from the administrator. BES Servers also include a built-in **Web Reporting** module to allow authorized users to connect via a web browser to view all the information about computers, vulnerabilities, actions, and more. BigFix supports multiple servers, adding a robust redundancy to the system.

- **BES Relays** increase the efficiency of the system. Instead of forcing each networked computer to directly access the BES Server, relays spread the load. Hundreds to thousands of BES Clients can point to a single BES Relay for downloads, which in turn makes only a single request of the server. BES Relays can connect to other relays as well, further increasing efficiency. A BES Relay does not need to be a dedicated computer – the software can be installed on any Windows 2000, Windows XP, or Windows Server 2003 computer with the BES Client installed. As soon as you install a BES Relay, the BES Clients on your network have the ability to automatically discover and connect to them.

- **The BES Console** ties all these components together to provide a system-wide view of all the computers on your network, along with their vulnerabilities and suggested remedies. The BES Console allows an authorized user to quickly and simply distribute fixes to each computer that needs them without impacting any other networked computers. The BES Console can be run on any Windows 2000, Windows XP, or Windows Server 2003 computer that has network access to the BES Server. BES Consoles for large deployments are often hosted from Terminal Servers or Citrix Servers.

Using this Guide

The process of getting BigFix up and running varies, depending on your network environment and your security policies. This guide focuses on a standard BigFix deployment, which applies to workgroups and to enterprises within a single administrative domain. For the sake of readability and generality, this guide assumes these restrictions:

- The BES Servers are able to make connections to the Internet on port 80. The BES Server can be set up to use a proxy, which is a common configuration. Alternatively, an air-gap can be used to physically separate the BES Server from the Internet Fixlet Server (for more information, visit http://support.bigfix.com/bes/install).

- Each BES Server must have access to a SQL server, located locally on the BES Server machine or remotely on a separate SQL Server.

- Each BES Console operator can make an ODBC connection to the database and an HTTP connection to the BES Server.

- Each BES Client computer in the network must be able to make an HTTP connection to a BES Server or a BES Relay on the specified port (the default port is 52311 but any available port will serve).

Some enterprises will violate one or more of these conditions, but BigFix can still be deployed in these environments – the section titled **Deployment Scenarios** (page 80) shows you how. If your network configuration does not match any of the scenarios in that chapter, talk to a BigFix support technician for more options.

The initial deployment of a minimal BigFix system (BES Server, BES Console, and a few BES Clients) should take roughly an hour to complete.

If you are installing the BigFix evaluation version, be sure to read the *BES Evaluation Guide*. When you are ready to install the full system, you will want to pay extra attention to the sections in this document on BES Client and BES Relay deployment, to ensure an efficient rollout.

Several steps in the BigFix installation depend on the completion of prior steps. For this reason, it is recommended that you follow this guide in the order presented.

BES Operating Requirements

BigFix has been designed to run efficiently using minimal server, network and client resources. The requirements for the BES Client programs are not stringent. The hardware required by the BES Server and the BES Console will depend on the number of computers that are administered and the total number of BES Consoles. The distributed architecture of BigFix allows a single BES Server to support hundreds of thousands of computers.

BES Server Requirements

The BES Servers must be Windows 2000 or Windows Server 2003 computers. 64-Bit versions of Windows 2000 and Windows 2003 are supported for BES 6.0 and above.

A 2-3 GHz CPU with 1 GB RAM is sufficient for a couple of hundred BES Clients, but the requirements scale with the number of computers. To support 200,000 computers, you would likely need 8 cores and 16 GB RAM.

A minimum of 5 GB free disk space is needed by the database, data files, and the file caches to run BigFix. However, an additional 20-50 GB of disk space can be useful for database backups and further growth. To support more than a couple hundred BES Clients, you will need RAID Arrays. For 200,000 computers, you will need about 3 Arrays (RAID 10). For optimal performance, the disk cache should be set to 50/50 read/write.

The exact hardware requirements for the BES Servers will vary depending on how many BES Clients are attached. The latest references can be found at: http://support.bigfix.com/cgi. Consult with your support technician for more information about the BES Server requirements.

The following network configuration is recommended for security and performance reasons:

- All internal network communication will be on one specified port (52311 is the default) to allow for simplicity and flexibility of deployment. TCP/IP and UDP on this port must be completely unblocked at all internal routers and internal firewalls (you can optionally disable UDP but that may negatively affect performance).

- The BES Server should connect to the network at 100 mbps or higher.

- The BES Consoles must be able to make connection to the SQL Server 2000 or 2005 database using ODBC. SQL Server 2005 (32-Bit and 64-Bit) is supported for BES 6.0 and above. BES Consoles should have high speed connections to the BES Server (100 mbps or higher)

- The Windows Firewall must be turned off on the BES Server machine.

- The BES Client must be installed on the BES Server machine.

These networking recommendations are typically easy to satisfy for most organizations maintaining a moderate security posture. If these requirements cannot be met in your organization, see **Configuring the BES Components** (page 49). For information on larger installations, see **Deployment Scenarios** (page 80).

The BES Server requirements and performance may also be affected by other factors in addition to the number of BES Clients. These include:

- **The number of BES Console Operators.** Multiple BES Console operators can connect to the BES Server(s) at the same time to manage subsets of the networked computers – some deployments may have hundreds of operators. If you plan on having more than 30 operators, you may want to have a more powerful BES Server to support the additional load.

- **BES Relays.** BES Relays should be used to lighten the load on the BES Server(s) by accepting connections from BES Clients and then forwarding the data to a BES Server. In most deployments, very few BES Clients report directly to the main BES Server.

- **The number and type of Retrieved Properties and Analyses.** Custom Retrieved Properties and Analyses can provide extremely useful data. But if custom properties are poorly implemented or overused, they can also create undue load on the system by requiring too much bandwidth or too many BES Client resources. For instance, it would be unwise to create a custom retrieved property that returned the names of every file on every computer, due to the load on the client computers and the network.

For more information about these performance issues, please view http://support.bigfix.com/cgi or contact your BigFix support technician.

BES Console Requirements

To install the BES Console, you must have a computer that meets the following minimum requirements:

- **Hardware:** Intel Pentium III–class processor with 512 MB RAM. Larger deployments will require more capable computers.
- **Software:** Windows 2000, XP, 2003 or Vista with Internet Explorer version 5.0 or better.

The BES Console can be installed on a laptop or any moderately powerful computer. However, as the number of computers that you are managing with the BES Console grows, you may need a more powerful computer. The latest BES Console recommendations can be found at: http://support.bigfix.com/cgi.

The BES Console also requires a high bandwidth connection (LAN speeds work best) to the BES Server due to the amount of data that needs to be transferred to the BES Console. If you need to remotely connect to the BES Server across a slow bandwidth connection, it is recommended that you use a remote control connection to a computer (such as a Citrix server or Terminal Services computer) with a high-speed connection to the BES Server.

Contact your support technician for more information about BES Console scaling requirements.

NOTE: The BES Console is the primary interface to BigFix and manages a great deal of information about the BES Clients. If the BES Console computers are underpowered or on a slow connection, it can adversely impact performance.

BES Client Requirements

The BES Client can run on computers that meet the following minimum requirements:

- **Hardware:** x86-based computers, Mac or SPARC with 32 MB RAM and 20 MB free hard disk space. Extra temporary disk space may be required for some patches.

- **Software:** Windows 95, 98, NT 4+, Me, 2000, Server 2003, XP, Vista, Longhorn, Red Hat Linux 8.0, & 9.0, Red Hat Linux Enterprise 3.0 & 4.0, Red Hat Fedora Core 3.0, 4.0 & 5.0, Solaris 7, 8, 9 & 10, HPUX 11.00 & 11.11, AIX 5.1, 5.2 & 5.3, SUSE 8, 9 & 10, Mac OS X 10.3 & 10.4.

New versions of the BES Client are always in development so please check with your support technician for more details. For Windows platforms, IE 5 or greater must be installed.

You can find the latest BES Clients at http://support.bigfix.com/cgi.

Database Requirements

BigFix requires SQL Server 2000/2005 or Microsoft Data Engine (MSDE) 2000/2005, which will store all of the data retrieved from the BES Clients.

MSDE 2000 is the free version of SQL Server 2000 and although it is sufficient for some BigFix installations (especially evaluation installations), it is not recommended for production deployments. MSDE 2000 is included with the BES Server and you will be prompted to install it if a supported database is not already installed. However, MSDE comes with some restrictions set by Microsoft, including a limit on the number of simultaneous database connections you can establish before performance degrades. Since some of these connections are used by BES Server components, it is recommended that you install the commercial version SQL Server if you expect to have more than one operator at a time using a BES Console. Also, SQL Server comes with Client Tools that allow easy administration of database activities such as backups and other maintenance activities.

Security Requirements

The BigFix system authenticates all Fixlet messages and actions using secure public-key infrastructure (PKI) signatures. PKI uses public/private key pairs to ensure authenticity.

Before you can install BigFix, you must use the BES Installer to generate your own **private key** and then apply to BigFix for a signed certificate containing your **public key**. Your private key (which only exists on your computer and is unknown to anyone else, including BigFix) is encrypted by a password of your choosing, so if someone steals it, they still need to know your password in order to use it. Nevertheless, you should guard it well. *Anyone who has the private key and password for your site, access to the server and a database login will be able to apply any action to your BES Client computers.*

Treat your private key just like the physical key to your company's front door. Do not leave it lying around on a shared disk. Instead, store it on a removable disk or a secured location – and *do not lose it*. In the physical world, if you lose your master key you have to change all the locks in the building. Similarly, if you lose your digital key, you will need to do a migration to a new authorization key or a fresh install of the entire system (including all the BES Clients). It is not unreasonable to store a backup copy of your site level key files in a secured safe deposit box.

As the BigFix Site Administrator, you will authorize trusted people within your enterprise to deploy, or publish, remedial Fixlet actions across the network. These BES Console operators will have publishing rights, and they must sign all the actions they publish with their own private key. Like the BigFix Site Administrator, they have a password to encrypt their private key. Both the password and the key should be carefully guarded for each authorized operator.

Whenever operators issue an action, it must be signed by their private publisher key. Then when the BES Client receives the action, it validates the signature using the public key information. If the signature validation fails on the BES Client, the operator's action is discarded. This prevents unauthorized personnel from using the BES Console to propagate actions.

Fixlet messages are also digitally signed. The Fixlet site author signs each message with a key that can be traced back to the BigFix root for authentication. This signature must match the Fixlet site's masthead, which is placed in the BES Client install folder upon subscribing to the site. This procedure prevents spoofing and man-in-the-middle attacks, and guarantees that the Fixlet messages you receive are from the original certified author.

There are a few other security-related issues to address before installing BigFix in your organization:

- Make sure the BES Server computer is running Windows 2000 or Windows Server 2003 with the latest Service Pack available from Microsoft.

- Make sure that SQL Server/MSDE is secured with the latest security-related patches from Microsoft.

- Verify that your network firewall forbids inbound and outbound traffic on the specified port (default 52311) so that BigFix-related traffic will not be able to flow into or out of your network.
  It is possible to administer roaming laptops by opening this port on your firewall. However, a better technique is to use SSH tunnels to route the relay through a non-default port and avoid opening this port altogether.

- Make sure that TCP/IP and UDP on the specified port (default 52311) is completely unblocked at all internal routers and internal firewalls.

- Verify with your network administrator that you can allow the BES Server to access the Internet via port **80**. The BigFix Gather service is the only component of the BES Server that accesses the Internet and by default it runs as the Windows SYSTEM account. If the SYSTEM account cannot reach the Internet because of proxy or firewall restrictions, then you will need to set the BigFix Gather service to logon as a user with Internet and administrative access on the BES Server computer. Detailed instructions on how to do this are in the knowledge base available at http://support.bigfix.com/.

  It is also possible to maintain a physical disconnect from the Internet with an air-gapped implementation. For more information, see http://support.bigfix.com/bes/install.

- You should secure the BES Server computers and the database (SQL Server or MSDE) using company or industry-wide standards. Contact your network administrator or database administrator for more information.

NOTE: Certain rare lockdown procedures may cause the BES Servers to function improperly. Contact your support technician if you have any specific questions about lockdown procedures.

A Basic Installation

A simplified BigFix deployment resembles the diagram below. There is at least one BES Server that gathers Fixlet messages from the Internet where they can be viewed by the BES Console operator and distributed to the BES Relays. Each BES Client inspects its local computer environment and reports any relevant Fixlet messages back to the BES Relay, which compresses the data and passes it back up to the server(s).
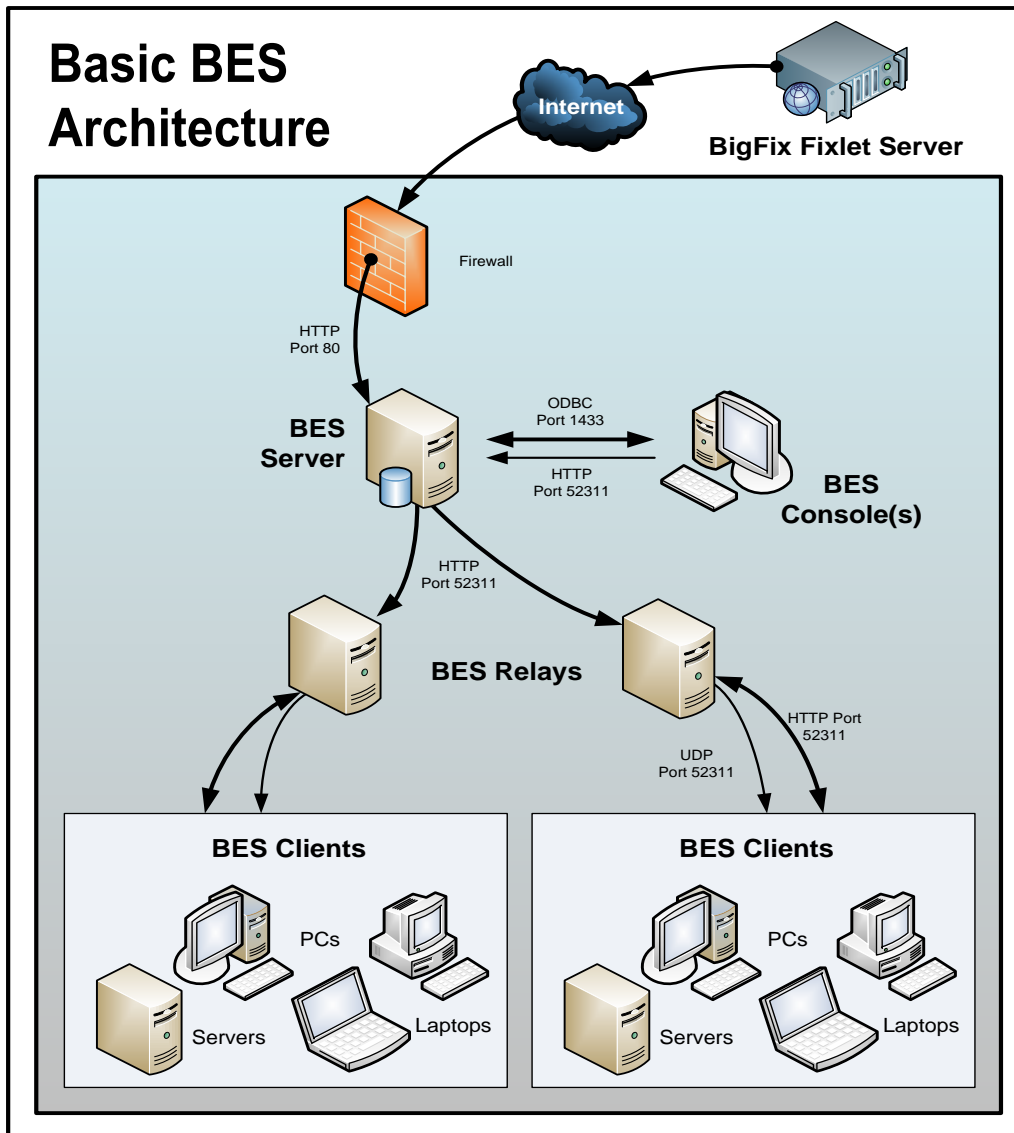
The BES Consoles oversee all this activity. They connect to the BES Server(s) and periodically update their displays to reflect changes or new knowledge about your network. The BES Console operator can then target actions to the appropriate computers to fix vulnerabilities, apply configuration policies, deploy software, etc. The progress of the actions can be followed in near real-time as they spread to all the relevant computers and, one by one, address these critical issues.

This diagram labels all the default ports used by BigFix, so you can see which ports need to be open and where. These ports were selected to avoid conflict, but if you are currently using any of these ports, they can be customized upon installation.

NOTE: The arrows in the diagram are intended to illustrate the flow of information throughout the enterprise. The arrows from the Fixlet Server to the BES Server(s) represent the flow of Fixlet messages into your network. This data transfer is strictly one-way; information never leaves your network. BES Clients gather Fixlet messages and action information from BES Relays. They then send small amounts of information back to the BES Server(s) through the BES Relays. The UDP packets from the BES Relay to the BES Clients are small packets sent to each BES Client to inform them that there is new information to be gathered. The UDP messages are not strictly necessary for BigFix to work properly. Please view http://support.bigfix.com/cgi or ask your support technician for more details.

BigFix Message Level Encryption (MLE) Overview

BES has added Message Level Encryption (MLE) to its 7.1 platform release. With MLE, your BES Clients can encrypt upstream data using a combination of an RSA public/private key-pair and an AES session key.

The RSA key-pair can be of 1024, 2048, or 4096-bit key length, with longer keys offering additional security but requiring more processing power for decryption at the server. The AES session key uses the maximum FIPS-recommended length of 256 bits. You can configure your BES relays to reduce the load on the BES Server by decrypting and repackaging the Client data before relaying it.

The RSA public key encrypts the session key and adds it to the AES-encrypted report. At the BigFix Server (or a decrypting BigFix Relay) the corresponding RSA private key is used to decrypt the AES session key which is then used to decrypt the BES Client report.

There are three levels of report encryption:

- **Required:** Clients require encryption of reports and uploads. The client will not report or upload files if it cannot find an encryption certificate or if its parent relay does not support receipt of encrypted documents.
- **Optional:** Clients prefer, but do not require encryption of reports and uploads. If encryption cannot be performed, reports and uploads are done in clear-text.
- **None:** Clients do not encrypt, even if an encryption certificate is present.

A Typical Installation

Although the basic installation discussed above shows many of the specific ports needed to establish the BigFix network, it does not illustrate two important aspects of many BigFix deployments: a DMZ and direct connections. In the DMZ example, an office connected by a VPN can share the content from a BES Relay or Server. In the direct connection, home PCs and laptops can connect directly to the Internet for content from BigFix Fixlet servers through their own private firewalls. For the sake of clarity, these extra connections may not be shown in all diagrams, but they are generally present in most deployments. Here is a typical installation.
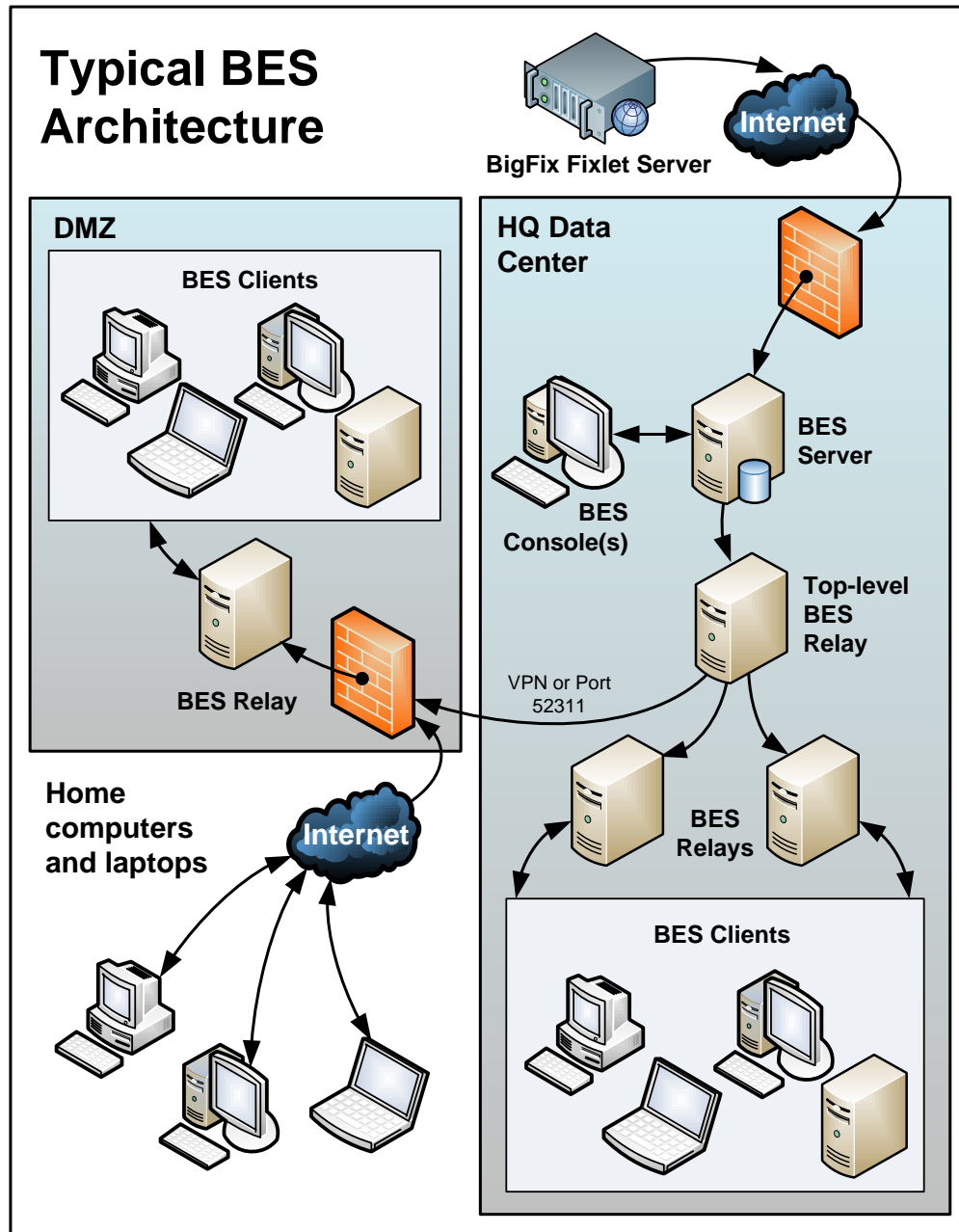
A Multiple Server Installation

BES Version 7.0 introduced the important ability to add multiple, fully redundant BES Servers, called Distributed Server Architecture (DSA). Each Server maintains a replica of the BigFix database and can be positioned anywhere in the world. In the case of a network fracture, these Servers continue to provide uninterrupted service to the local network. As soon as the connection is re-established, the Servers automatically reconnect and sync up. The BES Relays and Clients (version 7.0 and later) are also capable of gracefully recovering from such a disconnect. DSA provides the following capabilities:

- Continued service availability on both sides of a network split (automatic failover).

- Continued availability in the event of a server outage.

- Distribution of Console database load during normal operation.

- Automatic failback upon reconnection.

To take advantage of this functionality, you will need one or more additional servers with a capability at least equal to your primary server.

All BigFix servers in your deployment must run the same version of SQL Server. If your existing BES Server is running SQL 2000, your new servers must run SQL 2000 as well. If your version of SQL was put there as the BigFix Installer default, it is the desktop edition (MSDE) of SQL 2000.

Understanding Replication

Additional servers help to distribute the work load and create a redundant system that is hardened to outages. Knowing how it accomplishes this can help you to create the most efficient deployment for your particular network. Here are some of the important elements of multi-server installations:

- Servers communicate on a regular schedule to replicate their data. You review the current status and adjust the replication interval through **BES Administration > Replication**.

- When each server goes to replicate from the other servers in the deployment, it calculates the shortest path to every other server in the deployment. Primary links are assigned a length of 1, secondary links 100, and tertiary links 10,000. Links which resulted in a connection failure the last time they were used are considered to be non-connected.

- When an outage or other problem causes a network split, it is possible to for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected, precedence will go to the version on the server with the lowest BES Server ID.

- If multiple copies of **Web Reports** are installed, they will operate independently. Each Web Report Server can connect to the BES Server that is most convenient, since they all contain an equivalent view of the database.

- By default, server 0 (zero) is the master server. **BES Administration** will only allow you to perform certain administrative tasks (such as creating and deleting users) when connected to the master server.

- If you want to switch the master to another server, you can do so with a setting. For more information, see **Managing Replication** on page 59.

Distributed Server Architecture (DSA)

The following is a diagram of a typical DSA setup with two servers. Each BES Server is behind a firewall, possibly in a separate office, although it is easy to set up multiple servers in a single office as well. It is important that the BES Servers have high-speed connections to replicate the BigFix data (generally LAN speeds of 10-100MBPS are required). The BES Servers will communicate over ODBC and HTTP protocols. This DSA configuration provides automatic failover and failback services, minimizing loss of data.
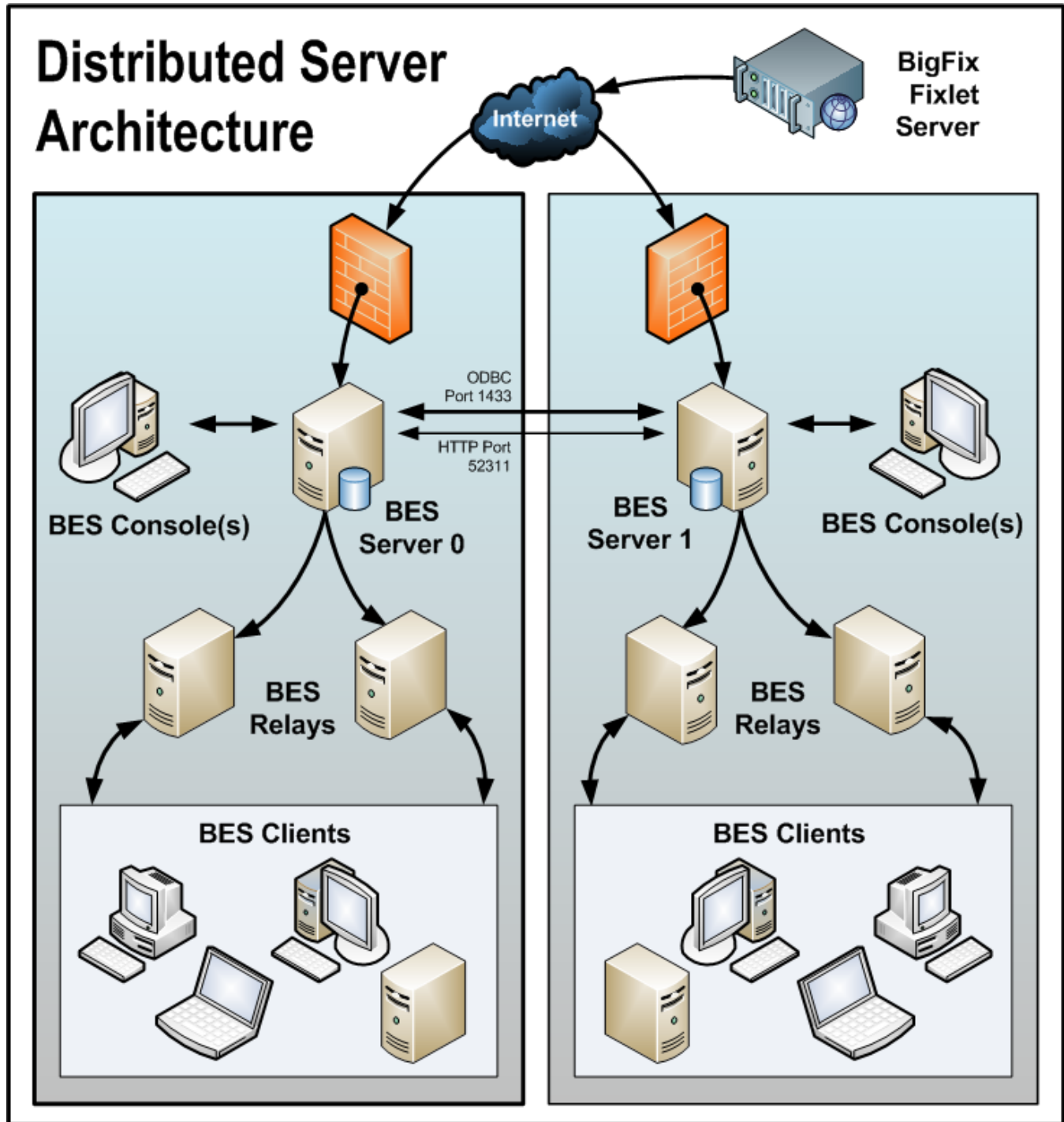
Automating Failover and Failback

If a BES Server goes down, whether due to disaster or planned maintenance, the DSA deployment reconfigures itself (hot failover) as the orphaned BES Relays find a new server connection. When the disabled server comes back online, its data will automatically be merged with the data on the healthy server.
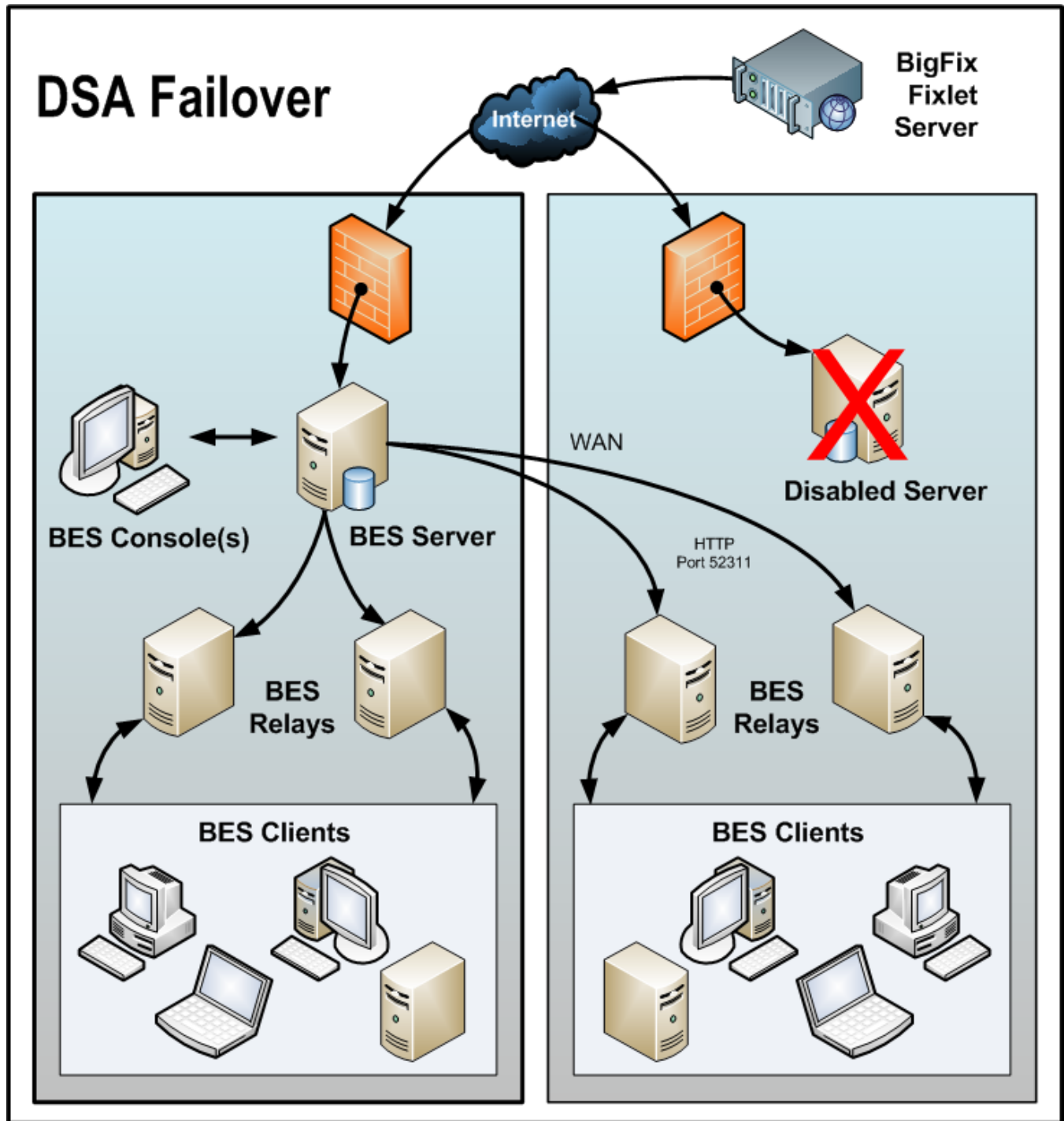
Getting Started

Administrative Roles

To install and maintain BigFix typically requires the cooperation of several administrators and operators:

- **The Network Administrator.** This person will need to allow the BES Server to connect to the Internet through the existing proxy server (if applicable) as well as resolve any network-specific issues that may prevent BigFix from working properly. The network administrator will also provide information about WAN link connection speeds and subnet addresses if necessary. When starting a deployment of BigFix, it is best to make the Network Administrator aware of how BigFix uses the network by reviewing this page: http://support.bigfix.com/cgi

- **The Database Administrator.** This person will be responsible for setting up and maintaining the SQL Server 2000 or MSDE 2000 database for the BES Server. Note that if you perform a local database installation and no SQL server is found, MSDE 2000 will automatically be installed and set up. No extra database administration is required unless SQL Server 2000 is installed or there are other policies regarding databases that need to be enforced (i.e., backups, password changes, etc.).

- **The BigFix Site Administrator.** This person will install and maintain the BigFix software, including the BES Server, BES Console, and the BES Client programs. The Site Administrator will also be responsible for creating, distributing, and revoking publisher keys and management rights that allow BES Console operators to deploy actions. The Site Administrator is the only person in an organization who can authorize new BES Console Operators or Master Operators (see below). A Site Administrator holds this position by virtue of having administrative access to the BES Server computer as well as access and the password to the site-level signing keys.

- **BES Console Master Operators.** These people are operators with access to all the BigFix computers with the added authority to assign management rights to other BES Console operators. Master Operators can do most of what you can do as the Site Administrator. In fact, Master Operators are often referred to as administrators. However, only the BigFix Site Administrator can create new operators and a Master Operator can only create custom content with permission from the Site Administrator.

- **BES Console Operators.** These people will manage the day-to-day operation of BigFix, including Fixlet management and action deployment, typically on a subset of computers subject to the management rights assigned by a BigFix Site Administrator or Master Operator.

Often these administrative roles will overlap and one person may be assigned multiple duties. The network and database duties are limited to minimal setup procedures, which are covered in this document. The BES Console Operators (including Master Operators) should read the separate *BES Console Operator's Guide*.

Duties of the BigFix Site Administrator

This BigFix Site Administrator has the following primary responsibilities:

- **Obtaining and securing the Action Site Credentials.** In order to install BigFix, the BigFix administrator needs to generate a private key, receive a license certificate from BigFix, and create a masthead with the digital signature and configuration information.

- **Certifying Users.** The BigFix Site Administrator must create an account and private key files for each operator. Use unique values – it is not wise to use your site-level password for any of these keys, because it could lead to signature errors.

- **Preparing the BES Server.** The BES Server must be properly set up to communicate externally with the Internet and internally with the BES Clients. The BES Server also needs to be configured to host the BigFix database (or another computer can be used as the SQL Server database).

- **Installing the various BigFix Components.** The BigFix Site Administrator will install the BES Client, Server, Relay and Console modules.

- **Assigning Management Rights.** BigFix Master Operators can assign management rights to the BES Console operators. These rights constrain operators to specific computers. You can also grant or revoke the right to make custom content or to view unmanaged assets.

- **Maintaining the BES Server**. The BES Server runs a database (SQL Server or MSDE) and many BigFix specific services. Standard maintenance tasks like upgrades or fixes will be managed using Fixlet technology or may be performed manually by the BigFix Site Administrator.

- **Maintaining security**. The BigFix system is protected by password-encrypted private keys. The BigFix Site Administrator controls access to these and can create new private publisher keys or revoke them as the need arises. BigFix authentication uses public key infrastructure (PKI) technology with key lengths of up to 4096 bits.

Each of these administrative duties is described fully in the following sections of this guide.

Getting Authorized

Because BigFix is powerful, you will want to limit access to trusted, authorized personnel only. BigFix operates from a central repository of Fixlet actions called the **Action site**, which uses public/private key encryption to protect against spoofing and other unauthorized usage. To get started, you need authorization from BigFix, Inc.

If you have not yet purchased a license to use BigFix, please contact sales@bigfix.com or visit the BigFix Website at http://www.bigfix.com. The sales agent will want to know how many BES Clients you intend to install. Based on this, the agent will create, sign and email you a **BES License Authorization** file which will have a name like "CompanyName.BESLicenseAuthorization". Save this file in a safe place, typically in your Documents folder or a PGPDisk on a USB key. For security reasons, we recommend that you *not* store it on the BES Server itself.

The Installer program will collect further information about your deployment and then create a file called the **action site masthead**. This file establishes a chain of authority from the BigFix root all the way down to the BES Console operators in your organization. The masthead combines configuration information (IP addresses, ports, etc.) and license information (how many BES Clients are authorized and for how long) along with a public key used to verify the digital signatures. To create and maintain the digital signature keys and masthead, you will use the **BES Installer**, which you can download from BigFix, Inc.

NOTE: If you are using an evaluation version of BigFix, you may skip the following section. During installation, the **BES Evaluation Generator** will create your signing keys through an expedited process, and the generation of separate publisher keys will not be necessary.

Creating the Action Site Masthead

Before you perform the steps below, you must have purchased a license and received a BES License Authorization File (see previous section).

Once you have your license authorization file, you are ready to create a personalized **action site masthead** that will, in turn, allow you to install and use BigFix. The masthead includes URLs for the BES Server CGI programs and other site information in a signed MIME file. The masthead is central to accessing and authenticating your action site. To create the masthead and activate your site, follow these steps:

1. Run the BES Installer that you downloaded from the BigFix site (www.BigFix.com). At the welcome screen, click **Next**.

2. You will see a dialog offering to install the Evaluation or Production version of BES. Select **Production** and click **Next**.

3. After reading the License Agreement, click **Yes** to accept it and continue. The **Setup Type** dialog appears:
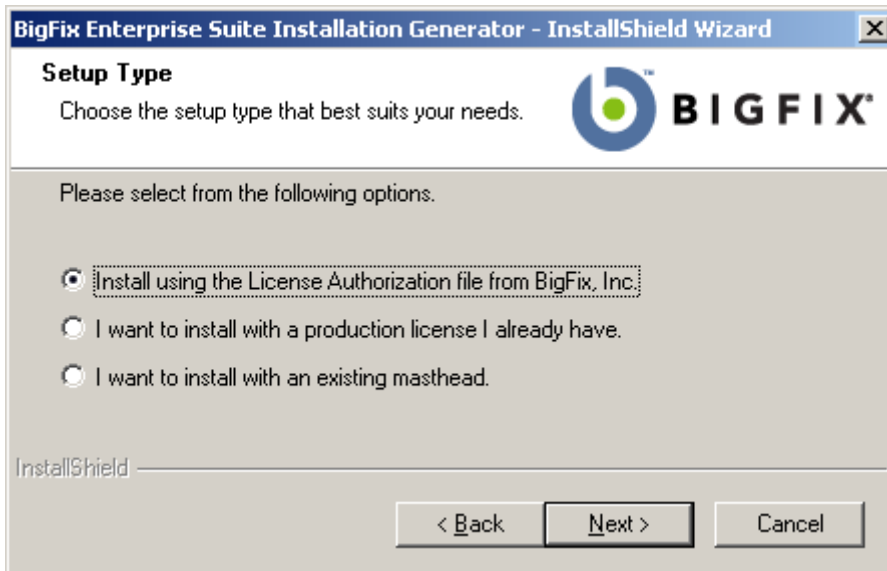
Select the choice to **install using the License Authorization file from BigFix, Inc.**, then click **Next**.

4. The BigFix Action Site Masthead Creation Wizard launches. It asks you for the location of your license authorization file. Click the **Browse** button to bring up a standard Windows open-file dialog. Navigate to your license authorization file, which has a name like CompanyName.BESLicenseAuthorization. Select the file and click **Open.**

5. A dialog appears displaying the current contents of your license authorization:
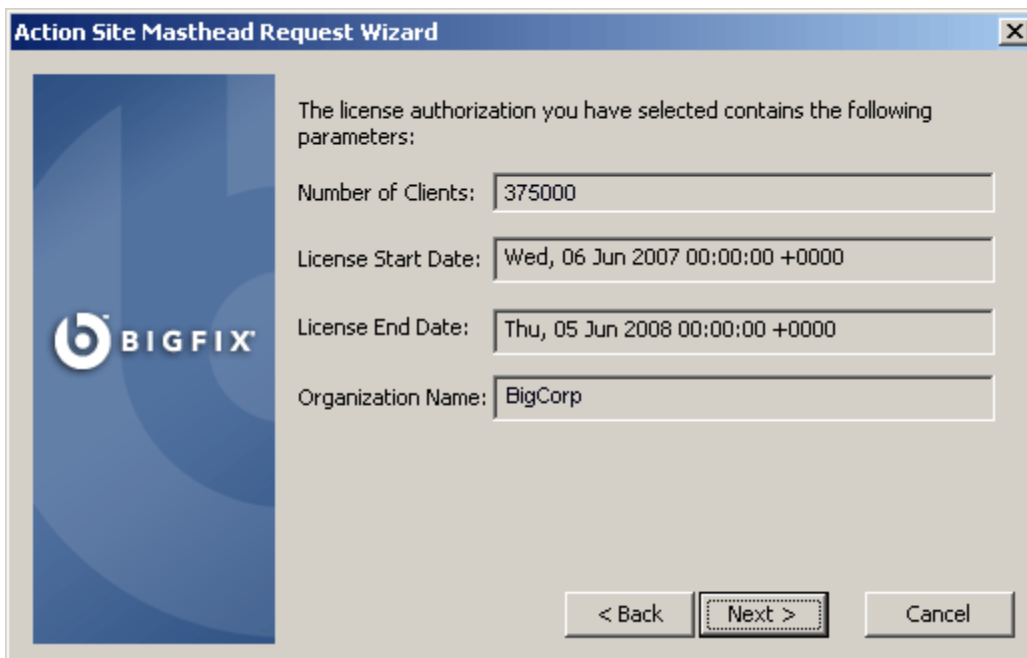
Click **Next**.

6.   The next screen in the Wizard prompts you for the **DNS name** or **IP address** of your BES Server. Type this in and click **Next**.

> NOTE: The DNS/IP address that you choose becomes a permanent part of your deployment and must never change.

7.   The next screen in the Wizard prompts you for a site-level **password** so you can create a site admin key for your deployment. Type in your password twice (for verification), and specify a key size (from 1K- to 4K-bits) for the public/private key pair. Click **Next**.

8.   From the **Save As** dialog, find a folder to save your private key file (license.pvk) to a secure location, such as a PGPDisk on a USB drive. Click **Save**.

9.   The next screen in the Wizard prompts you to submit your masthead request to BigFix. This request consists of your original authorization, your server DNS name and your public key, all packaged into a single file. Typically, you will select the first choice, **submit request**, to post the request via the Internet. Click **Next**. The Wizard will then retrieve your certificate (license.crt) from the BigFix License Server.

      (Alternatively, the Wizard will let you save the request as a file named request.BESLicenseRequest. Then you can visit the BigFix website, post your request and download your certificate.)

10.   Upon a successful request submission, the Wizard retrieves your license (license.crt) and prompts you to save it. Click **Save**. This action completes the Wizard, returning you to the **Setup Type** dialog. You are now ready to install the programs with your new production license.

Keep in mind that the private key (license.pvk) to your action site authorizes you, as the BigFix Site Administrator, to create BES Console operators with publisher credentials. This key is *not* sent to BigFix during the creation process, and should be carefully protected. For the highest level of security, it is recommended that you save the BigFix Credentials to an encrypted disk, such as a PGPDisk on a USB key or other removable media..

> **Warning!** If you lose your site credential files or password, then no one – not even BigFix – can recover your keys or your password. You will need to reinstall the entire system, including all the BES Clients, with a freshly generated key.
>
> If the main BES Server is lost, you may also lose your encryption key file. For disaster recovery you have two options: you can back up your encryption key now, so you can restore it after recreating the BES Server, or you can generate a new encryption key after recreating the BES Server.

Installing the Programs

Once you have your license and/or your action site masthead, you are ready to install the programs. Here is how:

1.   If the installer is not already running, launch it. From the **Setup Type** dialog, select the second choice to **install with a production license**. Click **Next**.

2.   Browse to the location of your license key and click **Open**.

3.   A dialog appears, prompting you for your private **site signing key** (license.pvk). This is typically stored in the same folder as the license.crt file. Browse to it and click **Open**.

4. A dialog prompts you for the **Site Admin Private Key Password**. Enter the password you selected to protect your private key (see the previous section) and click **OK**.

5. The program prompts for a server port number that BigFix will use for all its data transmissions. The default port is **52311**.
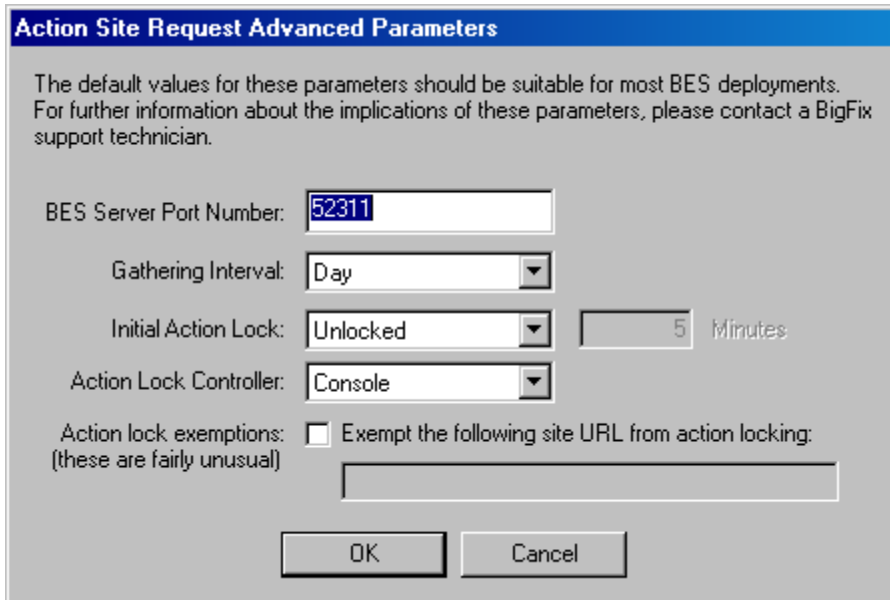
This is the recommended port number, but you may choose a different port if that is more convenient for your particular network. Typically, you would choose a port from the IANA range of private ports (49152 through 65535). You could use a reserved port number (ports 1-1024), but it is not considered best practice because it inhibits the ability to monitor or restrict traffic properly and it defeats the idea of port numbers for specific applications. The lock options in this dialog typically do not need to be changed unless you want a computer to automatically be locked after installation. Click **OK**.

You should accept the default settings on this page unless you have a specific reason to change them. Improper settings can cause BES to work in a sub-optimal fashion. Consult with a support technician for more details.

6. A standard Windows **Save As** dialog prompts you to save the **Masthead**. This is a public file that does not require protection. Navigate to the desired folder, name the file (e.g. actionsite.afxm), and click **Save**.

7. You are now ready to generate the **BigFix Enterprise Suite installation components**. Select the default directory (BESInstallers) or click **Browse** to choose a different folder. Click **Next**.

8. The Install Wizard will then generate and save various BigFix installation components. After saving the files, a dialog appears confirming the installation and reminding you of their location. Click **Finish** to exit and start the **BES Installation Guide**.

Installing the BigFix Components

Running the BES Installers

So far, you have created a private key, requested and received a certificate, used the certificate to create a masthead and then generated the various BigFix installation components, including the **BES Installation Guide**. When the components have been saved, the **BES Installation Guide** automatically launches. You may also run it at any time by selecting it from the Start Menu.

To install the three major components of BigFix (BES Server, Console, and Client), follow these steps:

1. If it is not already running, launch the BES Installation Guide (**Start > Programs > BigFix Enterprise > BES Installation Guide**).
2. Select the button labeled **Install BES Components**.
3. A dialog box appears, prompting you to select a BigFix component to install. Click the buttons on the left, in order from top to bottom, to install the BigFix components. The component installers include:

    - **Install BES Server**
    - **Install BES Console**
    - **Install BES Clients**
    - **Browse Install Folders**
4. The BES Server, Console and Clients all have their own installers. Follow the instructions for each, as described in the following sections.

Installing the Primary BES Server

The BES Server is the heart of the BigFix System. It runs on a server-class computer on your network that should have direct Internet access as well as direct access to all the BES Client computers in your network. Make sure your server meets the requirements outlined in the **BES Server Requirements** section (page 5). Also, you can consult the knowledge-base article at http://support.bigfix.com/bes/install/serverreq71.html.

To install the BES Server, follow these steps:
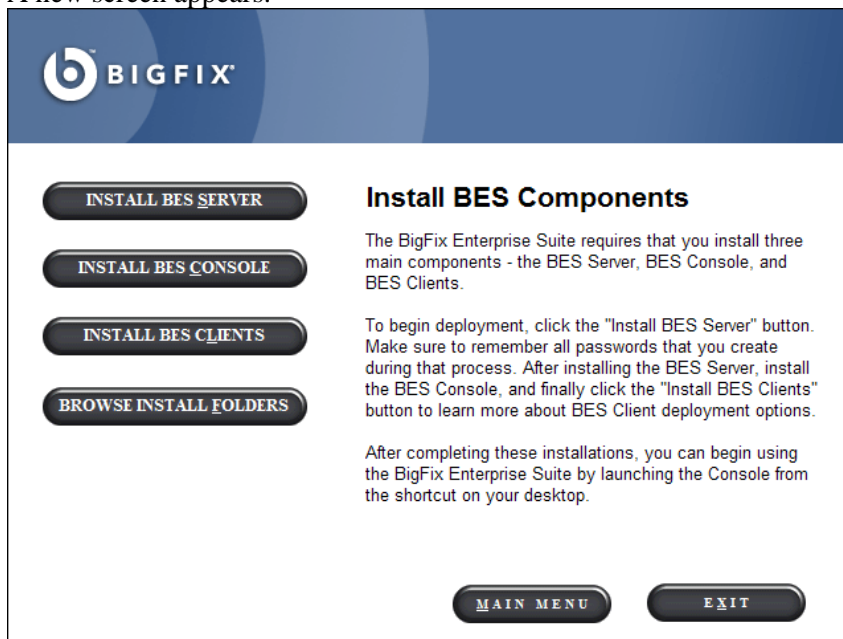
1. If you have not already done so, run the BES Installation Guide (**Start > Programs > BigFix Enterprise > BES Installation Guide**). Click the button labeled **Install BES Components**.

2. A new screen appears.

Click the top button labeled **Install BES Server.** The BES Server Install Wizard presents a welcome screen. Click **Next** to continue.

3. After reading the **License Agreement**, click **Yes** to accept it and continue.

4. A dialog prompts you to choose a **Master** or **Replicated** database. Click the first button to create a Master database for later replication – or if you only need a **Single** database in your deployment. Click the second button to create a Replica of an existing Master. If this is your initial installation, click the top button.

5. A dialog prompts you to select a **Local** or **Remote** database. If you want to use another computer to host the BigFix Database, it must have a SQL Server already installed. The most common choice is to use the local database. If the program cannot detect a database server, the program will install MSDE 2000 SP4 in the directory you specify.

6. A dialog displays a list of the BES Server components about to be installed.
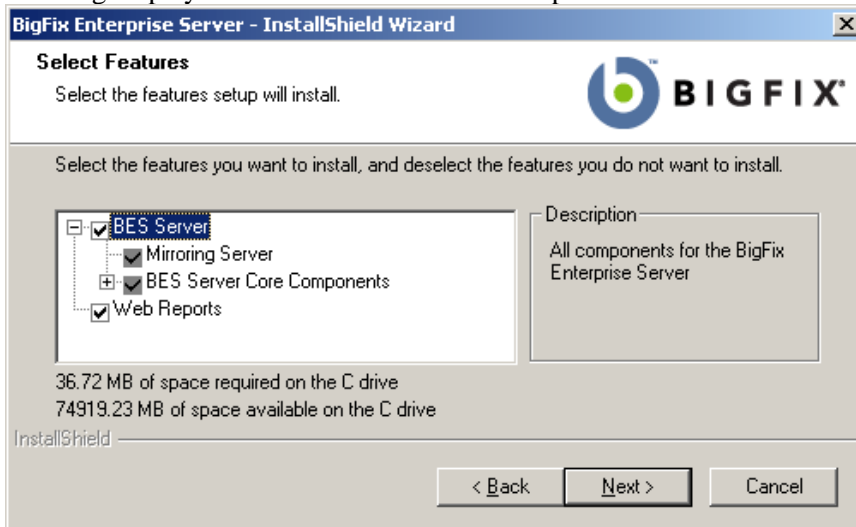
In general, you should accept the default components and click **Next**.

7. The installer prompts you for the desired destination of the BES Server components. The default location is **C:\Program Files\BigFix Enterprise\BES Server**, but you can specify a different location by clicking the **Browse** button. Once you have decided on the destination, click **Next**.

8. The Server Properties dialog prompts you to enter a location for the BES Server web root folder (if different from the default). This is where downloaded files for the BES Clients will be stored. The default URL is also available for editing, should you wish to change it.
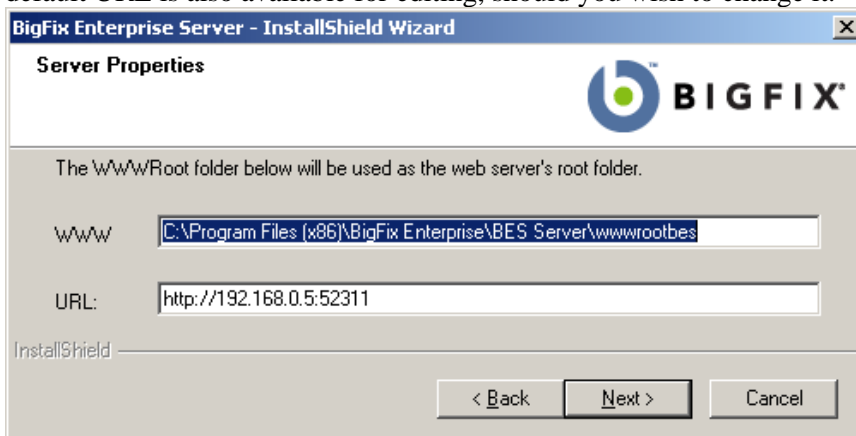
NOTE: No other application should be listening on the BES port or errors will occur.

9.   Next a dialog prompts you for a location and port number for BES Web Reports. By default, it will use
      port 52312.
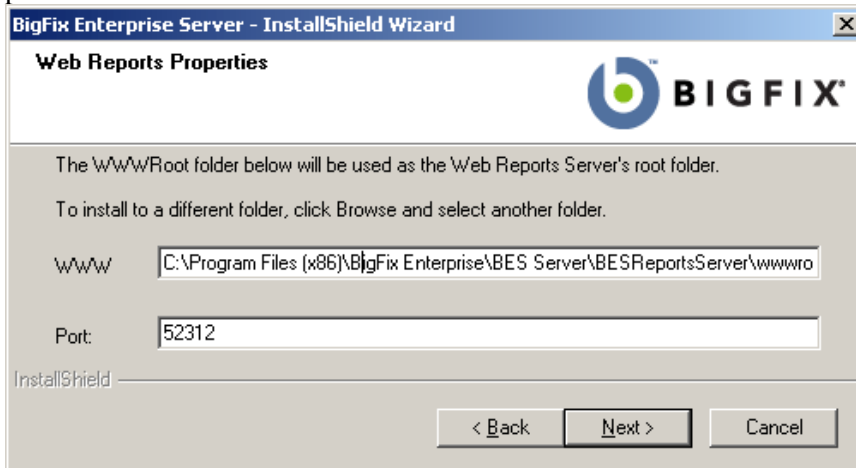
10.   The BES Server installer then presents a window displaying the selected inventory of server
      components to be installed as well as some other installation programs to run.
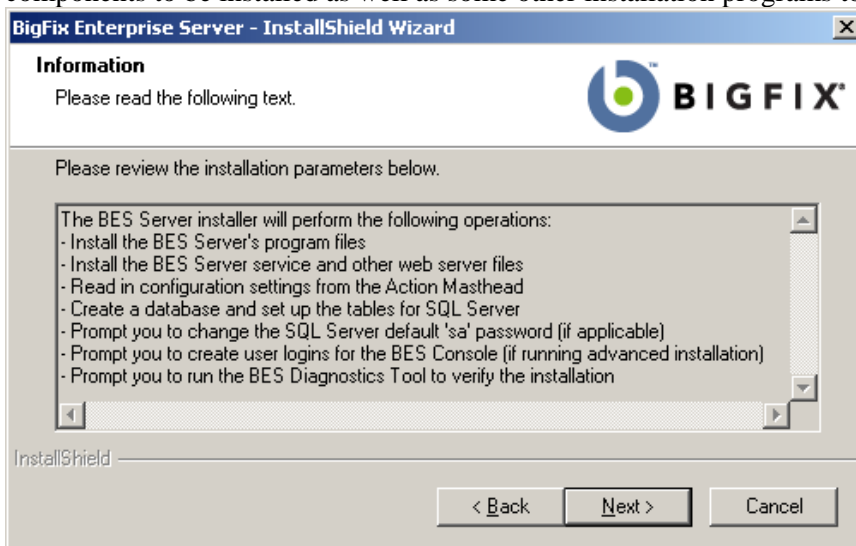
      Click **Next** to continue the installation.

11.   When the files have been properly installed, the program prompts you for specific information,
      depending on your installation parameters. The program will ask you to set a default 'sa' password if the
      'sa' password for the SQL Server or MSDE database is currently blank (this is done for security
      reasons).

12.   The program then prompts you to locate the **Action Site Masthead**. Click **OK** to continue. At the
      Windows Open dialog, navigate to the folder where you stored your masthead, select it and click **Open**.

13.   The program may prompt you for the location of your **license certificate**. Click **OK** to continue. At the
      Windows Open dialog, navigate to the folder where you stored your license (license.crt), select it and
      click **Open**.

14.   Next, the program may prompt you for the location of your private key (license.pvk). Accept the default
      path (if specified) or click the **Browse** button to find a different location. Finally, enter your password to
      initialize the database.

15.   The program then prompts you to create an administrative user.
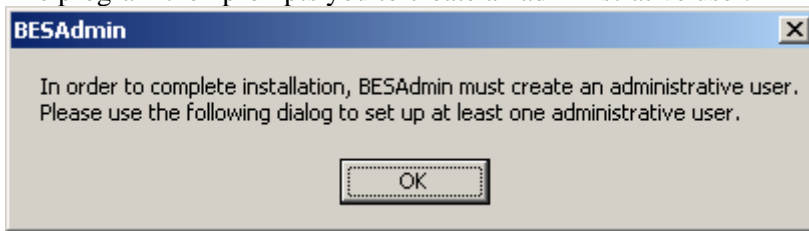
Click **OK** to open the **BigFix Enterprise User Management** dialog.
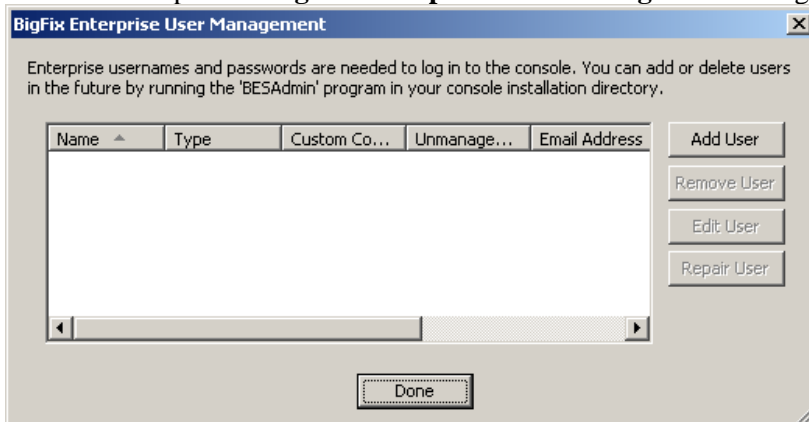
You do not need to add all the users at this point; you will be able to add more users by running the **BES Administration Tool** later. Enter the name of the BigFix operator (no spaces allowed), the email address and a password for this user. Indicate whether you want to allow this user to **administer management rights** or to **create custom content**.
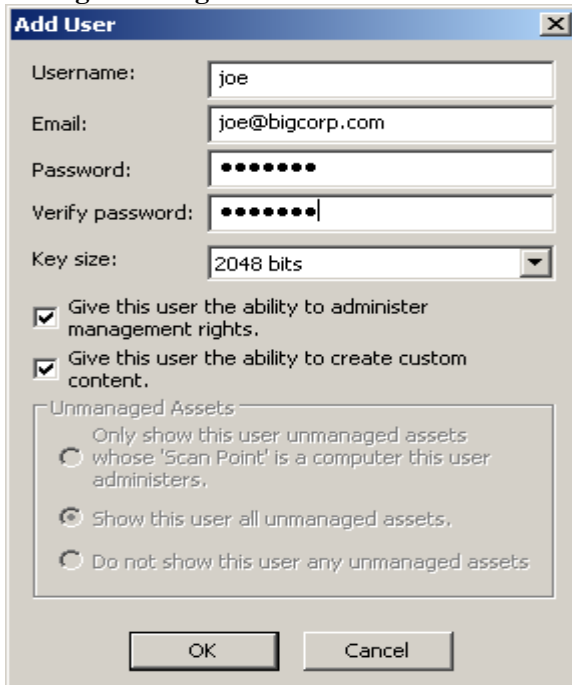
You must grant administrative rights to at least one user, typically yourself. You can limit user rights to view **unmanaged assets**. You can also limit users to their specific domain (using Scan Point), allow unfettered access or disallow all access. Click **OK** when done.

16.   When you have finished entering users, click **Done**.
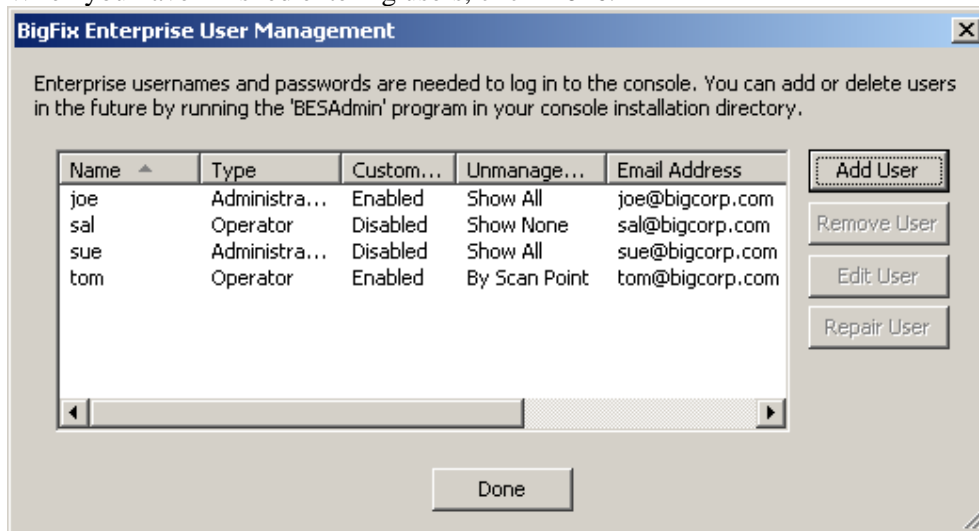
The program prompts you for your site admin password in order to propagate the BigFix Operator information.

17.   The BES Server installation is now complete. As the program exits, it gives you a chance to assess the installation. Make sure the box labeled **Run the BES Diagnostic Tool** is checked and then click **Finish**. Click the **Full Interface** button to run the BES Diagnostics in order to ensure that the installation is functioning properly and to present a complete analysis for your inspection. For more information on this dialog, refer to the section labeled **Running the BES Diagnostics Tool** later in this guide.

Authenticating Additional Servers (DSA)

Multiple servers can provide a higher level of service for your BigFix installation. If you choose to add Distributed Server Architecture (DSA) to your BigFix installation, you will be able to recover from network and systems failures automatically while continuing to provide local service. To take advantage of this functionality, you will need one or more additional servers with a capability at least equal to your primary server. Because of the extra expense and installation involved, you should carefully think through your needs before committing to DSA.

First, you must decide how you want your BES Servers to communicate with each other. There are three inter-server authentication options: the first two are flavors of NT and the third is SQL. Because it is more secure, BigFix recommends NT Authentication. You cannot mix and match; all BES Servers must use the same authorization.

Using NT Authentication with Domain Users/User Groups

With this technique, each BES Server uses the specified domain user or a member of the specified user group to access all other BES Servers in the deployment. To authenticate your BES Servers using Domain Users/User Groups, follow these steps:

1.   Create a service account user or user group in your domain. For a user group, add authorized domain users to your BES Servers. You may need to have domain administration privileges to do this.

2.   On the Master BES Server, use SQL Enterprise Manager (or the SQL 2005 Management Studio) to create a login for the domain service account user or user group, with a default database of

BFEnterprise, and give this login System Admin (sa) authority or the DBO (DataBase Owner) role on the BFEnterprise and master databases.

3.   On the Master BES Server, change the LogOn settings for the BES FillDB service to the domain user or member of the user group created above, and restart the service.

Using NT Authentication with Domain Computer Groups

With this technique, each BES Server is added to a specified domain computer group and each server accepts logins from members of that domain group. To authenticate your BES Servers using Domain Computer Groups, follow these steps:

1.   Create a Global Security Group in your domain containing each desired BES Server. You may need to have domain administration privileges to do this.

2.   After creating the group, each server will need to be rebooted in order to update its domain credentials.

3.   On the Master BES Server, use SQL Enterprise Manager (or the SQL 2005 Management Studio) to create a login for the domain group, with a default database of BFEnterprise, and give this login System Admin (sa) authority or the DBO (DataBase Owner) role on the BFEnterprise and master databases.

Using SQL Authentication

With this technique, each BES Server is given a login name and password, and is configured to accept the login names and passwords of all other BES Servers in the deployment. Be aware that the password for this account is stored in clear-text under the HKLM branch of the registry on each BES Server. To authenticate your BES Servers using SQL Authentication, follow these steps:

1.   Choose a single login name (for example, 'besserverlogin'), and a single password to be used by all servers in your deployment for inter-server authentication.

2.   On the Master BES Server, use SQL Enterprise Manager (or SQL 2005 Management Studio) to create a SQL Server login with this name. Chose SQL Server Authentication as the authentication option and specify the password. Change the default database to BFEnterprise and grant it System Admin (sa) authority or the db_owner role for the BFEnterprise and master databases.

3.   On the Master BES Server, add the following String values under the key

     HKLM\Software\BigFix\Enterprise Server\FillDB:
     ReplicationUser = <login name>
     ReplicationPassword = <password>

4.   Restart the BES FillDB service.

NOTE: This choice must be made on a deployment-wide basis; you cannot mix domain-authenticated servers with SQL-authenticated servers. Also, all BigFix servers in your deployment must be running the same version of SQL Server.

Installing Additional Servers (DSA)

Before proceeding with this section, determine your authentication method and complete the appropriate steps in the **Authenticating Additional Servers (DSA)** section discussed previously.

For each additional BES Server you wish to add to your deployment, make sure they are communicating with each other, and then follow these steps:

1. Install the same SQL Server version being used by the Master BES Server.

2. Run the **BES Server installer** on each machine that you wish to configure as an additional BES Server. You should use the same domain administration that you used for the local SQL Server install (so you have sa authority).

3. If you are extracting the server installer from the BES Installation Generator, select **Production Deployment**, and **I want to install with an existing masthead**. Specify the masthead.afxm file from the Master BES Server. Otherwise, use the Server install package from the BESInstallers folder on the Master BES Server.

4. On the **Select Database Replication** page of the server installer, select **Replicated Database**.

5. On the **Select Database** page, select **Local Database** to host the database on the server (typical for most applications).

6. Proceed through the installer screens as usual until the installer gets to **Configuring your new installation** and prompts you with a **Database Connection** dialog box. Enter the hostname of your master server, and the credentials for an account that can log into the master server with DBO permissions on the BFEnterprise database.

7. The Replication Servers window shows you the BES Server configuration for your current deployment. By default, your newly installed BES Server should be configured to replicate directly from the master server every 5 minutes. You can adjust this as necessary.

8. For large installations, the initial database replication can take several minutes and may get interrupted. If you experience this problem, you can discuss it with your BigFix technical contact or read the KB article on UnInterrruptableReplicationSeconds at:
    http://support.bigfix.com/cgi-bin/kbdirect.pl

9. Use SQL Enterprise Manager (or SQL 2005 Management Studio) to create the same SQL Server login you created earlier on the Master BES Server with BFEnterprise as the default database and System Admin (sa) authority or the DBO role on the BFEnterprise and master databases.

    For NT Authentication via Domain User/User Group, change the LogOn settings for the BES FillDB service to the domain user or member of the user group created above, and restart the service.

    For SQL Authentication, add the following string values to the FillDB registry keys, and restart the BES FillDB Service.

    > HKLM\Software\BigFix\Enterprise Server\FillDB:
    > ReplicationUser = <login name>
    > ReplicationPassword = <password>

10. On the newly-installed server, run the **BES Administration Tool** and select the **Replication** tab to see the current list of servers and their replication periods. Select the newly installed server from the pull-down menu, and verify in the list below that it is successfully connected to the master server. Then select the master server in the server dropdown, and verify that is properly connected to the new server. You may need to wait for the next replication period before both servers show a successful connection.

© 2008 by BigFix, Inc.

NOTE: The initial replication could take several hours depending on the size of your database. Wait for the replication to complete before taking any actions from a Console connected to the replica BES Server.

11. You can see a graph of the servers and their connections by clicking the **Edit Replication Graph** button. You can change the connections between servers by simply dragging the connecting arrows around.

Connecting the BES Console to a Different Server

When a BES Console is installed on a BES Server, you will have the option to connect to the local BES Server via the bfenterprise connection and the Master BES Server via the EnterpriseServer connection, by default. All standalone Consoles will only connect to the Master BES Server via the EnterpriseServer connection. To enable standalone Consoles and the Master BES Server Console to connect to the new replica BES Server, a new ODBC System DSN must be created:

1. From **Control Panel > Administrative Tools > Data Sources (ODBC)**, select the **System DSN** tab, and click **Add**.

2. Select the **SQL Server** driver, and click **Finish**.

3. Specify the following information

4. On the subsequent dialog, enter bes_<servername> for the **Name**, and <servername> for the **Server**, where <servername> is the hostname of the new replica BES Server. Click **Next**.

5. On the following dialog, specify NT Authentication or SQL Authentication as appropriate for your deployment. If unsure, use SQL Authentication. Uncheck the box to Connect to SQL Server to obtain default settings. Click **Next**.

6. Check the top box and change the default database to BFEnterprise. Click **Next**, and on the following screen, click **Finish**.

Now when the Console is started, the drop-down menu will offer you the choice between EnterpriseServer (to connect to the Master BES Server), <servername> (to connect to the new replica BES Server) and, on BES Servers only, bfenterprise (to connect to the local BES Server).

Running the BES Diagnostics Tool

The BES Diagnostics tool verifies the proper functioning of the BES Server components. It identifies components that are incorrectly configured or non-functional and displays the results. To run the diagnostics, follow these steps:

1. If you have just installed the BES Server, the BES Diagnostics Tool should already be running. Otherwise, log on to the BES Server as an administrator and launch the program (**Start > Programs > BigFix Enterprise > BES Diagnostics Tool**). The program analyzes the server components and creates a report.

2. For more in-depth information, click the **Full Interface** button. The BES Diagnostic control panel is displayed. This window has tabs corresponding to the categories of server diagnostics, including **Services** and **Web Reports.**
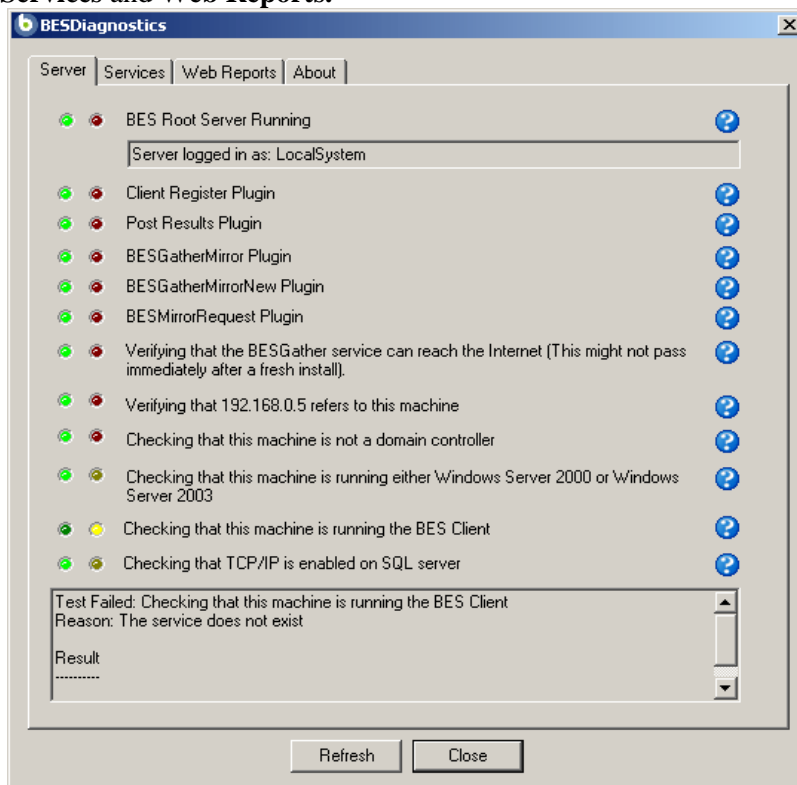
Note that if you have not yet installed the Client, a warning light will appear. It will register green as soon as you install the Client.

3.   The **Services** tab shows you if the database and gathering services are properly installed and running.
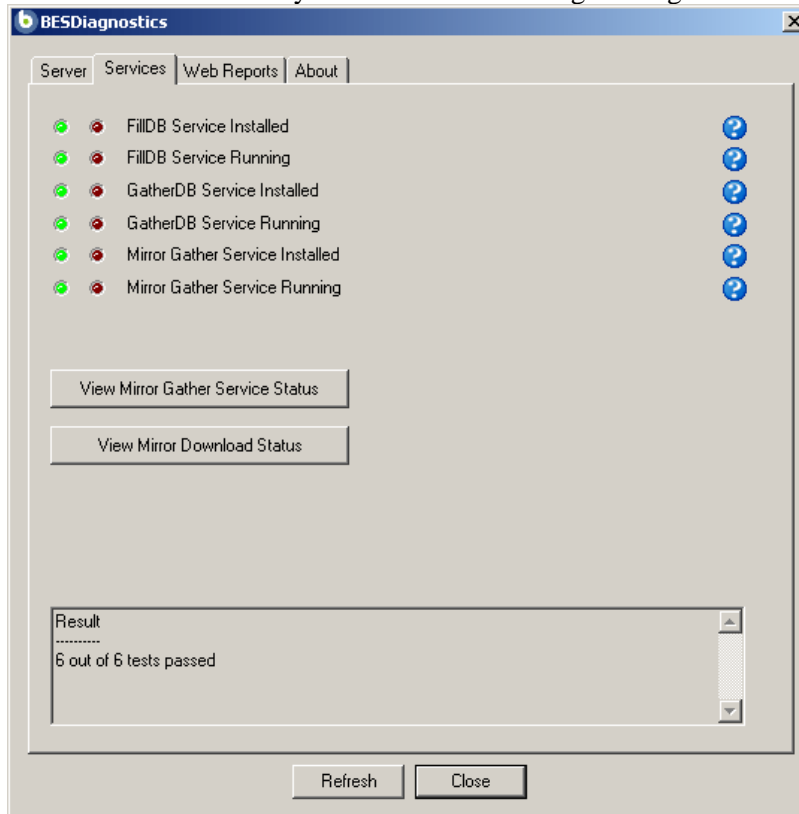
If a red light is glowing next to an item, it indicates a failure of that component. You must address the stated problem before you can be sure that the BES Server is functioning properly.

4.   To find out more information, click the question mark button to the right of any item. These buttons link to knowledge-base articles at the BigFix Support Site.

5.   If all the buttons are glowing green, click **Close** to exit the Diagnostic.

NOTE: If the BES Server computer is a member of a domain, but you are logged in as a local user, the BES Diagnostics Tool will sometimes improperly report that permissions are incorrect. If you see your permissions tests are incorrectly failing, you can safely ignore the diagnostics warnings.

Understanding the BES Server Components

The BES Server is now successfully installed. It will respond to messages and requests from the BES Relay, Client and Console computers using a variety of components. To better understand what the BES Server does, here is a list of some of the components along with a short description:

- **Client Registration Component.** When the BES Client is installed on a new computer, it registers itself with the client registration component of the BES Server and the BES Client is given a unique ID. If the computer's IP address changes, the BES Client will automatically register the new IP address with the client registration component.

- **Post Results Server Component.** When a BES Client detects that a Fixlet has become relevant, it reports to the Post Results server component using an HTTP POST operation. It identifies the relevant Fixlet along with the registered ID of the BES Client computer. This information is passed on to the BES database through the FillDB service and then becomes viewable in the BES Console. Also, other state changes are periodically reported by the clients to the server directly or though BES Relays.

- **Gather Server Component.** This component watches for changes in Fixlet content for all the Fixlet sites to which BES is subscribed. It downloads these changes to the BES Server and makes them available to the GatherDB Component.

- **FillDB Component.** This component posts BES Client results into the database.

- **GatherDB Component.** This component gathers and stores Fixlet downloads from the Internet into the database.

- **Download Mirror Server Component.** The Download Mirror Server Component hosts Fixlet site data for the BES Relays and BES Clients. This component functions as a simplified download server for BigFix traffic.

Installing the BES Console

The BES Console lets the operator monitor and fix problems on all managed computers across the network. It can be installed on any computer that can make a network connection via ODBC port **1433** to the BES Server. Except in testing or evaluation environments, it is not a good idea to run the BES Console on the BES Server computer itself due to the performance and security implications of having the publisher key credentials on a computer that is running a database and/or web server.

To install the BES Console, follow these steps:

1. Run the BES Installation Guide (**Start > Programs > BigFix Enterprise > BES Installation Guide**). Click the button labeled **Install BES Components**.

2. From the next screen, click **Install BES Console.**

3. After a welcome screen, you will see the BES Console license agreement. After reading the agreement, click **Yes** to accept the terms and continue the installation.

4. From the Select Features dialog, you can select specific features to install.
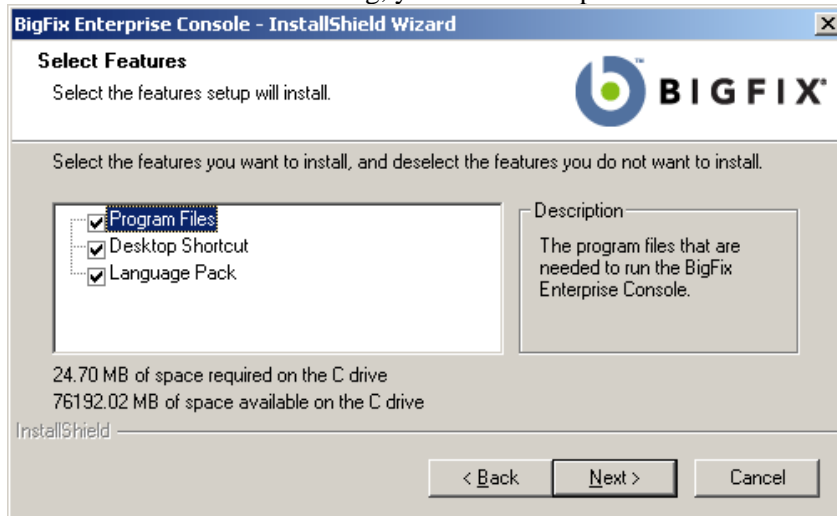
    Typically, however, you will accept the default. Click **Next**.

5. The next screen prompts you for an installation location for the BES Console. The default location is **C:\Program Files\BigFix Enterprise\BES Console**. To choose another destination, click **Browse** and navigate to the desired location. Click **Next** to continue.

6. After the files are installed, click **Finish** to complete the installation. At this point, you can choose to launch the BES Console, or continue to the next section to install the BES Clients.

See the *BES Console Users Guide* for more details on using the Console program.

Installing the BES Clients

The BES Client should be installed on every computer in your network that you want to administer with BES – including those computers running the BES Server and the BES Console. That allows those computers to receive important Fixlet messages (like security patches, configuration files or BES upgrades).

If you are running the BES Installer, you can select **Install BES Components > Install BES Clients > Install Locally**, which will install the Client on your local machine in the directory you specify.

There are several different techniques for installing the BES Client on remote computers, including the **BES Client Deploy Tool**, login scripts, third-party utilities and manual installation. Once the BES Clients are installed, upgrades and other maintenance tasks can be automated with Fixlet messages.

Using the BES Client Deploy Tool

On smaller networks (less than about 5,000 computers) connected to Active Directory or NT Directory domains, you can use the BES Client Deploy Tool to install Windows BES Clients. For larger networks, you may find it easier to use other deployment methods. This is an easy way to roll out clients, but there are some requirements and conditions:

- You must have an Active Directory or NT Directory domain (there is also an option to deploy to a list of computers if you have an administrator account on the computer).

- The BES Client Deploy Tool can only target computers running Windows NT, 2000, Server 2003, or XP.

- The computer running the BES Client Deploy Tool must be connected to the domain, but should not be the domain controller itself.

- The Service Control Manager (SCM) and the Remote Procedural Call (RPC) services must be running on the target machines.

- There must be no security policy on the computer that would prevent either a remote connection to the SCM or the issuance of a Remote Procedural Call.

- The dnsName property of every target computer in the Active Directory must be properly defined.

The Client Deploy Tool is designed to make it easier to push the BES Client to computers, but is not a full-featured enterprise-class software distribution tool. If you already have a software distribution tool, it is recommended that you use the existing software distribution tool instead.

The BES Client Deploy Tool starts by getting a list of computers from the Active Directory server and remotely connecting to the computers (accessing 100 computers at a time) to see if the BES Client service is already installed on each computer. If so, it reports **Installed** along with the status of the BES Client service such as **Running**, **Stopped**, etc. If it cannot determine the status due to a permissions problem or for any other reason, it will report **Status Unknown**. Otherwise it reports **Not Installed** – unless it cannot communicate with the computer at all, in which case it reports **Not Responding**.

If the BES Client is not yet installed, the tool provides interfaces that allow you to issue a Remote Procedural Call that accesses the shared installer and – with the proper domain administration credentials – runs it silently, with no end user interaction. Here is how to use the tool:

1. The BES Client Deploy Tool is created by the BES Installation Generator. You can launch the tool from the BES Installation Guide (click the **Install BES Components > Install BES Clients > Install Remotely** button) or launch it directly from **Start > Programs >BigFix Enterprise > BES Client Deploy**.

2. The resulting dialog offers three ways to deploy the BES Clients:

   - **Find computers using Active Directory.** The BES Client Deploy tool contacts the Active Directory server to get a list of all of the computers in the domain. It checks each of the computers to see if the BES Client is already installed and displays this information in a list.

   - **Find computers using NT 4.0 Domains.** All the computers in the domain are listed with a status flag indicating whether the BES Client has been installed or not.

   - **Find computers specified in a list.** Based on how your network resolves computer addresses, you will need to provide a list of computer names, IP address ranges, or hostnames. The list must have one **name / IP address range / hostname** per line. Using this option, the BES Client Deploy Tool will not attempt to discover any computers, but instead will attempt to install directly to all the listed computers.

3. Type in a username and password that has administrative access to the desired computers. In most cases, this is a domain administrator account. If you are using the computer list option, you can specify a local account on the remote computers (such as the local administrator account) that have administrative privileges. The rest of the client deployment process will use this username/password so if the account does not have the appropriate access on the remote computers, you will receive errors that access is denied.
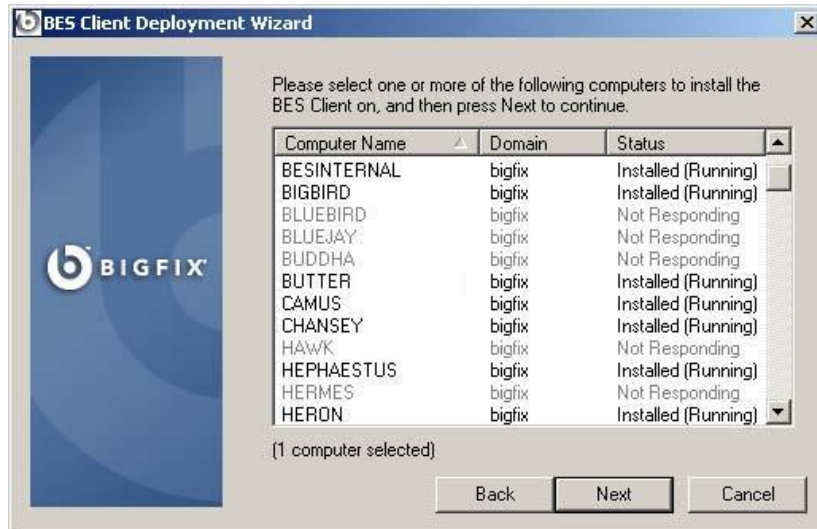
4.   When the list of computers is displayed, shift- and control-click to select the computers you want to administer with BES. Click **Next.**

5.   You will see a list of the computers you have selected. The default options are usually sufficient, but you may want to select **Advanced Options** to configure the following installation parameters:

- **File Transfer:** You can elect to **push** the files out to the remote server for installation or to have the files **pulled** from the local computer. Unless there are security policies in place to prevent it, for most cases pushing the files to the remote computer works best.

- **Connection Method:** There are two ways to connect to the remote computers. Using the **Service Control Manager** (SCM) is recommended, but you may also use the **task scheduler** if the SCM does not work.

- **Installation Path:** Specify a path for the Client, or accept the default (recommended).

- **Verification:** Check this box to verify that the BES Client service is running after waiting for the installation to finish, which will allow you to know if the installation completed successfully.

- **Custom Setting:** Add a BES Custom Setting to each BES Client deployed, in the form of a Name / Value pair.

6.   To begin the installation, click **Start**.

7.   When completed, a log of successes and failures is displayed. Simply retrying can resolve some failures; use advanced options if that does not work. For more information, see: http://support.bigfix.com/cgi.

Installing the BES Client Manually

The BES Client can always be installed by manually running the BES Client installer on each computer. This is a quick and effective mechanism for installing the BES Client on a small number of computers.

1.   Log on to the desired computer with administrator privileges and copy the **BES Installers\Client** folder from the BES installation computer to the local hard drive.

2.   Or run the BES Installation Guide (available at **Start > Programs > BigFix Enterprise > BES Installation Guide**) and click the button marked **Browse Install Folders**. It opens the **BESInstallers** folder and displays the **Client** folder.

3.   Once you have copied the Client folder to the target computer, double-click on **setup.exe** from that folder to launch the installer.

4.   After the welcome screen, you will be prompted for a location to install the software. You may accept the default, or click **Browse** to select a different location.

5.   After the files have been moved, click **Done** to exit the installer. The BES Client application is now installed and it will automatically begin working in the background.

6.   Repeat this process on every computer in your network that you want to place under BES administration.

Installing the BES Client with MSI

You can use the Microsoft Installer (MSI) version of the BES Client to interpret the package and perform the installation automatically. This MSI version of the client (BESClientMSI.msi) is stored in the **BESInstallers\ClientMSI** folder. You can run this program directly to install the client or you can call it with arguments. Here are some sample commands, assuming that the MSI version of the Client is in the c:\BESInstallers\ClientMSI folder:

- `msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi /qn`
  The \qn command performs a silent install.

- msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi INSTALLDIR="c:\myclient"
  This command will install the program to the given directory.

You can find the full list of installation options at the Microsoft site:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp.

With the MSI version of the client installer, you can create a Group Policy Object (GPO) for BESClientMSI deployments. For more information on Group Policies, see the Microsoft knowledge base article:
http://support.microsoft.com/kb/887405.

Using Software Distribution Tools

If you have access to a software distribution tool such as Microsoft SMS, IBM's Tivoli, CA Unicenter, or Novell's ZENworks, and all the intended computers have the tool enabled, you can use the tool to deploy an installation package for the BES Client. **This is the most effective way to deploy to an enterprise because the infrastructure and deployment procedure is already in place**.

Using Group Policies

It is possible, using Active Directory Group Policy Objects (GPO), to define a policy insisting that the BES Client should be installed on every machine in a particular group (Organizational Unit, Domain, etc.). This policy is applied every time a user logs into the specified domain, making it a very effective way to deploy the client if GPO is enabled. Consult your Active Directory administrator for more details.

Using Login Scripts

In an NT or AD domain, login scripts can be written that check for the presence of the BES Client. When the computer logs in and finds the BES Client missing, it can automatically access the BES Client installer from a specified location on a global file share. The BigFix Support Site at http://support.bigfix.com has a knowledge-base article with a sample login script (Keywords: example login script) and instructions on how to use login scripts to install the BES Client.

If your network will be adding new computers from time-to-time, this approach can be very convenient, ensuring that the BES Server will discover and manage new machines automatically. However, in some networks using Windows 2000 or XP, users must log in with administrator privileges for this technique to work.

These scripts pass arguments to the installer, which was created using InstallShield Professional, version 7. For more information about command line options for setup.exe, please refer to InstallShield's support web site. Here are some examples of command line switches for the BES Client installer that can be used in a login script:

- To install the BES Client silently while writing a log to the C:\, execute a DOS command of the form:
  `setup.exe/s /f2"C:\besclientinstall.log"`

- To change the default installation location, the appropriate form of the command is:
  setup.exe/s /f2"C:\besclientinstall.log" --InstallFolder="<InstallPath>"
  Where <InstallPath> is the full windows path to the folder where the BES Client should be installed.

NOTE: The Windows user running setup.exe must have Administrative privileges on the computer and must be able to write a log file to the same folder that contains the "setup.exe" file, otherwise the installation will fail and a log file will not be created.

Embedding in a Common Build

If your organization employs a specific build image or common operating environment (COE) on a CD or image that is used to prepare new computers, you can include the BES Client in this build. To create the image, follow these directions:

For Windows

1. Install the BES Client on the computer to be imaged.
2. The BES Client will immediately attempt to connect to the BES Server. If it successfully connects to the BES Server, it will be assigned a **ComputerID**. This ComputerID is unique to that particular computer, so it should ***not*** be part of a common build image. The next steps will delete this ID.
3. Open the Windows services dialog and stop the **BES Client service**.
4. Open the registry to **HKLM\Software\BigFix\EnterpriseClient\GlobalOptions** and delete the values ComputerID, RegCount, and ReportSequenceNumber.
5. The computer is now ready to be imaged with the BES Client (the BES Client will start again when the computer is restarted).

NOTE: if the BES Client is started before the image is completed, the BES Client will re-register itself and the registry values will need to be removed again (steps 3 and 4).

For Macintosh and Linux

1. Let the client register.
2. Stop the BES Client in the approved way, using **sudo systemstarter stop BESClient**.
3. If they exist, remove **RegCount**, **ReportSequenceNumber**, and **ComputerID** from the client preferences folder: /Library/Preferences/com.bigfix.besagent.plist. (On Linux systems edit the .config file in this location).
4. Delete the **__BESData** folder. The default location is **\Library\Application Support\BigFix\BES Agent**.

Using Email

You can send users an e-mail containing a URL and asking them to use it to install the BES Client when they log in to the network. This is an effective technique for Win9x computers since there are no limitations on user rights on those platforms. However, where administrative rights are enforced, this method requires users to log in with administrator privileges.

Enabling Encryption on BES Clients

Once installed, you can set up your BES Clients to encrypt all outgoing reports to protect data such as credit card numbers, passwords and other sensitive information.

> NOTE: You must have encryption enabled for your BigFix deployment before enabling it for your Clients. In particular, for the **required** option, your clients will go silent if you enable them without first setting up your deployment.

To enable encryption, follow these steps:

1. Click the **Computers** tab and select the computer or set of computers you wish to use encryption.
2. From the right-click context menu, select **Edit Computer Settings**.
3. From the **Edit Settings** dialog, click **Add**.
4. In the **Add Custom Setting** dialog, enter the setting name as **_BESClient_Report_Encryption** (note the double underline starting the name). There are three possible values for this setting:

   - **required:** causes the BES Client to always encrypt. In the event that there is no encryption certificate available in the masthead or if the target computer (BES Relay or Server) cannot accept encryption, the BES Client will not send reports.

   - **optional:** the BES Client encrypts if it is able, otherwise it sends its reports in clear-text.

   - **none:** No encryption will be done, even if an encryption certificate is present. This allows you to turn off encryption after you enable it.

5. Click **OK** to accept the value and **OK** again to complete the setting. You will need to enter your private key password to deploy the setting action.

Running the BES Administration Tool

The Installer automatically creates the BES Administration Tool (also called BES Admin), when it installs the other components of the Console program. This program operates independently of the BES Console and is intended for Administrative Operators only. You can find it from the Start menu: **Start > All Programs > BigFix Enterprise > BES Administration Tool.** To run the program, you must first browse to the signing key (license.pvk):
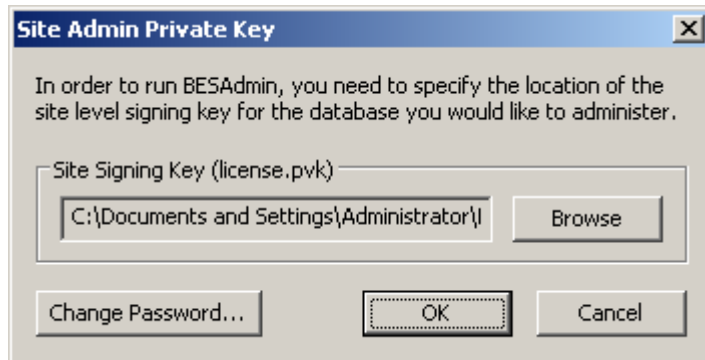
Note that you can also change your administrative password through this interface. Once you have selected the signing license, click OK to continue. You will need to supply your private key password to proceed.

User Management

If this is the first time you have run the program, the Administration Tool will provide you with a blank slate of users. Click **Add User** to include new BES Operators. This is where you will return when you want to add, remove or edit the management rights of your users.
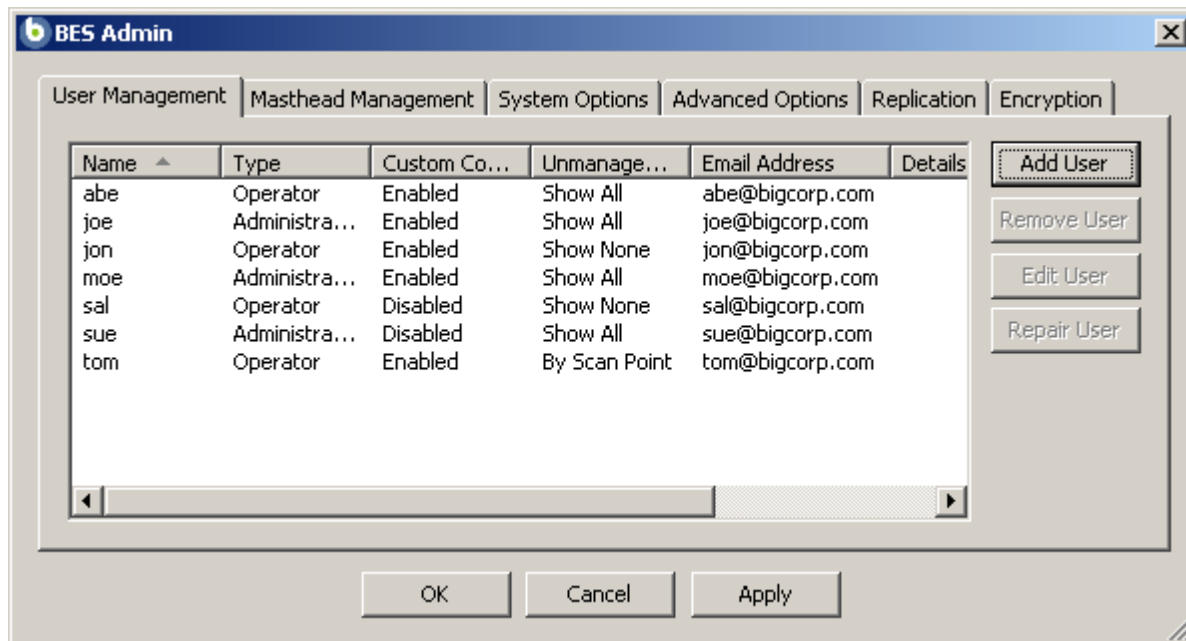
You can find out more about how to assign management rights in the section titled **Adding BES Console Operators**, page 47.

Masthead Management

Click the second tab to view the **Masthead Management** dialog.
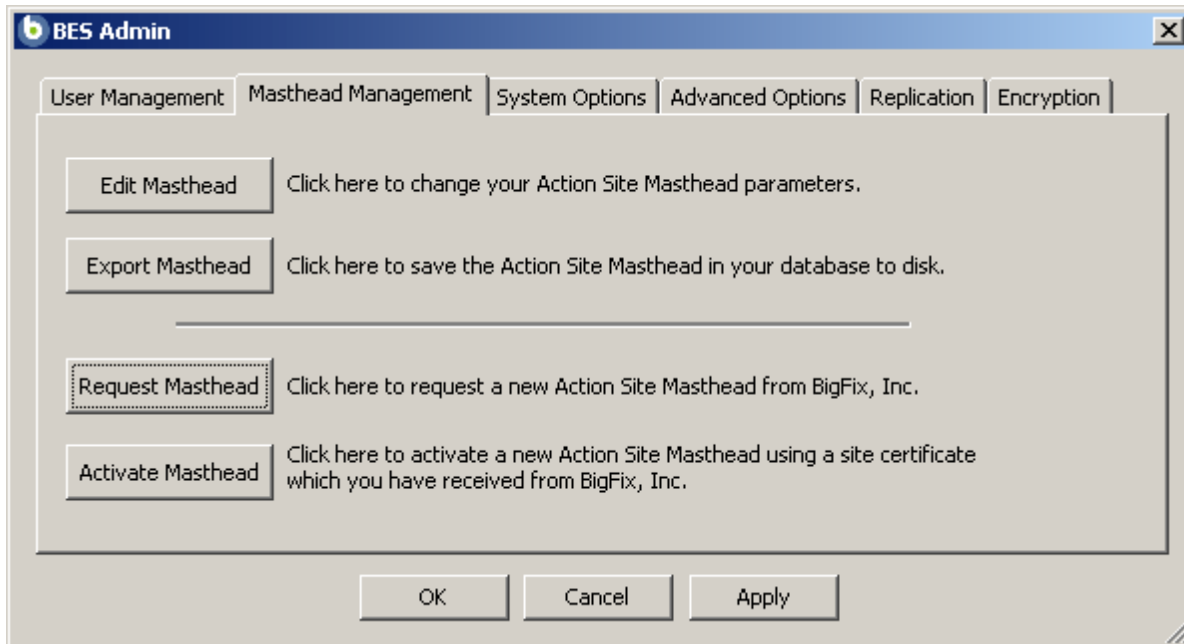
If you don't yet have a masthead, which is required to run the BES Console, this dialog provides an interface to request and subsequently activate a new masthead. If you have an existing masthead, you can edit it to change ports, gathering intervals and locking. For more information on managing your masthead, see the section named **Editing the Masthead**, page 71. You can also export your masthead, which can be useful if you want to extend your BES network to other servers.

System Options

The third tab opens the **System Options** dialog. The first option sets a baseline minimum for refresh intervals. This refers to the Fixlet list refresh period specified in the Preferences dialog of the BES Console. The default period is 15 seconds, but if you feel that your network can handle the bandwidth, you can lower this number to make the Console more responsive. Conversely, if your network is strained, you may want to increase this minimum.
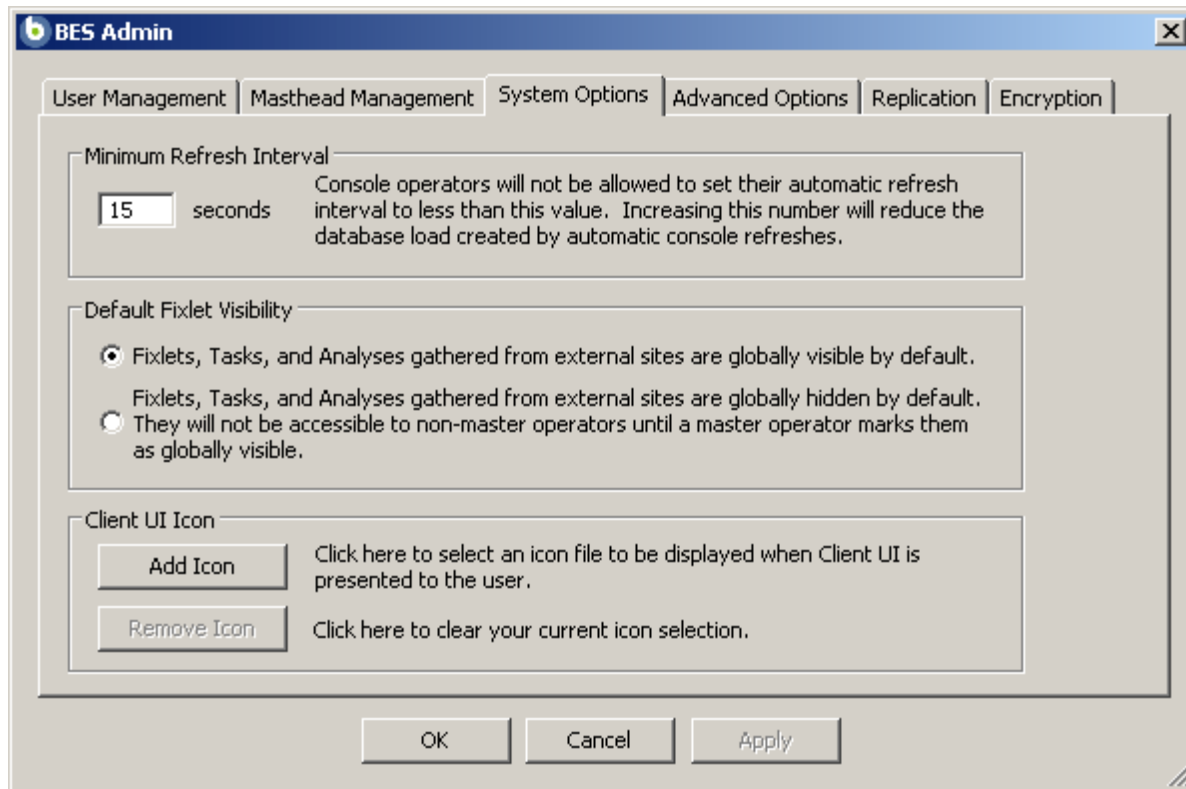
This dialog also lets you set the default visibility of external sites. These are, by default, globally visible to all Console operators. To give you extra control, you can set the visibility to hidden, and then adjust them individually through the Console. You must be an administrator or a master operator to make these hidden sites become visible.

This dialog also lets you add your own logo to any content that is presented to the user through the BES Client. Branding can be important to reassure your users that the information has corporate approval.

Advanced Options

The fourth tab opens the **Advanced Options** dialog. This dialog lists any global settings that apply to your particular BES installation.
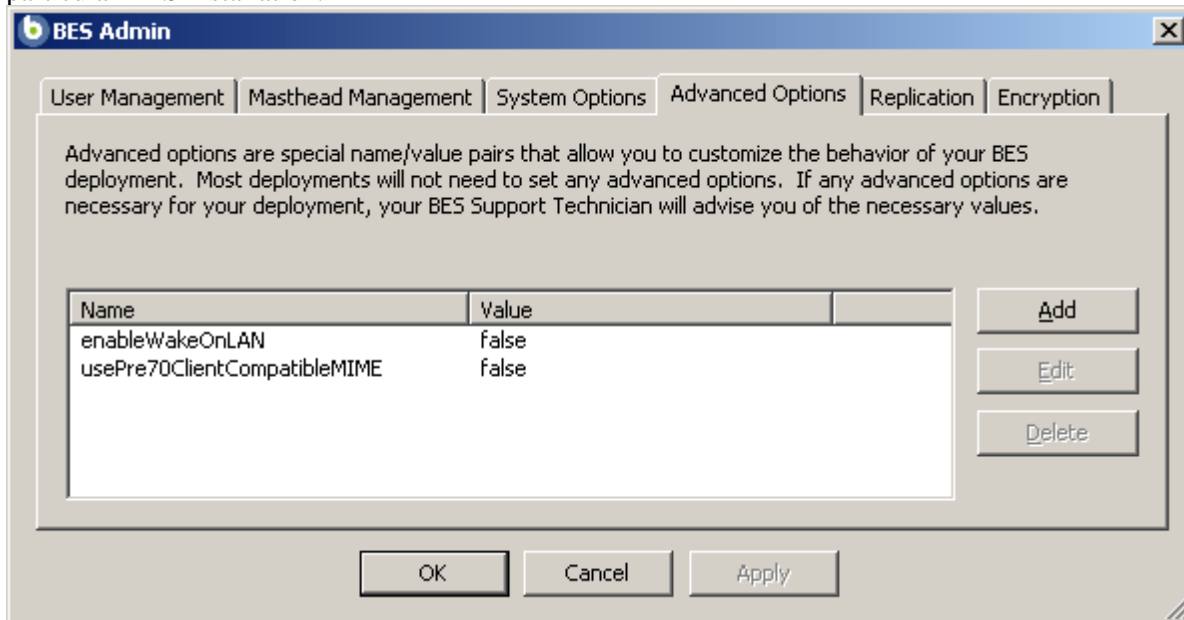
These options are name/value pairs, and are typically supplied by your BES Support Technician. As an example, if you are subscribed to the Power Management site, one of these options would allow you to enable the WakeOnLAN functionality.

Replication

The fifth tab opens the **Replication** dialog. This dialog helps you to visualize your replication servers. For more information, see the section titled **Managing Replication (DSA)**, page 59.

Encryption

The final tab opens the **Encryption** dialog. This dialog allows you to generate a new encryption key or to disable encryption altogether. For more information, see the section titled **Managing Client Encryption**, page 69.

Understanding Operator Rights

BES Console users, also known as publishers or operators, can be in charge of flexibly defined groups of computers with varying degrees of freedom. As the Site Administrator, you are in charge of each operator's domain and the specific rights they have over that domain. You can manage your team of operators and administrators by using the **BES Administration Tool**. This program is usually found in the start menu, under **Programs > BigFix Enterprise > BES Administration Tool**.

There are three basic classes of users: Site Administrators, Master Operators and ordinary (Non-Master) Operators. They each have different responsibilities and restrictions, described below.

Site Administrators

As a Site Administrator, you are the caretaker of the site-level key. This is a special key and should only be used for site-level tasks, and never for BES Console operations. For day-to-day operations, you must create a Master Operator key. Only use your Site Administrator key when performing top-level management tasks, including the following:

- **Creating/Modifying/Deleting Users** with the BES Administration Tool.

- Setting global system options including the **Minimum Refresh Interval**, **Default Fixlet Visibility**, and the **Client UI Icon** with the BES Administration Tool.

- Editing **Mastheads**.

- Initializing **Action Sites**. Although this is typically done by the Site Administrator, a Master Operator can also create an Action site.

- Administering **Distributed Server Architecture** (DSA) configurations. This includes setting the replication rate and the linkage between Replication Servers.

Master Operators

Master Operators can perform all of the functions of ordinary operators. In addition, they can also:

- **Edit the management rights** settings for other operators. This allows you to divide up the computers on your network among various operators so they each see a smaller subset of client computers.

- Create new **computer settings**, which monitor and control BES Client behavior and hold various labeled values for filtering. For more information, see http://support.bigfix.com/bes/misc/besconfigsettings.html.

- Create or edit **global retrieved properties**, which are used to filter and sort computers and can be used to create reports.

- View all unmanaged assets.

- Change the **BES Client heartbeat**, to optimize BES performance.

- **Subscribe** or **unsubscribe** from Fixlet sites.

- Create new custom Fixlet sites.

- Designate operators to be custom site owners, writers and readers.

- Globally **hide** or **unhide** Fixlet messages.

- Audit all actions taken in the BES Console.

- Manage External Fixlet Site subscriptions.

Operators

Ordinary operators can perform various management functions on computers under their control depending on the management rights that are delegated to them by master operators. They can:

- Deploy **Actions**.

- Create **custom content**, including Fixlet messages, Tasks, Baselines and Analyses. The Site Administrator can grant or revoke this right from the BES Administration Tool.

- Change or delete **computer settings**, which monitor and control BES Client behavior and hold various labeled values that can be used for sorting and filtering.

- View **unmanaged assets** according to each Operator's scope (as defined by Scan Points). The Site Administrator can grant or revoke this right from the BES Administration Tool.

- Be custom site owners, writers, and readers if granted the privilege by Master Operators.

Operators and Analyses

Operators have various rights and restrictions when it comes to activating and deactivating analyses:

- Ordinary operators cannot deactivate an analysis activated by other operators on computers they administer.

- Master Operators cannot directly activate custom analyses authored by ordinary operators. They can, however, make a copy of an analysis and activate the copy.

This chart summarizes the privileges and abilities of both types of Console Operator:

User Privileges	Master Operator	Operator
Initialize Action Site	Yes	No
Manage Fixlet Sites	Yes	No
Change BES Client heartbeats	Yes	No
Create Fixlets	Requires Custom Authoring	Requires Custom Authoring
Create Tasks	Requires Custom Authoring	Requires Custom Authoring
Create Analyses	Requires Custom Authoring	Requires Custom Authoring
Create Baselines	Requires Custom Authoring	Requires Custom Authoring
Create Groups	Yes	Manual Groups Only
Activate/Deactivate Analyses	All	Administered
Take Fixlet/Task/Baseline Action	All	Administered
Take Custom Action	Requires Custom Authoring	Requires Custom Authoring
Stop/Start Actions	All	Administered
Manage Administrative Rights	Yes	No
Manage Global Retrieved Properties	Yes	No
View Fixlets	All	Administered
View Tasks	All	Administered
View Analyses	All	Administered
View Computers	All	Administered
View Baselines	All	Administered
View Computer Groups	All	Administered
View Unmanaged Assets	Administered by BES Admin	Administered by BES Admin
View Actions	All	Administered
Make Comments	All	Administered
View Comments	All	Administered
Globally Hide/Unhide	Yes	No
Locally Hide/Unhide	Yes	Yes
Use Wizards	Requires Custom Authoring	Requires Custom Authoring
Remove computer from database	All	Administered
Create Manual Computer Groups	Yes	Yes
Delete Manual Computer Groups	Yes	No
Create Automatic Computer Groups	Yes	Requires Custom Authoring
Delete Automatic Computer Groups	Yes	Requires Custom Authoring and Administered
Create Custom Site	Yes	No
Modify Custom Site Owners	Yes	No
Modify Custom Site Readers/Writers	Yes	Site Owners

Administered: The operator must own or have permissions
Requires Custom Authoring: Granted by the Site Administrator through BES Admin
Administered by BES Admin: Granted by the Site Administrator through BES Admin

Adding BES Console Operators

As the BES Site Administrator, you must create accounts for each new BES Console operator, allowing them to view the database using the BES Console. For security purposes, a password-protected public/private key is also generated so the new operator can properly create and sign actions. To add a new operator, use the BES Administration Tool.

1. When you install the BES Server, the BES Admin Tool is automatically run so you can add new operators. However, you may add operators at any time by launching **Start > Programs > BigFix Enterprise > BES Administration Tool**.

2. If not already displayed, browse to your **site signing key** (license.pvk) and select it. Click **OK**.

3. Click the **User Management** tab. Click **Add User** to start adding new BES Console operators with publishing credentials. For each operator/publisher you add, you will fill out data in the **Add Publisher** dialog:

4. Enter the **Username** and **Email** address of the person you want to designate as a publisher, or operator. Start with yourself, making sure you grant yourself management rights.

5. Create a **Password** and retype it for confirmation. Once you hand the keys over to your operators, they can change their passwords if they wish.

6. Enter a **Private Key Length** from the pull-down menu, or accept the default.

7. Check the first box if you want this operator to **administer management rights**, making them a Master Operator. As the BES administrator, you should check this box when you add yourself to the user list.

8. Check the second box if you want this operator to be able to **create custom content** such as custom Fixlet messages, Tasks and Baselines. The availability of this feature depends on the license granted you by BigFix, Inc.

    WARNING! Custom actions grant the user the ability to create and deploy custom actions across the entire network with just a few mouse clicks. Use good judgment when granting these rights to operators.

9. At this point, you can also grant rights to view **unmanaged assets**. You can grant all-or-none access, or limit users to their personal Scan Point scope. Make note of this operator and password in a safe place and then click **OK**.

10. A dialog will appear prompting you to choose a location in which to create a new folder that will contain the operator's credentials. You will need to choose both the parent folder and the name for the new folder, which will default to the operator's name. Consider using a removable disk for additional security. You will hand this folder, along with the password, to the designated BES Console operator.

11. BES will ask you for the **Site Admin Private Key Password** (this is the password you created when you first installed BES) to authenticate you as the BES Site Administrator. Type it in and click **OK**. Note that you will have opportunities later to change this password.

12. Repeat this process for each operator you wish to authorize as a BES Console operator. These operators will then have a personal folder that acts as their key to the BES Console. They should take care to protect the disk containing this folder, which holds the following files:

    - **publisher.pv**k: the private key created for each authorized operator/publisher. As with the key to the front door, the operator must understand the responsibility of caring for this file.

    - **publisher.crt:** the signed certificate authorizing each operator/publisher to issue actions. This file is also stored in the database.

13. Once you have granted publishing rights to all your designated BES Console operators, click **APPLY** and provide your site level password again.

14. The BES Administration Tool must propagate the action site – with the new operator information – throughout your network. Click **Yes** to send the updated user information to all the BES Clients. At any time, you can add new authorized operators by running the BES Administration Tool again.

Notes on Operators:

- You should propagate the action site whenever you change any operator information, especially when you revoke operators.

- If two operators were created prior to BES Version 7.0 with the same email address, their signing certificates may conflict with each other and they will not be able to use the custom site functionality until one of them is deleted and reissued. Such users will be highlighted in red in BES Admin – clicking on **repair** will pop up a message box explaining the problem.

- A user's status as Operator or Master Operator is permanently associated with the username and cannot be changed.

- To be on the safe side, Site Administrators would be wise to create users with a default password and store a backup copy of the console key files with those default passwords. Console operators who forget their password can be provided with the saved copy.

Configuring the BES Components

Now that the BES components have been installed, you can configure your system for greater efficiency or to support larger or non-standard deployments.

The picture below represents a large and fairly complex deployment of BES. Study the picture to understand how the system communicates. In particular, notice that all information flows into the BES Server in the HQ/Data Center, that there are multiple levels of BES Relays, and that all communications flow through the relay chain back to the server.
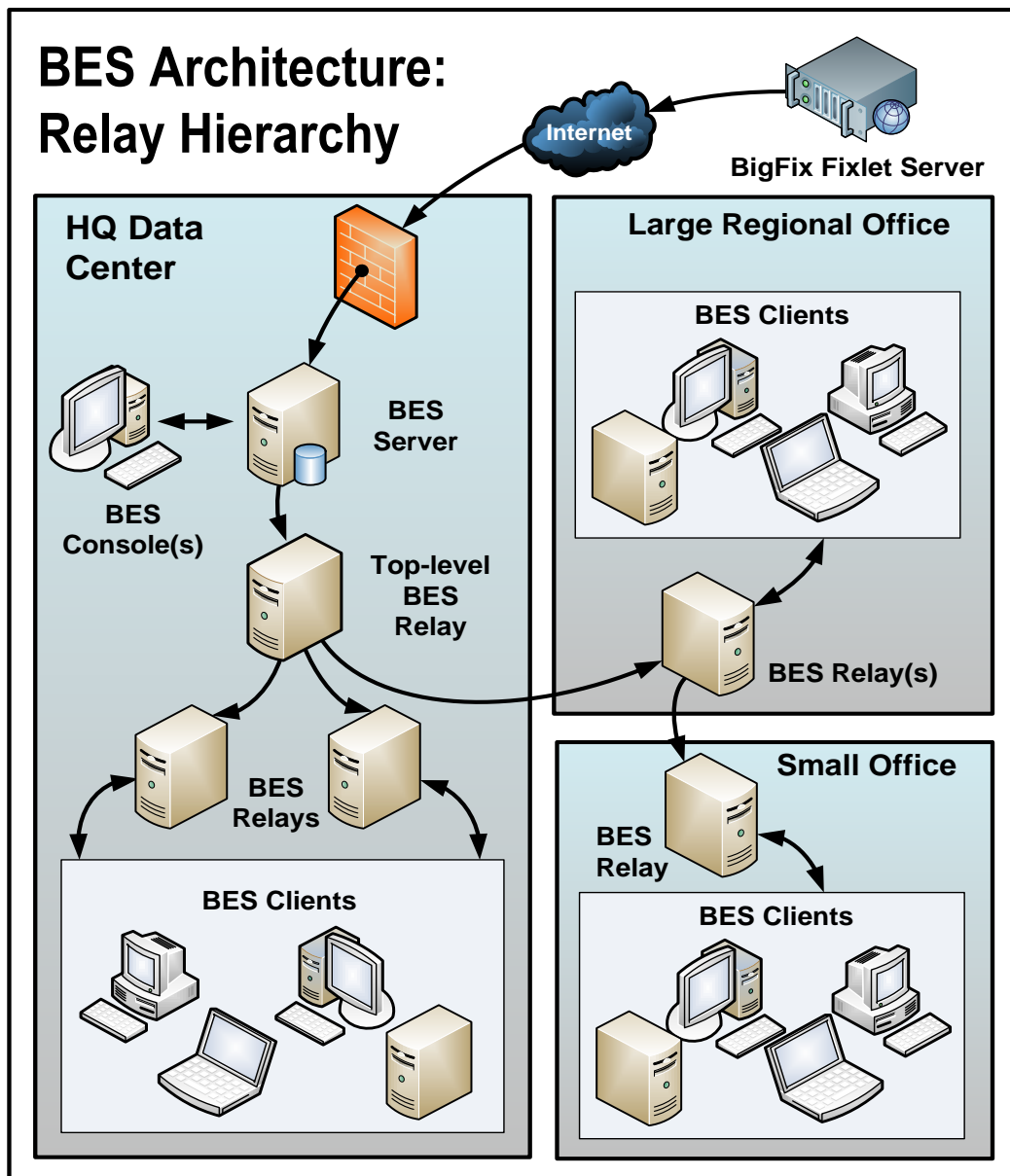
Using BES Relays

BES Relays can significantly improve the performance of your BES installation. BES Relays are designed to lighten both upstream and downstream burdens on the BES Server. Rather than communicating directly with a BES Server, BES Clients can instead be instructed to communicate with designated BES Relays, considerably reducing both server load and client/server network traffic. BES Relays work by:

- **Relieving Downstream Traffic.** The BES Server has many duties, one of the most taxing of which is distributing files, such as patches or software packages, and Fixlet messages to the BES Clients. BES Relays can be set up to ease this burden, so that the BES Server does not need to distribute the same file to every BES Client. Instead, the file is sent once to the BES Relay, which in turn distributes it to the BES Clients. In this model, the BES Client connects directly to the BES Relay and does not need to connect to the BES Server.

- **Reducing Upstream Traffic.** In the upstream direction, BES Relays can compress and package data (including Fixlet relevance, action status and retrieved properties) from the BES Clients for even greater efficiencies.

- **Reducing Congestion on Low-Bandwidth Connections.** If you have a BES Server communicating with computers in a remote office over a slow connection, designate one of those computers as a BES Relay. Then, instead of sending patches over the slow connection to every BES Client independently, the BES Server only sends a single copy to the BES Relay (if it needs it). That BES Relay, in turn, distributes the file to the other computers in the remote office over its own fast LAN. This effectively removes the slow connection bottleneck for remote groups on your network.

- **Reducing the Load on the BES Server.** The BES Server has many duties including handling connections from BES Clients and BES Relays. At any given instant, the BES Server is limited in how many connections it can effectively service. BES Relays, however, can buffer multiple BES Clients and upload the compressed results to the BES Server. BES Relays also distribute downloads to individual BES Clients, further reducing the workload of the BES Server and allowing BES to operate faster and more efficiently.

BES Relays are an absolute requirement for any network with slow links or more than a few thousand BES Clients. Even with only a few hundred BES Clients, BES Relays are recommended: they make downloads faster by distributing the load to several computers rather than being constricted by the physical bandwidth of the BES Server.

BES is quite powerful; it is easy to deploy an action causing hundreds of thousands of BES Clients to download very large files all at once. Windows XP SP2 alone is more than 200MB and it is not uncommon to distribute software packages that are gigabytes in size. Without BES Relays, even network pipes as fast as T1 (or faster) lines can be overwhelmed by many BES Clients requesting large, simultaneous file downloads.

Establishing the appropriate BES Relay structure is one of the most important aspects of deploying BES to a large network. When BES Relays are fully deployed, an action with a large download can be quickly and easily be sent out to tens of thousands of computers with minimal WAN usage.

In an effort to ease deployment burdens and reduce the total cost of ownership of BES, the BES Relays are designed to run on shared servers such as file/print servers, domain controllers, SMS servers, AV distribution servers, etc. As a consequence, a typical BES installation will have less than 1% of its relays running on dedicated computers.

For the most part, the BES Relay uses minimal resources and should not have a noticeable impact on the performance of the computer running it (see the section below for BES Relay requirements). The BES Clients can be set to automatically find their closest BES Relay. These features allow for significant savings in both hardware and administrative overhead.

NOTE: If the connection between a BES Relay and BES Server is unusually slow, it may be beneficial to connect the BES Relay directly to the Internet for downloads. More information about BES Relays can be found by visiting http://support.bigfix.com/cgi, or by talking to your BigFix sales engineer or support technician.

BES Relay requirements

A BES Relay takes over most of the download duties of the BES Server. If several BES Clients simultaneously request files, the BES Relay may consume a fair amount of bandwidth to serve them up. Generally, however, the duties of the BES Relay are not too demanding. When many actions are being deployed at once, CPU and disk usage can spike, but typically for only a short duration. The primary resource constraint for the BES Relay will be disk space.

The requirements for a BES Relay computer vary widely depending on a number of factors. Here are some requirements for the BES Relays:

- The BES Relay must have a two-way TCP connection to its parent (which can be a BES Server or another BES Relay).

- The BES Relay can be installed on an ordinary workstation, but if many BES Clients simultaneously download files, it may slow the computer down. Also, for the BES Relay to work properly, the computer must be powered on so workstations that are commonly powered off are poor choices for BES Relays.

- Workgroup file servers, print servers, SMS servers, AntiVirus servers, domain controllers, test servers, and other server-quality computers that are always turned on are good candidates for installing a BES Relay. BES Relays were designed to be installed on an existing shared server to reduce the total hardware cost of deploying BES. Most companies already have partially utilized servers in the appropriate places throughout their networks. Fortunately, should you need to purchase a new computer for the task, the BES Relay requirements are low. An inexpensive workstation-class computer or bottom-of-the-line server should suffice.

- BES Relays must be installed on Windows NT SP6a, Windows 2000, XP, Server 2003 or Windows Vista computers.

- Due to the fact that older versions of Internet Explorer used outdated network libraries, the computers running the BES Relays must have at least Internet Explorer 4.0 or above to work properly.

- More information about BES Relay requirements can be found at http://support.bigfix.com/cgi.

- The BES Relay cache size is configurable but is set to 1GB by default. It is recommended that you have at least 2 GB available for the BES Relay cache to prevent hard drive bottlenecks.

Designating a BES Relay

To set up a BES Relay, you need to designate a **Windows NT**, **Windows 2000, Server 2003,** or **Windows XP** computer that is running a BES Client to act as the BES Relay. The BES Clients on your network will detect the new Relays and automatically connect to them. To create a BES Relay, use the BES Console, and follow these steps:

1. In the BES Console, click the **Tasks** tab to bring up a tree/list of all Tasks.
2. Find the Task with the title **Install BES Relay** (it may include a version number after it). This Task will be relevant as long as there is at least one BES Client that meets the requirements for the BES Relay.
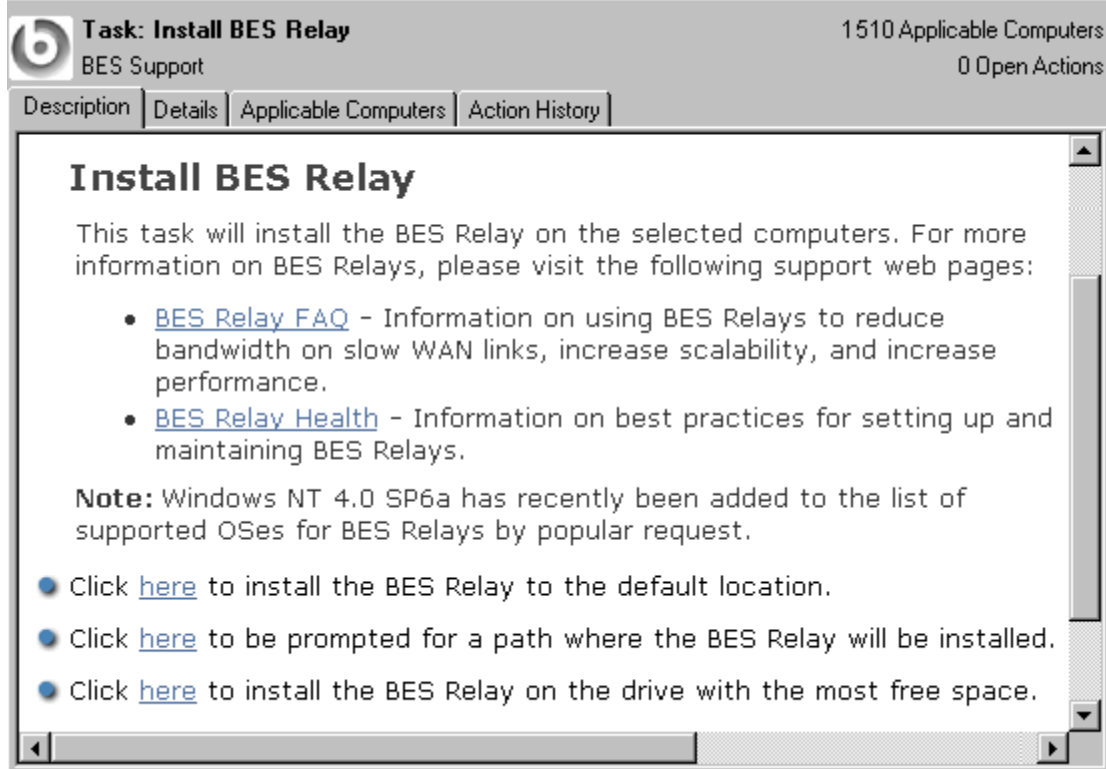
3. Choose your deployment option by choosing one of the actions in the Task. You can target single or multiple computers with this action.

Automatically Discovering Relays

Once you have set up your BES Relays, you are almost done. If they are configured to perform automatic relay selection, the BES Clients will automatically find the relay that is the fewest hops away and point to that computer instead of the server. This is the recommended technique, since it dynamically balances your system with minimal administrative overhead. To make sure your BES Clients are set up to automatically discover relays:

1. Start up the BES Console and click the **Computers** tab to bring up a filter/list of BES Clients.
2. Shift- and ctrl-click to select the set of computers you want to automatically detect BES Relays. Press ctrl-A to select the entire set of BES Clients.
3. Right-click on this highlighted set and choose **Edit Computer Settings** from the pop-up menu. Depending on whether you selected one or more computers, the dialog boxes are slightly different. Typically, you will have selected all the BES Clients in your network, so you will see the multiple-select dialog.
4. Check the box marked **BES Relay Selection Method**.
5. Click the button marked **Automatically Locate Best BES Relay**.
6. Click **OK**.

Defaulting to Automatic Relay Discovery

As you install BES Clients, you may want them to automatically discover the closest BES Relay by default. Here is how to set this up:

1. From the **Edit Computer Settings** dialog (see above), select the **Target** tab.
2. Click the button labeled **All computers with the property…**
3. In the window below, select **All Computers**.
4. Select the **Constraints** tab.
5. Uncheck the **Expires On** box.
6. Click **OK**.

Now as new BES Clients are installed, they will automatically find and connect to the closest BES Relay without any further action.

Notes about Automatic Relay Discovery

The BES Clients use a sophisticated algorithm to figure out which BES Relay is the closest on the network. The algorithm uses small ICMP packets with varying TTLs to discover and assign the most optimal relay. If multiple optimal relays are found, the algorithm automatically balances the load. If a relay goes down, the Clients will perform an auto-failover. This represents a major improvement over manually specifying and optimizing relays. However, there are a few important notes about automatic relay selection:

- ICMP must be open between the BES Client and the BES Relays. If the BES Client cannot send ICMP messages to the BES Relays, it will be unable to find the optimal BES Relay (in this case it would use the failover relay if specified or pick a random relay).

- Sometimes fewer network hops are not a good indication of higher bandwidth. In these cases, BES Relay Auto-selection may not work properly. For instance, a datacenter may have a BES Relay on the same high-speed LAN as the BES Clients, but a BES Relay in a remote office with a slow WAN link is fewer hops away. In a case like this, you should manually assign the BES Clients to the appropriate optimal BES Relays.

- BES Relays will use the DNS name that the operating system reports. This name must be resolvable by all BES Clients otherwise they will not find the BES Relay. This DNS name can be overridden with an IP address or different name using a Task in the BES Support site.

- BES Clients can report the distance to their corresponding relays. This information is valuable and should be monitored for changes. Computers that abruptly go from one hop to five, for instance, may indicate a problem with their relays.

- More information about BES Relays, automatic relay selection, and troubleshooting BES Relay issues can be found at http://support.bigfix.com/cgi-bin/redir.pl?page=besrelays.

Using Relay Affiliation

BES 7.0 introduces a new feature called BES Relay Affiliation that is intended to provide a more sophisticated control system for automatic relay selection. The feature is very flexible and may be used in many different ways but the primary use case is to allow the BES infrastructure to be segmented into separate logical groups. A set of BES Clients and BES Relays can be put into the same affiliation group such that the BES Clients will only attempt to select the BES Relays in their affiliation group. This feature is built on top of automatic relay selection and you should understand that process (see the previous section) prior to implementing BES Relay Affiliation.

BES Relay Affiliation only applies to the automatic relay selection process. The manual relay selection process (see next section) is unaffected even if computers are put into BES Relay Affiliation groups.

Creating BES Client Affiliation Groups

BES Clients are assigned to one or more Relay Affiliation groups through the BES Client setting:

_BESClient_Register_Affiliation_SeekList

This BES Client setting should be set to a semi-colon (;) delimited list of relay affiliation groups.

Example: AsiaPacific;Americas;DMZ

Creating BES Relay and Server Affiliation Groups

BES Relays and BES Servers can be assigned to one or more Affiliation groups through the BES Client setting:

_BESRelay_Register_Affiliation_AdvertisementList

This BES Client setting should also be set to a semi-colon (;) delimited list of relay affiliation groups.

Example: AsiaPacific;DMZ;*

NOTE: BES Relays and BES Servers are not required to have a SeekList setting. The SeekList is only used by the BES Client.

BES Relay Affiliation List Information

There are no pre-defined relay affiliation group names; you are free to pick group names that are logical to your deployment of BES. There are some naming rules you should observe:

- Do not use special characters (including ".") when picking names

- Group names are not case sensitive

- Leading and trailing whitespaces are ignored in comparisons

The ordering of Relay Affiliation groups is important for the BES Client. The asterisk (*) has a special meaning in a Relay Affiliation list: it represents the set of unaffiliated computers. Unaffiliated computers are BES Clients or BES Relays which do not have any relay affiliation group assignments or have the asterisk group listing.

For more information on BES Relay Affiliation, see the article at the BigFix website:
http://support.bigfix.com/bes/install/besrelayaffiliation.html.

Manually Selecting Relays

You may have a reason to manually specify exactly which BES Clients should connect to which BES Relay. You can do that too. Here is how:

1. Start up the BES Console and click the **Computers** tab to bring up a filter/list of BES Clients.
2. Shift- and ctrl-click to select the set of computers you want to attach to a particular BES Relay.
3. Right-click on this highlighted set and choose **Edit Computer Settings** from the pop-up menu. As with creating the relays (above), the dialog boxes are slightly different if you have selected one or multiple computers.
4. Check the box labeled **Primary BES Relay** and then select a computer name from the drop-down list of available BES Relay servers.
5. Similarly, you can assign a **Secondary BES Relay**, which will be the backup whenever the Primary Relay Server is unavailable for any reason.
6. Click the **OK** button**.**

Viewing BES Relay Selections

To see which BES Clients are selecting which BES Relays, click on the Computers tab in the BES Console and look under the **Relay** columns (these columns may be hidden; if so you will need to right-click on the column headings and make sure the Relay columns are checked). The BES Relay columns show information including the BES Relay method, service and computer.

By default, the BES Clients will attempt to find the closest BES Relay (based on the fewest number of network hops) every six hours. More information on BES Relays can be found at http://support.bigfix.com/cgi.

Monitoring BES Relay Health

BES allows you to monitor your BES Client/Relay setups to ensure they are working optimally. Before deploying a large patch, you may want to check the status of your BES Relays to guarantee a smooth rollout.

Here are some suggestions for monitoring your BES Relay deployment:

- Click on the **Analyses** tab and, from the BES Support site, activate the **BES Relay Status**. This Analysis contains a number of properties that will give you a detailed view of the BES Relay health.

- Click on the **Results** tab for the analysis to monitor the **Distance to BES Relay** property in the **BES Relay Status** Analysis to get a sense of what is normal in your network. If your topology suddenly changes, or you notice that some of your BES Clients are using extra hops to get to the server, it could indicate the failure of a BES Relay.

- Try to minimize the number of BES Clients reporting directly to the BES Server because it is generally less efficient than using BES Relays. You can see which computers are reporting to which BES Relays by studying this Analysis.

- Check http://support.bigfix.com/cgi or consult with your support technician for more information.

Optimizing the BES Server(s)

BES is designed to operate efficiently, with minimal impact on network resources. However, there may be installations that stretch the recommended configurations, where there just seem to be too many BES Clients for the allotted server power. The best solution is to buy another server, but short of that, you may be able to modify some preferences to get better performance. Most of these optimizations involve a trade-off between throughput and responsiveness, so proceed with caution. Your BigFix support technician has more information about which modifications might be best for your particular deployment.

Here are some possible optimization techniques:

- Deploy BES Relays to reduce the load on the server. This is by far the most effective way to increase the performance and responsiveness of BES. Generally, the more BES Relays, the better the performance (as a rule of thumb, one BES Relay for 500-1000 BES Clients is a good choice, although it can be much higher for a dedicated computer).

- Slow down the **BES Client heartbeat** from **File > Preferences**. This decreases the frequency of messages that are regularly dispatched by the BES Clients to update their retrieved properties. Reducing this frequency will reduce the amount of network traffic generated, but also decreases the timeliness of the retrieved properties. However, regardless of the heartbeat settings, the BES Clients always send up their latest information whenever they receive a refresh ping from the BES Server or when they notice that a Fixlet is relevant.

- Slow down the **Fixlet List Refresh** rate from **File > Preferences**. This decreases the update frequency for the information displayed in the BES Console. If there are many BES Consoles simultaneously connected or the database is very large, reducing this frequency can substantially reduce the load on the BES Server. If multiple BES Console operators are going to be simultaneously using the BES Console, you should set the refresh rate to be something higher than the default (15 seconds) to reduce the load on the BES database. Consider changing it to 60-120 seconds or more if there are many BES Console operators. The BES Admin tool on the BES Server will allow you to set a global minimum refresh rate.

If you are using SQL Server 2000 for the BES database, your database administrator may be able to help you with the following optimizations:

- Change the SQL Server 2000 Recovery Model for the BFEnterprise database to **Simple** rather than **Full** which is the SQL Server 2000 default (MSDE 2000 defaults to Simple).

- Reduce the percentage of memory allocated to SQL Server 2000 from 100% to 85%, to ensure that the web server and operating system are not starved for memory.

More performance recommendations can be found at http://support.bigfix.com/cgi-bin/redir.pl?page=besperformance and http://support.bigfix.com/bes/install/serverreq71.html.

Optimizing the BES Console(s)

To be responsive, the BES Console requires reasonable CPU power, memory and cache space. If you have a BES Console that is taking a long time to load or that is performing sluggishly, there are several techniques you can use to speed it up:

- **Make sure you have sufficient memory.** The BES Console benefits greatly from capacious memory to speed up the viewing, filtering and sorting of content (Fixlet messages, Tasks, Actions, etc.). If your computer does not have enough physical memory, the BES Console will run noticeably slower. You can check memory usage from the Task Manager (Ctrl-Shift-ESC). Select the Performance tab and refer to the Physical Memory section. If the available memory is less than 10% of the total memory, you are running low on RAM and can benefit from adding more.

- **Use high-speed network connections** between your BES Consoles and Servers, preferably with LAN connections of at least 100 MBPS. The BES Database can be sizeable for a large network, so running the BES Console from a computer with a slow connection will often result in very long load times.

- **Use remote control software.** With so much data to load and display, operating the BES Console in a remote office over a slow link can be tedious. In situations like this, you may be able to benefit from solutions such as Citrix, Terminal Services or other remote control software. Set up the remote control server on a computer with fast access to the BES Server. Allow that machine to present instances of the BES Console and let the branch office run these Consoles remotely. The database stays in the main office, and the remote office enjoys optimal performance. For more information, see **Citrix / Terminal Services Configuration**, page 91.

- **Delete old actions.** The BES database stores information about old actions which the BES Console loads in at startup and saves out at shutdown. If you do not need to track these old actions, you can delete them, allowing the BES Console to load and close faster. Note that deleted actions continue to exist in the database, but are simply not loaded into the BES Console or Web Reports and can be physically undeleted if necessary.

- **Close some windows.** When the BES Console does a refresh, it updates all the open BES Console windows. You can significantly speed up the refreshes by selecting **Window > Close All**.

- More information about enhancing the performance of BES is available at: http://support.bigfix.com/bes/misc/besperformance.html.

Managing Replication (DSA)

Replication servers are simple to set up and require minimal maintenance. You may wish to tweak the interval or allocate your BES Servers differently. Most of these changes are done through the BES Administration Tool. Here you can see the current settings for your BES Servers and make the appropriate changes.

Change the Replication Interval

1. Start up the **BES Administration Tool**.
2. Select the **Replication** tab.
3. Select the desired server from the drop-down menu. Using longer replication intervals will mean that the servers will need to replicate data less often, but they will have more data to transfer each time. Note that replication intervals can be different for "replicating from" and "replicating to" a server.
4. Select the desired replication interval from the menu at the right.
5. Click **OK**.

Uninstalling a Replication Server

To uninstall a replication server, you will have to call the database-stored procedure **delete_replication_server**, which removes the specified ID from the replication set. Be careful not to delete the wrong server, or you may lock yourself out. The details of this procedure are beyond the scope of this guide, but basically you must log into the database with SQL Query Analyzer or Enterprise Manager (or the equivalent SQL 2005 tool) where you should be able to see this stored procedure. You can call the procedure from SQL Query Analyzer or from OSQL with something like:

-   dbo.delete_replication_server(1)

This would delete the BES Server with ID=1.

Switching the Master Server

By default, server 0 (zero) is the master server. BES Administration will only allow you to perform certain administrative tasks (such as creating and deleting users) when you are connected to the master server. If you wish to switch the master to another server, you must set the deployment option **masterDatabaseServerID** to the desired ID. Here is how:

1. Start up the **BES Administration Tool.**
2. Select the **Advanced Options** tab and click the **Add** button.
3. Type masterDatabaseServerID as the name, and then enter the desired ID as the value.
4. Click **OK**.

Once that value has successfully replicated to the new server, it will become the master server. If a server suffers a failure while it is the master, another server will need to be made the master server by direct manipulation of the ADMINFIELDS table in the database. The details of this are beyond the scope of this guide, but broadly speaking, you might use a tool like SQL Enterprise Manager to view and alter the ADMINFIELDS table. Set the variable name masterDatabaseServerID to the desired value.

Managing Bandwidth

File downloads consume the bulk of the bandwidth in a typical BES Installation. You can control this bandwidth by throttling, which limits the number of bytes per second. You can specify the bandwidth throttling on either the BES Server or on the BES Client or on both (in which case the lower of the two values is used). This can be important whenever you have bandwidth issues, as in the following situations:

- A remote office with a thin channel

- Remote dial-in users or users on a slow connection

- A shared channel with higher-priority applications

- A WAN or LAN that is already saturated or has stringent load requirements

Bandwidth throttling settings (and other BES Relay, BES Server, and BES Client settings) can be set using the Tasks from the BES Support site. Select the **Tasks** tab to see the entire task list. You can narrow down the list by selecting **BES Server/Relay Settings** from the filter panel on the left.

For more information About BES Relay/BES Client throttling, please visit http://support.bigfix.com/cgi.

Dynamic Throttling

When a large download becomes available, each link in your BES deployment may have unique bandwidth issues. There are server-to-client, server-to-relay and relay-to-client links to consider, and each may require individual adjustment. As explained in the previous section, it is possible to simply set a maximum value (throttle) for the data rates, and for this there are broad-based policies you can follow. You might, for instance, throttle a BES Client to 2Kb/s if it is more than three hops from a BES Relay. However, the optimal data rates can vary significantly, depending on the current hierarchy and the network environment.

A better technique is to use **dynamic bandwidth throttling**, which monitors and analyzes overall network capacity. Whereas normal throttling simply specifies a maximum data rate, dynamic throttling adds a "busy time" percentage. This is the fraction of the bandwidth that you want to allocate when the network is busy. For instance, you could specify that BES downloads should not use any more than 10% of the available bandwidth whenever BES detects existing network traffic. Dynamic throttling also provides for a minimum data rate, in the case the busy percentage is too low to be practical.

When you enable dynamic throttling for any given link, BES monitors and analyzes the existing data throughput to establish an appropriate data rate. If there is no competing traffic, the throughput is set to the maximum rate. In the case of existing traffic, BES will throttle the data rate to the specified percentage or the minimum rate, whichever is higher.

You control dynamic bandwidth throttling with computer settings. There are four basic settings for each link:

- **DynamicThrottleEnabled:** This setting defaults to zero (disabled). Any other value enables dynamic throttling for the given link.

- **DynamicThrottleMax:** This setting usually defaults to the maximum unsigned integer value, which indicates full throttle. Depending on the link, this value sets the maximum data rate in bits or kilobits per second.

- **DynamicThrottleMin:** This setting defaults to zero. Depending on the link, this value sets the minimum data rate in bits or kilobits per second. This value places a lower limit on the percentage rate given below.

- **DynamicThrottlePercentage:** This setting defaults to 100%, which has the same effect as normal (non-dynamic) throttling. It represents the fraction of the maximum bandwidth you wish to use when the network is busy. It typically has a value between five and ten percent, to prevent it from dominating existing network traffic. (A zero for this setting is the same as 100%.)

As with any other setting, you can create or edit the dynamic bandwidth settings by right-clicking on an item (or group of items) in any computer list and choosing Edit Computer Settings from the context menu.

The specific variable names include the BES Server/Relay settings:

```
_BESRelay_HTTPServer_DynamicThrottleEnabled

_BESRelay_HTTPServer_DynamicThrottleMaxKBPS

_BESRelay_HTTPServer_DynamicThrottleMinKBPS

_BESRelay_HTTPServer_DynamicThrottlePercentage
```

The BES Client settings:

```
_BESClient_Download_DynamicThrottleEnabled

_BESClient_Download_DynamicThrottleMaxBytesPerSecond

_BESClient_Download_DynamicThrottleMinBytesPerSecond

_BESClient_Download_DynamicThrottlePercentage
```

The BES Gathering settings:

```
_BESGather_Download_DynamicThrottleEnabled

_BESGather_Download_DynamicThrottleMaxBytesPerSecond

_BESGather_Download_DynamicThrottleMinBytesPerSecond

_BESGather_Download_DynamicThrottlePercentage
```

NOTE: For any of these settings to take effect, you must restart the affected services (BES Server, Relay or Client).

If you set a BES Server and its connected BES Client to differing maximums or minimums, the connection will choose the smaller value of the two.

Creating Client Dashboards

You can create custom Client Dashboards, similar to those in the BES Console. Dashboards are HTML files with embedded Relevance clauses that can analyze the local computer and print out the current results. BES Clients with a dashboard have an extra tab to display the resulting report.

To create a Client Dashboard, you must create a new folder named __UISupport (note the leading underlines) in the __BESData folder. This is a subfolder of the BES Client folder, so the final pathname looks like:

Program Files/BigFix Enterprise/BES Client/__BESData/__UISupport

Place the Dashboard file (named _dashboard.html) and any accompanying graphics files into this folder. The next time the Client starts up, it will incorporate these files into its interface, adding a tab labeled **Dashboard**. When the user clicks on this tab, the Dashboard will calculate the latest values of each Relevance clause and display them.

The Relevance statements are embedded in the HTML inside special tags with the form:

```
<?relevance statement ?>
```

For instance, to find and print the time, use the following:

```
<?relevance now ?>
```

When the BES Client displays the page containing this statement, the BES Client evaluates the Relevance clause "now" and substitutes the value for the tag. The following sample HTML prints out the word "Date:" and then the current date and time:

```
<html>
 <body>
 Date: <?relevance now ?>
 </body>
</html>
```

To allow the user to refresh the Relevance evaluation, add this line to the file:

```
<html>
 <body>
 Date: <?relevance now ?>
 <A href="cid:load?page=_dashboard.html"> Refresh </A>
 </body>
</html>
```

This link, labeled **Refresh**, causes the page to reload. When it does, it reevaluates the relevance clauses. It is easy to see how you would add other Relevance expressions to this page.

For instance, to print out the OS and the computer name, add these two lines:

```
<html>
 <body>
 Date: <?relevance now ?>
 Operating System: <?relevance name of operating system ?>
 Computer Name: <?relevance computer name ?>
 <A href="cid:load?page=_dashboard.html"> Refresh </A>
 </body>
</html>
```

You can use style sheets to format the output. You can even use the default style-sheet, **offer.css** for some preset formatting. Here is an example of a Dashboard with a title, a header, a refresh link and a section of retrieved property values:

```
<html>
 <head>
   <link type="text/css" rel="stylesheet" href="offer.css"></link>
   <title>BigFix Dashboard Example</title>
 </head>
 <body>

  <div class="header">
   <div class="headerTitle">
     <font size="6"><?relevance computer name ?></font></div>
   <div class="headerCategory">
     <font size="1">(Last updated: <?relevance now ?>)</font><BR>
     <div><font size="1">
       <a href="cid:load?page=_dashboard.html">Refresh</a></font>
     </div>
   </div>
  </div>

  <div class="section">
   <div class="sectionHeader">Computer Information</div>
   <div class="subsection">
     <table>
       <tr> <td valign="top">OS: </td>
            <td><?relevance operating system ?></td></tr>
       <tr> <td valign="top">RAM: </td>
            <td><?relevance (size of ram)/1048576 ?> MB</td></tr>
       <tr> <td valign="top">DNS Name: </td>
            <td><?relevance dns name ?></td></tr>
     </table>
   </div>
  </div>
 </body>
</html>
```

When executed from the BES Client, this dashboard will produce the following output:

To learn more about Relevance expressions, see the *BigFix Relevance Language Reference*.

Geographically Locating BES Clients

Since the BES Clients are often deployed in remote offices, it is useful to create a property that lets the BES Clients report their own location. You can create a location property in BES using the **Location Property Wizard**.

1. In the BES Console, go to **Wizards > Location Property Wizard**. A wizard dialog pops up.
2. The wizard creates a named property allowing the BES Clients to identify themselves based on their subnet, IP range, or other information. Read the instructions in the wizard to create the property.

Viewing Reports over the Web

The **BES Web Reports** component of the BES Server can monitor, print or analyze the status of the local database. It also has the ability to read the databases of other BES Servers and include their data. That offers the administrator a top-level view of a large or far-flung enterprise with multiple database servers and hundreds of thousands of managed computers.

BES Web Reports can be viewed at any time from **Start > Programs > BigFix Enterprise > BES Web Reports** or from the BES Console under **Tools > View Web Reports**.

Aggregating Multiple BES Servers into One Web Reports Server

Any BES Web Report server can be set up to include data from any other BES Server. In order to do so, the program must be able to connect to the other databases using ODBC communications over TCP/IP (i.e., the computers must be on the same LAN or connected by VPN, etc.).

Using a SQL Server Authenticated Account

To set up the BES Web Reports using a SQL Server authenticated account, perform the following steps:

1. From the BES Console, open the BES Web Reports page under **Tools > View Web Reports**.

2. Log into the BES Web Reports as an administrator.

3. Click on the **Databases** tab, and then click on the **Add New Database** link.

4. Enter a Server Name that will identify this database. If connecting through a DSN (Data Source Name), enter the **DSN name**. If connecting through an IP address, select **Use a default DSN-less connection** and type in the IP address of the BES Server you wish to include (e.g., 192.168.100.123 or besserver1.acme.com).

5. There are two ways to provide authentication for your database. The first option is **Windows Authentication**, which is convenient if you have access to the Microsoft SQL Server Enterprise Manager and the servers are in the same domain.

6. Alternatively, you can choose the option labeled **Use Username and Password to login**. With this option, you need to enter the **Username** and **Password** of a user with access to the desired database. You can use your BES Console username and password, or you can use the Microsoft **SQL Server Enterprise Manager** to create a new user who has *total* access to the **AggregatedBy** table and *read* access to all other tables in the BFEnterprise database.

7. Confirm or edit the Web Reports Server **URL**, which will be inserted into this database as an identifier.

Logging Web Reports

You can keep track of your Web Reports usage of by setting up a log file. The name of the log file is stored in the registry. Here is how to set or access the name:

1. Run Regedit and find the **HKey Local Machine\Software\BigFix\Enterprise Server\BESReports** key. You will see some variables and pathnames used by Web Reports. You need to add two values to this key; one for the logging flag, and one for the filename.

2. Create a new DWORD value named LogOn and set it to 1 to turn on logging.

3. Create a new string value named LogPath and set it to the full pathname of your desired log file, e.g. "C:\fullpath\file.txt".

The next time you launch Web Reports, a log of the session will be saved to the specified file.

HTTPS Configuration

To provide more security to Web Reports, you can use HTTPS instead of HTTP to make your browser connection. To use HTTPS, you must have a proper SSL certificate. The SSL certificate should be in standard OpenSSL PKCS7 (.pem) file format. If the certificate meets all of the trust requirements of the connecting browser, then the browser will connect without any interventions by the user. If the certificate does not meet the trust requirements of the browser, then the user will be prompted with a dialog asking if it is OK to proceed with the connection, and provided with access to information about the certificate. Typically, a trusted certificate is one which is signed by a trusted authority (e.g., Verisign), contains the correct host name, and is not expired. The .pem file is your SSL certificate, which you must obtain through your favorite CA. If you don't require authentication back to a trusted root, you can also generate a self-signed certificate with the OpenSSL utilities (see http://support.bigfix.com/cgi-bin/kbdirect.pl?id=359 for more information). Once you have a certificate, place it on the computer running web reports (usually the BES Server) and follow these directions:

1. Run **regedit** and locate HKEY_LOCAL_MACHINE\Software\BigFix\EnterpriseClient\Settings\Client. You need to add or modify three subkeys; one for the HTTPS flag, one for the location of the SSL certificate, and one for the HTTPS port number.
    Note: For x64 systems, the key will be here:
    HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\EnterpriseClient\Settings\Client

2. Create a new sub-key of **Client** called _WebReports_HTTPServer_UseSSLFlag (it may already exist).

3. Create a new string value (reg_sz) for the key _WebReports_HTTPServer_UseSSLFlag called **value** and set it to 1 to enable HTTPS.

4. Create a new sub-key of **Client** called _WebReports_HTTPServer_SSLCertificateFilePath (it may already exist).

5. Create a new string value (reg_sz) for the key _WebReports_HTTPServer_SSLCertificateFilePath called **value** and set it to the full path name of the SSL certificate (cert.pem).

6. Create a new sub-key of **Client** called _WebReports_HTTPServer_PortNumber (it may already exist).

7. Create a new string value (reg_sz) for the key _WebReports_HTTPServer_PortNumber called **value** and set it to port number you would like to use (typically 443).

8. Update the Web Reports URL to use https:// instead of http:// and Port 443 instead of Port 80. You can do this by editing the URL string within Web Reports. To do this, from the Overview page select the **Databases** link. Then select the **Edit Database** link under the appropriate database. Then you can modify the entry for **Web Reports URL**.

9. Restart the **BESWebReports** Service.

Managing and Maintaining BES

Now that you have installed the BES components and customized the configuration to suit your own needs, this section explains how to maintain and manage your BES installation.

Adding New Operators and Master Operators

There are two classes of operator for the BES Console: Ordinary Operators and Master Operators.

- **Ordinary Operators** manage a subset of the BES Clients based on their management rights and have restricted privileges to administer BES functions.

- **Master Operators** have the ability to manage all the BES Clients and can also assign management rights to other operators.

The Site Administrator has the most important primary key (license.pvk), and can do anything a Master Operator can. However, it is bad practice to use your site key for ordinary operations. Instead, create a Master Operator account and use that key (publisher.pvk) exclusively for Console operations. To add new Operators and Master Operators to the BES system, simply repeat the steps outlined in **Adding BES Console Operators** (page 47).

Assigning Management Rights

In a typical BES deployment, there will be anywhere from a couple hundred to a couple hundred thousand computers reporting to a single BES Server. At these scales, it is often important to separate out which computers can be controlled by different BES Console operators for organizational and security reasons.

BES allows you to break down management rights into separate sections based upon geography, department, computer type (servers vs. workstations), or any other property. Each BES Console operator can be assigned management rights to the appropriate computers. All of this is done by assigning computers to operators based on computer properties. For instance, you could allow a member of a server team to control all computers that have server-based operating systems in the company datacenter. First specify which subnets are in the datacenter, then any computer in that subnet with a server OS will be managed by the given operator.

Using this approach, the operators can see a subset of computers and will not be able to see information or change anything on computers that they do not manage. When they view the BES Console or BES Web Reports, it appears to them that they have their own BES Server with no other computers.

Because different operators can be assigned to overlapping groups of computers, any kind of configuration is possible. BES Console operators only receive information from their assigned computers, improving manageability and responsiveness.

Here is how to **Add** or **Delete** management rights:

1. Log in to the BES Console as a Master Operator.

2. Click on the **Console Operators** tab (if this choice is not available, you may not have the proper authorization to perform this command). You will see a filter/list of BES Console operators.

3. Right-click on a single operator from the list and select **Assign User Management Rights** from the pop-up menu.

4. If user rights have already been set for this user, you will see them here. Click the **Add** button to assign management rights to the selected operator. (You can also *revoke* specific management rights using this dialog box by clicking on the **Delete** button.)

5. Use the filter panel on the left to narrow down the computers you want to assign to this operator. By shift- or ctrl-clicking on items in the **Retrieved Properties** or **Group** folders, you can specify a set of computers that share common properties or settings. As new computers are added to the network, they will automatically be classified by their retrieved properties or group, and the proper BES Console operators will automatically be assigned to manage them.

NOTE**:** If you grant a user access to computers with a specific retrieved property value and the property value changes, then the user will no longer have access to those computers. For instance, if you assign a user permissions on a certain subnet and a laptop moves to a different location with a different subnet, the user will no longer be able to administer the laptop unless it comes back to the original office.

6. Click the **OK** button.

Changing a Publisher Password

Any console operator can change their publisher credential password from the BES Console:

1. Select **Manage Signing Keys** from the **Tools** menu.
2. Click the **Change Password** button at the bottom of the dialog.
3. Type in your old password to authenticate yourself, then enter your new password and confirmation.

Note that the publisher password and database passwords are normally created as the same password, but they can be different if desired.

Changing a BES Database Password

You can change your database password from the BES Console.

1. Select **Change Database Password** from the **File** menu (you must have the proper permissions to select this item).
2. Type in your old password to authenticate yourself, and then enter your new password and confirmation.

Note that the publisher password and database passwords are normally created as the same password, but they can be different if desired.

Removing a BES Console Operator

When an employee leaves, you will want to delete their access rights to the BES database. This is done with the **BES Administration Tool**:

1. Launch the program by selecting **Start > Programs > BigFix Enterprise > BES Administration Tool**.

2. Select a user from the list, and click **Remove User**.

3. When you have deleted the desired operator, click **OK.** This will remove that operator's privileges from the database, stop all of the user's pending actions and notify the BES Clients that the private keys from that user are no longer valid.

4. You will be prompted to propagate the action site masthead to reflect the user changes. Click **Yes** to continue.

5. Enter your private key password and click **OK**.

Using NT Authentication

By default, BES Consoles create an ODBC connection to the SQL database, and the DSN is set to use SQL authentication. You can change this DSN to use NT authentication through the Windows ODBC Data Source Administrator. Doing so will cause the BES Console to ask the current Windows user to authenticate with the SQL Server. For more information, see the article at http://support.bigfix.com/cgi.

Managing Client Encryption

Server and Relay-bound communications from BES Clients (version 7.1 and greater) can be encrypted to prevent unauthorized access to sensitive information. To enable it, you must generate a key and provide a setting value. The setting is accomplished in the BES Console and is described elsewhere in the section labeled **Enabling Encryption on BES Clients**. The key is generated from the **Encryption** tab of the BES Administration Tool:

1. Launch the **BES Administration Tool** by selecting **Start > Programs > BigFix Enterprise > BES Administration Tool**.

2. Select the **Encryption** tab.

At the top of the dialog is a statement of the current state (in this example: **Report encryption is currently DISABLED**). BES Client encryption has four states, Disabled, Pending, Enabled and Pending Rotation:

- **Disabled**: This state indicates that no encryption certificate is included in your deployment masthead, which means that Clients cannot encrypt their reports even if they are told to do so. Click on **Generate Key** to create an encryption certificate (and the corresponding private key which can be used to decrypt reports at the receiving end). This will cause you to enter the **Pending** state.

- **Pending**: In this state, an encryption certificate has been generated and is ready for deployment, but the private key has not yet been distributed to all necessary decrypting relays and servers. Once you have manually distributed the private key, click on the **Enable Encryption** button to embed the certificate in the masthead and send it out to all clients. At that point, you will enter the Enabled state. You can also click **Cancel** to return to the Disabled state.

- **Enabled**: In this state, an encryption certificate has been found in your deployment masthead, which means that you are able to turn on encryption (using the setting discussed previously) for any of the clients in your deployment. At any time, you can click on **Generate new key** to create a new encryption certificate. This is useful if you have a key rotation policy or if your encryption key is ever compromised (see next section). Generating a new key returns you to the Pending state (unless you elect to deploy immediately as described in the next section). You can also click **Disable** to move back to the Disabled state.

- **Pending Rotation**: In this state, an encryption certificate is included in your deployment masthead, and a new certificate has been generated and is ready to replace the existing certificate.

Generating a New Encryption Key

Should your private key be compromised or if you have a policy of rotating keys, you can easily generate a new key from the **BES Administration Tool**. Here is how:

3. Launch the **BES Administration Tool** by selecting **Start > Programs > BigFix Enterprise > BES Administration Tool**.
4. Select the **Encryption** tab.
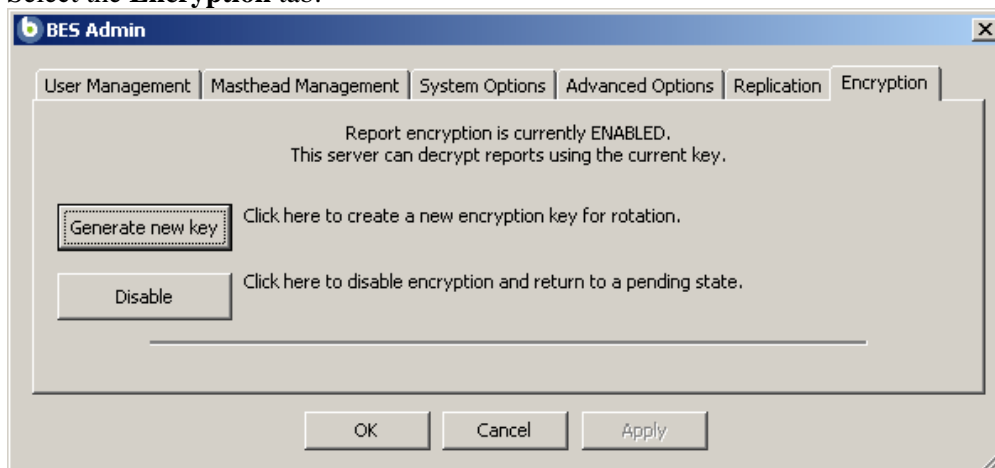
5.   Click the **Generate new key** button. The Create Encryption Credentials dialog opens.

6.   From this dialog, select the key size. The default is 2048, which is adequate for most purposes. Check the box to use this key immediately. However, if you have established BES Relays that use encryption, you should leave this box unchecked until you can distribute the new key to those Relays.

7.   Click **OK** to distribute this new key to your BES Clients. You must provide your Site Admin Private Key to propagate the Action. A final dialog will ask for confirmation. For more information, on encryption key sizes and server requirements, see the knowledge-base article at http://support.bigfix.com/bes/install/serverreq71.html.

Creating Top-level Decrypting BES Relays

When an Action is deployed, thousands of BES Clients may report back in a short time-frame, typically to a BES Relay. If you have elected to encrypt these reports, the Relay will bundle the reports together and pass them up to the BES Server, which must then split up and decrypt each one of them. With many thousands of BES Clients, this can impose a significant computational burden on the BES Server.

To improve performance, you can lighten the load on your BES Server by allowing your top-level BES Relays to do the bulk of the decryption. If you have over 50,000 BES Clients, you may be able to substantially reduce the load on your BES Server by moving decryption down into the relay chain. If the BES Relay has its own decryption key, it can first decrypt the client messages into plain text and then bundle thousands of them into a single archive. This can then be compressed, encrypted and passed up to the BES Server. At that point, the server can perform a single decryption on the entire archive, noticeably reducing its overhead.

To spread the decryption duties, you simply need to distribute your encryption keys to your top-level BES Relays. For normal server-level encryption, BigFix creates an encryption key for you and places it in the BigFix program folder:

- C:\Program Files\BigFix Enterprise\BES Server\Encryption Keys

To allocate the load to your top-level BES Relays, place the encryption key in the equivalent BES Relay directory:

- C:\Program Files\BigFix Enterprise\BES Relay\Encryption Keys

These top-level BES Relays will decrypt all the documents received, bundle them together and then re-sign them with a single signature. You can put as many keys as you want in the folder and the BES Relay will attempt to use each of them when it gets an encrypted client report. Clients encrypt against the key found in the masthead file which should be the last key created. However, it is possible that a BES Client will transmit a report with an older version of the masthead (and thus a different encryption key) if it hasn't gathered the latest Action site for any reason.

There are a few considerations:

- You must manually transfer the key file from the server to the relay every time you create a new encryption key.

- During the transfer process, it is important not to expose your private key file. This means you shouldn't just move the key over the internet because anyone listening might be able make a copy of your private key file. Therefore it is best to physically transfer the key from one computer to another, for instance with a USB key.

- During the encryption key creation process, you have the option to create the private key file but not propagate it out in the masthead. This step allows you time to transfer the new key file to the BES Relays before clients start posting encryption messages with that key.

Managing Downloads

BigFix uses several methods to ensure that downloads are efficient and make the best use of available bandwidth. Among other techniques, caching is used extensively by all the BES elements, including Servers, Relays and Clients.

When an Action on a BES Client needs to download a file, the local cache is checked first. If the Client can't find it locally, it requests the file from its parent, typically a BES Relay. When the file is requested, the Relay checks it own cache. If it finds the file, it immediately sends it down to the requesting Client. Otherwise, it passes the request up to its parent, which may be another BES Relay and the process continues. Ultimately, a BES Server retrieves the file from an internal server or the Internet, caches it and then passes it back down the chain. After receiving the file, each Relay in the chain caches it, and continues to forward it down to the original BES Client, which also caches it.

Each cache retains the file until it runs out of room. At that point, the cache is purged of the least-recently used (LRU) files to provide more space. You can view the BES Relay cache size and other BES Relay information by activating the **BES Relay Cache Information** Analysis available from the BES Support Fixlet site. The default cache size is 1 GB, but it can be changed by using the **BES Relay/BES Server Setting: Download Cache Size Task**, also from the BES Support Fixlet site.

There may be situations that require files to be manually downloaded and cached, typically because such files are not publicly available, in which case you must download the files directly from the source. You can pre-populate the download cache by copying files to the download cache location. You can also clear these files out manually if you wish.

The caches are stored as subfolders of the BigFix Enterprise folder, which is created by default at **C:\Program Files\BigFix Enterprise**. The Server download cache is **BES Server\wwwrootbes\bfmirror\downloads\sha1**, and the Client download cache is found at **BES Client__BESData__Global__Cache\Downloads**. For security purposes, each file you save must be named with the sha1 hash value of the file. If the filename doesn't match the sha1, the file will be ignored.

As well as the download cache, BES Relays maintain an Action cache (also 1 GB) holding all the files needed for each Action, and BES Clients maintain a Utility cache.

For information about troubleshooting Relays, including bandwidth and downloading, see the KB article at http://support.bigfix.com/bes/misc/besrelayhealth.html.

Dynamic Download White-lists

A new feature called dynamic downloading has been added to version 7.2 of BigFix to extend the flexibility of Action scripts. Dynamic downloading adds the ability to use relevance clauses to specify URLs.

As with static downloads, dynamic downloads must specify files with the confirmation of a size or sha1. However, the URL, size, and sha1 are allowed to come from a source outside of the Action script. This outside source may be a manifest containing a changing list of new downloads. This technique makes it easy to access files that change quickly or on a schedule, such as antivirus or security monitors.

This flexibility entails extra scrutiny. Since any client can use dynamic downloading to request a file, it creates an opportunity for people to use your server to host files indiscriminately. To prevent this, dynamic downloading uses a white-list. Any request to download from a URL (that isn't explicitly authorized by use of a literal URL in the action script) must meet one of the criteria specified in a white-list of URLs on the BigFix server, located at **<BES Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt**. This file contains a newline-separated list of regular expressions using a Perl regex format, such as the following:
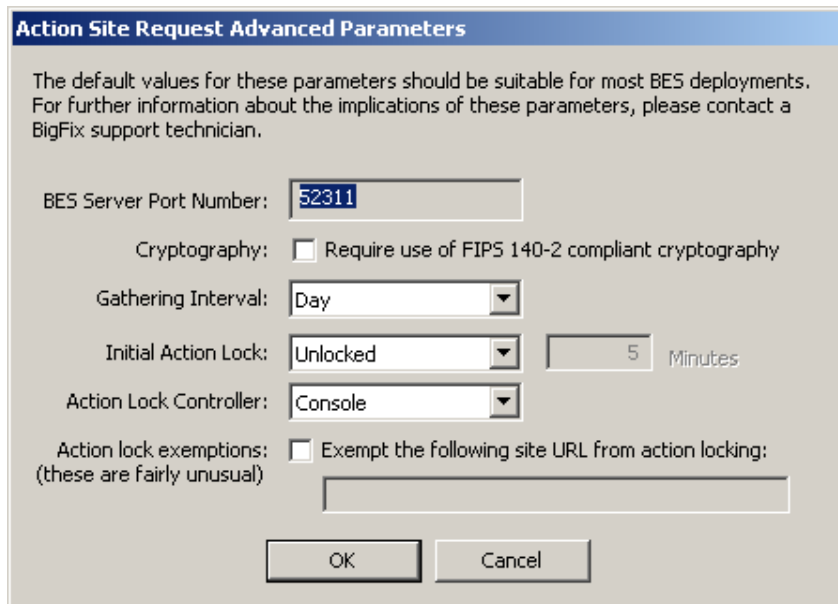
```
http://.*\.site-a\.com/.*

http://software\.site-b\.com/.*

http://download\.site-c\.com/patches/JustThisOneFile\.qfx
```

The first line is the least restrictive, allowing any file at the entire site-a domain to be downloaded. The second line requires a specific domain host and the third is the most restrictive, limiting the URL to a single file named "JustThisOneFile.qfx". If a requested URL fails to match an entry in the white-list, the download immediately fails with status NotAvailable. A note is made in the Relay log containing the URL that failed to pass. An empty or non-existent white-list will cause all dynamic downloads to fail. A white-list entry of ".*" (dot star) will allow any URL to be downloaded.

Editing the Masthead

You can change certain default parameters stored in the masthead for the BES system by using the **BES Administration Tool**. Here is how:

1. Launch the program from Start > Programs > BigFix Enterprise > BES Administration Tool.
2. Browse to the location of your site license and click **OK**.
3. Select the **Masthead Management** tab.
4. Click the **Edit Masthead** button.

NOTE: It is recommended you keep the default settings on this page unless you have a specific reason to change them. Improper settings can cause BES to work in non-optimal ways. Consult with a support technician for more details.

5. The parameters you can edit include:

    - **BES Server Port Number:** In general, you will not want to change this number. In addition, if you decide to change this number *after* deploying the BES Clients, BES will not work correctly. See **Modifying Port** Numbers, below.

    - **Cryptography:** Check this box to implement the Federal Information Processing Standard on your network. This changes the masthead so that every BES component attempts to go into FIPS mode. By default, the client will continue in non-FIPS mode if it fails to properly enter FIPS, which may be a problem with certain legacy operating systems. Be aware that checking this box can add 3-4 seconds to the BES Client startup time.

    - **Gathering Interval:** This option determines how long the BES Clients will wait without hearing from the BES Server before they check whether new content is available. In general, whenever the BES Server gathers new content, it attempts to notify the BES Clients that the new content is available through a UDP connection, circumventing this delay. However, in situations where UDP

is blocked by firewalls or where network address translation (NAT) remaps the IP address of the BES Client from the BES Server's perspective, a smaller interval becomes necessary to get timely response from the BES Clients. Higher gathering rates will only slightly affect the performance of the BES Server, because only the differences are gathered – a BES Client does not gather information it already has.

- **Initial Lock state:** You can specify the initial lock state of all BES Clients. Locked BES Clients will report which Fixlet messages are relevant for them, but will not apply any actions. The default is to leave them unlocked and to lock specific BES Clients later on. However, you may wish to start with the BES Clients locked and then unlock them on an individual basis in order to give you more control over newly installed BES Clients. Alternatively, you can set them to be locked for a certain period of time (in minutes).

- **Action Lock Controller:** This parameter determines who can change the action lock state. The default is **Console**, which allows any BES Console operator with management rights to change the lock state of any BES Client in the network. If you wish to devolve control over locking to the end user, you may select **Client**, but this is not recommended.

- **Action Lock Exemptions:** In rare cases, you may need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL.

6.   Click **OK** to enter the changes.
7.   Enter your site password at the prompt.

NOTE: The masthead changes do NOT affect BES Clients that are already deployed, but you can export the masthead using the BES Admin tool and replace the masthead in the BES Server so that BES Clients deployed with the new masthead will use these changes.

Modifying Port Numbers

The BES Console and BES Server communicate using ODBC, which operates on port **1433** by default. For more information about changing this port please ask your database administrator.

By default, the BES Server uses port **52311** to communicate with the BES Clients, but any port number can be chosen (although you should avoid the reserved ports between 1-1024 because of potential conflicts and difficulty managing network traffic).

Your choice of the BES Server Port Number is factored into the generation of the masthead, which specifies URLs for the action, registration, reporting, and mirror servers. As a consequence, you must finalize your port number *before installation*.

Modifying Global System Options

The BES Admin Tool allows you to modify a few basic system defaults, such as the minimum refresh, Fixlet visibility and the Client UI Icon. Here is how:

1. Launch the BES Admin Tool from Start > Programs > BigFix Enterprise > BES Administration Tool.

2. Select the **System Options** tab.

3. At the top, you can set the global **Minimum Refresh**. The default is 15 seconds, which is a good trade-off between responsiveness and low network load. If you find that BES communications are impacting your network, you can raise the minimum to 60 seconds or more.

4. External sites are visible to all Console operators by default, but you can change that in the section marked **Default Fixlet Visibility**. Click the lower button to make external content invisible to all but Master Operators.

5. Starting with BES 7.0, you can customize the Client User Interface with your own logo. You can use any graphic you choose, but because it is a global setting, corporate branding is typical. When you present your BES Clients with a message or an offer, they will see the icon you supply in the title bar, as well as the tray and task bar. The icon file should have several images of different sizes. The first image in the file should be a 64 x 64 image with transparency and will be used in the body of the dialogs. The title bar and task bar icons are chosen by size, targeting the size indicated by system metrics SM_CXICON and SM_CYICON. These are typically 16 or 32. The icon file should be created according to Microsoft's procedure for creating a Windows XP icon with transparency. Click the **Add Icon** button to browse for an appropriate icon (.ico) file.

Scheduling Replication

If you have multiple BES Servers in your deployment, you can schedule when each will replicate. The default is five minutes, but you can shorten the time for greater recoverability or increase it to limit network activity. Here is how:

1. Launch the BES Admin Tool from Start > Programs > BigFix Enterprise > BES Administration Tool.

2. Select the **Replication** tab.

3. Click the Refresh button to see the latest **Replication Graph**.

4. Select the IP Address of a BES Server and then choose the desired replication time.

Extending the BES License

When you first request your action site license, your query is archived with BigFix, Inc. and you are issued a license for a specific period of time. Before your license expires, BES will warn you, giving you sufficient time to renew your license. When you are coming close to the expiration date, BES will notify you using a Fixlet message. Similarly, if you start to exceed the number of BES Clients allocated by your license, BES will alert you. To extend your license expiration or add new BES Client licenses to your installation, follow these steps:

1.   Notify your BigFix support technician (if you have not paid for the extended license, you will need to talk to your sales person or reseller to buy an extended license), who will send you a new action site certificate (license.crt).

2.   Run the BES Administration Tool (**Start > Program Files > BigFix Enterprise > BES Administration Tool**).

3.   Specify the location of the site signing key and click **OK**.

4.   Click the **Masthead Management** tab.

5.   Click the **Activate Masthead** button.

6.   Browse to your **license.crt** file and import it.

7.   Enter the site password to propagate the file. Your new license extensions will be added to the database.

Recreating Site Credentials

Private/public key encryption creates a chain of signing authority from the BigFix root down through the BES Site Administrator and including each BES Console operator. If you lose your site credential or change the IP address of your BES Server, the chain is broken. The consequences are serious: you must start over with a new request to BigFix, Inc. for a site certificate. Then you must re-install the entire system, including all the BES Clients (contact your support technician for details on how you might migrate your BES Clients to a new BES Server) and re-create all the users. If this happens, please contact your support technician. To protect your site certificate, obey these important rules:

- **Do not lose the private key for your site** (saved in the file named **license.pvk**). Follow standard procedures for backing up and securing critical confidential information.

- **Do not change the IP address/hostname or port number of the BES Server**, since it is the primary identifier for your site certificate. Any change to the IP address or port number that was specified when the license was requested negates the license and will necessitate a fresh installation of the BES system. If you plan to decommission a BES Server, be sure to apply the same IP address and port number to the replacement server.

- **Do not forget your password.** Follow your corporate standards for noting and storing your password.

NOTE: The BES Site Administrator can change the password of the site-level key, provided he or she knows the current password.

Updating the BES Software

Like the other software installations in your enterprise, the BES software itself will need to be maintained and updated on occasion. Fortunately, that capacity is built into the system. To guarantee that you are running the latest version of BES, be sure to install the BES Client on all BES Server and BES Console computers. Whenever an update is issued, a Fixlet message will be delivered to you with everything you need to install the update. If, for whatever reason, you do not wish to use the Fixlet messages to automatically update the BES components, you can choose to manually update each BES component. Instructions on how to do this will be included in the upgrade Fixlet message or will be available from your support technician.

BigFix Announcements

BigFix maintains a mailing list to announce new products, updates, informational notices, and other information useful to BES Administrators. BigFix highly recommends that all BigFix customers subscribe to the BES Administrator announcements mailing list at:

http://bigmail.bigfix.com/mailman/listinfo/besadmin-announcements.

Changing the Client Icon

By default, the icon in the upper left corner of the Client UI is the BigFix logo. This same icon appears in the tray when an Action is pending and in the task bar when the program is running. You can change this icon to help you clarify to your end users who is the source of the action, and also to comply with corporate branding and trademark requirements. Here is how to change the icon:

1. Run the BES Administration Tool (**Start > Program Files > BigFix Enterprise > BES Administration Tool**).
2. Click the **System Options** tab.
3. Click the **Change Icon** button and use the **Open** dialog to browse for your icon (.ico) file.

The Administration Tool will immediately propagate this graphic to the Clients, but it will not be incorporated into the interface until the Client restarts. After that, when a Client interface appears (in response to an action, a dashboard or an offer), it will include the graphic icon you specified.

Maintaining and Troubleshooting BES

If you are subscribed to the **Enterprise Security Site** (Patches for Windows), you will be able to ensure that you have the latest upgrades and patches to your SQL Server or MSDE database servers. That means that you must install the BES Client on all your computers, including the BES Server and BES Console computers. In addition, you may want to take advantage of these other tools and procedures:

- If you have the SQL Server installed, you should become familiar with the **MS SQL Server Tools**, which can help you keep the database running smoothly.

- It is standard practice to back up your database on a regular schedule, and the BES database is no exception. It is also wise to run the occasional error-check to validate the data.

- If you start to notice any performance degradation, check for fragmentation. BES writes out many temporary files, which may create a lot of disk fragmentation, so defragment your drive when necessary. Of course, regular maintenance also involves running the occasional error-check on your disk drives as well.

- The **BES Diagnostics Tool** performs a complete test on the server components and can be run any time you experience problems. See **Running the BES Diagnostics**, page 30.

- Check the BES Support Fixlet site often. There are a number of Fixlets available that can detect problems with any of your BES components. This can often head off problems before they ever affect your network.

- Check the BigFix Knowledge Base at http://support.bigfix.com/. This site is continually updated, and if you cannot find an existing knowledge-base article about your question, you can find information on how to submit a question to a BigFix support technician.

- Add BES Relays to improve the overall system performance and pay close attention to them. Healthy BES Relays are key to a healthy BES deployment.

- Review the **Deployment Health Checks** dashboard for optimizations and failures.

- Set up monitoring activities on the BES Server(s) to notify you in the event of a software or hardware failure, including:

- BES Server powered off or unavailable

- Disk failure

- Event log errors about BES Server applications

- BES Server services states

- FillDB buffer directory data back-up situations

Deployment Scenarios

The next few pages contain deployment scenarios that illustrate some basic configurations taken from actual case studies. Your organization will look similar to one of the examples below, depending on the size of your network, the various bandwidth restrictions between clusters and the number of Relays and Servers. The main constraint is not CPU power, but bandwidth.

Pay careful attention to the BES Relay distribution in each scenario. Relays provide an dramatic improvement in bandwidth and should be thoughtfully deployed, especially in those situations with thin pipes.

BES Relays are generally most efficient in fairly flat hierarchies. A top-level BES Relay directly eases the pressure on the BES Server, and a layer under that helps to distribute the load. But hierarchies greater than two tiers deep may be counterproductive and must be carefully deployed. Multiple tiers are generally only necessary when you have more than fifty BES Relays. In such a case, the top tier BES Relays would be deployed on dedicated servers which would service anywhere from 50-200 second-tier BES Relays. The following examples will help you deploy the most efficient network layout.

Notice that additional BES Servers can also add robustness to a network, by spreading the load and supplying redundancy. Using redundant BES Servers allows failbacks and failovers to be automated, providing minimal data loss, even in catastrophic circumstances.

With the proper deployment of BES Servers and BES Relays, networks of any size can be accommodated. Beyond the examples we present here, your BES support technician will be happy to help you with other configurations.

Basic Deployment

This is a vastly simplified deployment designed to point out the basic hierarchy and the ports used to connect the components.
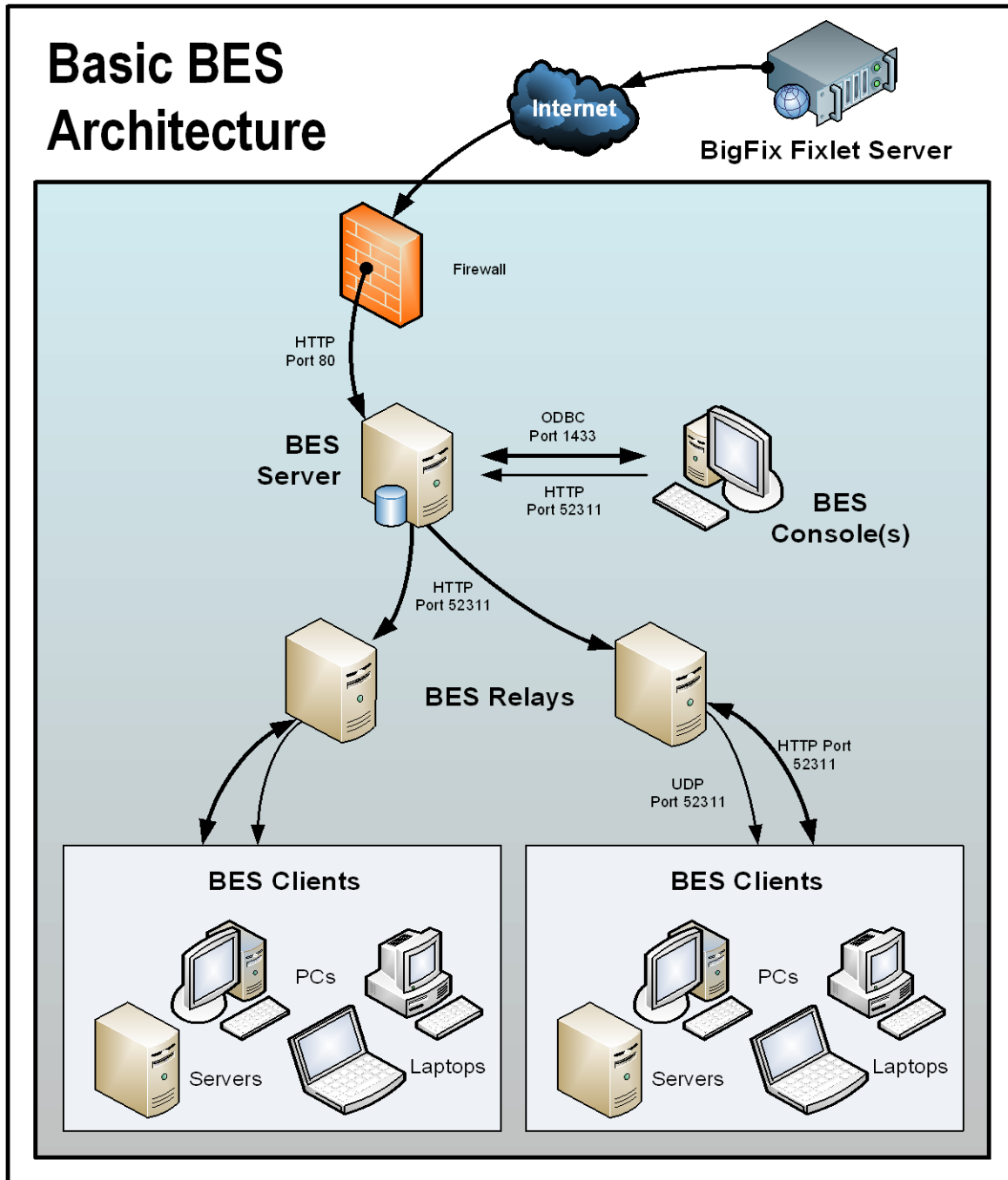
Note the following about the diagram:

- Information comes in from the Internet (across the firewall), but does not go out.

- Port 80 is used to collect Fixlet messages over the Internet from Fixlet providers such as BigFix.

- A dedicated port (defaulting to 52311) is used for HTTP communications between BES Servers, Consoles, Relays and Clients.

- You need both an ODBC and an HTTP connection to run the BES Console.

- BES Relays are used to share the server load. This diagram only shows two BES Relays, but you can use dozens or even hundreds of BES Relays in a similar flat hierarchy. Typically a BES Relay is deployed for every 500-1,000 computers.

- The BES Relays require an HTTP port (defaulting to 52311) to communicate with the BES Clients.

- The BES Relays can also take advantage of a UDP port to alert the BES Clients about updates, but this is not strictly necessary.

- The BES Clients are typically PCs or Workstations, but can include other servers, dockable laptops and more. Any device that can benefit from patches and updates is a candidate to include in the BigFix deployment.

BES has far greater flexibility and potential than this simple case suggests. It is capable of overseeing hundreds of thousands of computers, even if they are spread out around the world. The next scenarios build on this basic deployment.

Main Office with Fast-WAN Satellites

This configuration is common in many universities, government organizations, and smaller companies with only a few geographical locations. This type of deployment is relatively easy to set up and administer because there are no (or very few) slow WAN pipes to worry about.
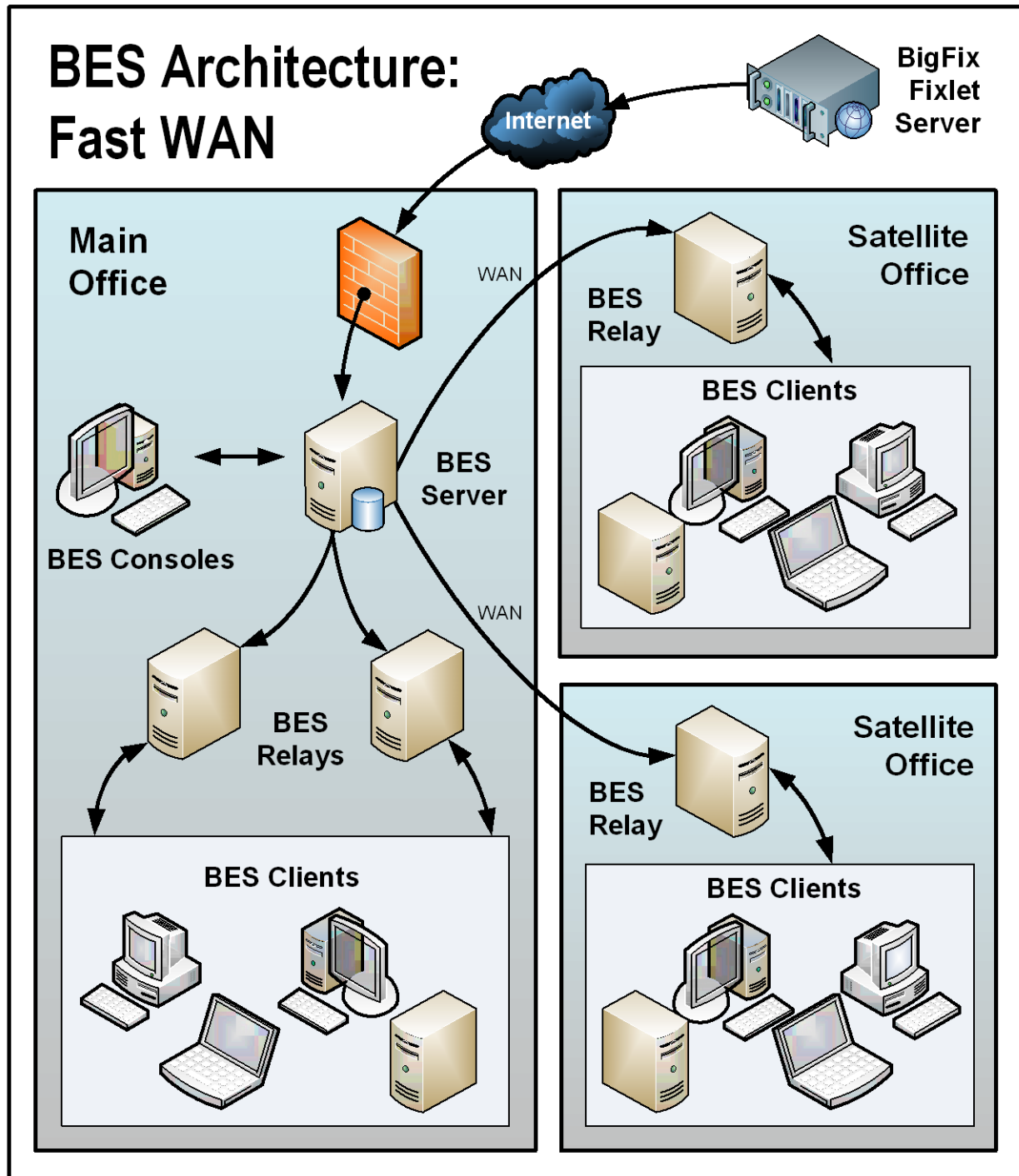
Note the following about the diagram:

- In this configuration, the BES Relays are used both to relieve the BES Server and to distribute the communications, optimizing the bandwidth.

- This scenario has large WAN pipes, so office relays can communicate directly to the main BES Server. A thin WAN could force a change in the layout of the BES Relays (see the scenarios above and below).

- The more BES Relays in the environment, the faster the downloads and response rates.

- Because of the nature of this network, when the BES Clients are set to **Automatically Locate Best BES Relays**, many of the BES Relays are the same distance away. In this scenario, the BES Clients automatically load-balance themselves amongst all the BES Relays that are nearby.

- For this high-speed LAN, a relatively flat hierarchy is recommended, with all BES Relays reporting directly to the main BES Server. Any extra levels in the hierarchy would only introduce unnecessary latency. However, if there were over 50-100 BES Relays in this environment, another level of BES Relays should be considered.

Distributed Server Architecture Setup

Companies with sensitive or high availability needs will want to deploy multiple, fully-redundant servers to maintain continuous operation even in the face of serious disruptions. Multiple BES Servers also help to distribute the load and create a more efficient deployment. Here is a bare-bones diagram of how multiple servers might be set up in a single location or in two widely separated offices:
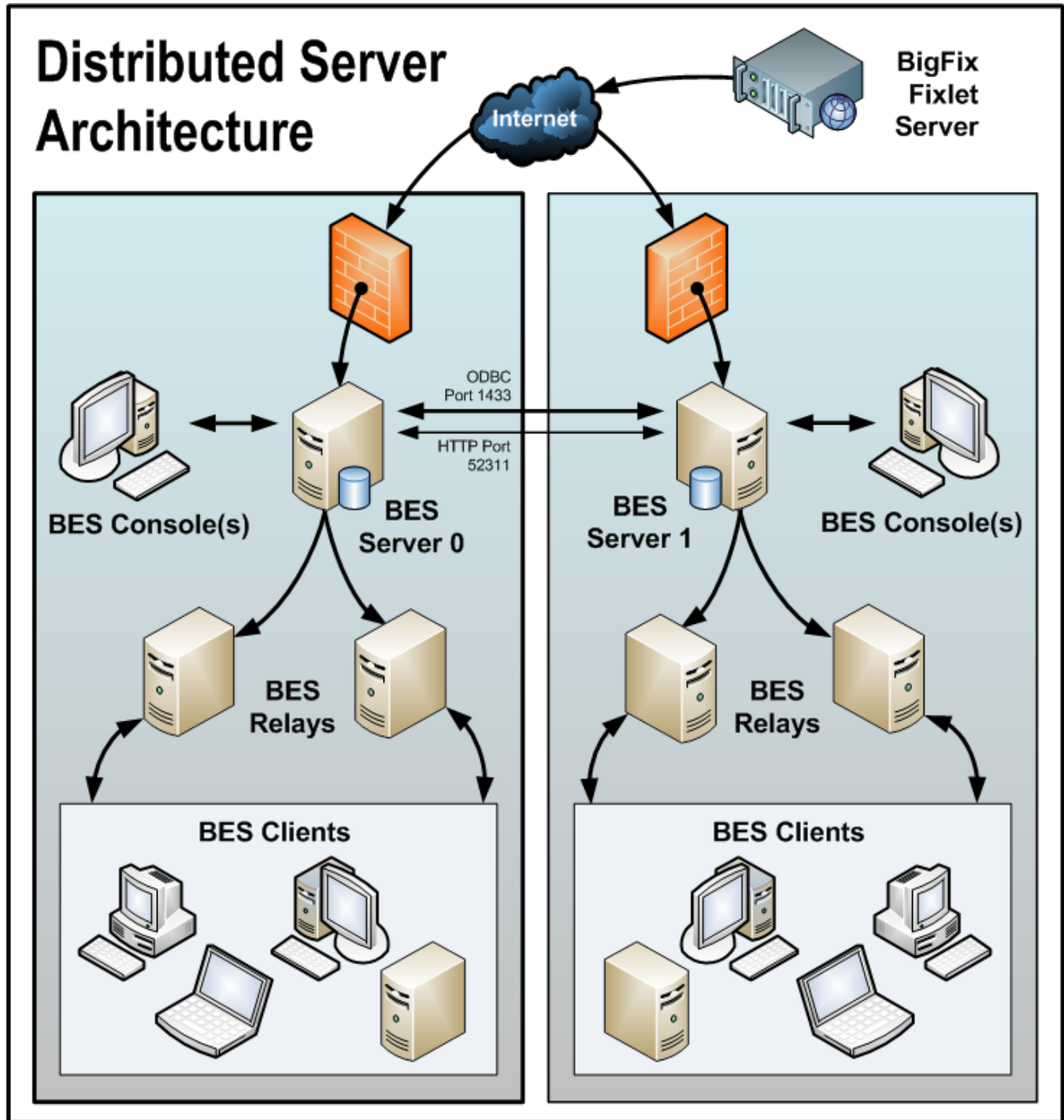
Note the following about the diagram:

- The BES Servers are connected by a fast WAN, allowing them to synchronize several times per hour.

- The servers need both an ODBC and an HTTP link to operate and replicate properly.

- There is a primary BES Server with an ID of 0 (zero). It is the first BES Server that you install, and it is the default server for running BES Administration.

- For the sake of clarity, this is a minimal configuration. A more realistic deployment would have a top-level BES Relay and other WAN connections to regional offices.

- The BES Servers and Relays are configured so that control can be automatically routed around a server outage (planned or otherwise), and upon failover reconnection, the databases will be automatically merged.

- The BES Servers communicate on a regular schedule to replicate their data. You can review the current status and adjust the replication interval through BES Administration > Replication. For the best possible performance, these pipes should be fat.

- This diagram only shows two BES Servers, but the same basic architecture would apply to each additional server. With multiple servers, a shortest-path algorithm is used to guide the replication.

- When an outage or other problem causes a network split, it is possible to for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected on failover, precedence will go to the version on the server with the lowest BES Server ID.

Efficient BES Relay Setup

To increase efficiency and reduce latency, this company has set up a hierarchy of BES Relays to help relieve the server load. Each BES Relay they add takes an extra burden off the BES Server for both patch downloads and data uploads. Setting up BES Relays is easy, and the BES Clients can be set to automatically find the closest relay, further simplifying administration.
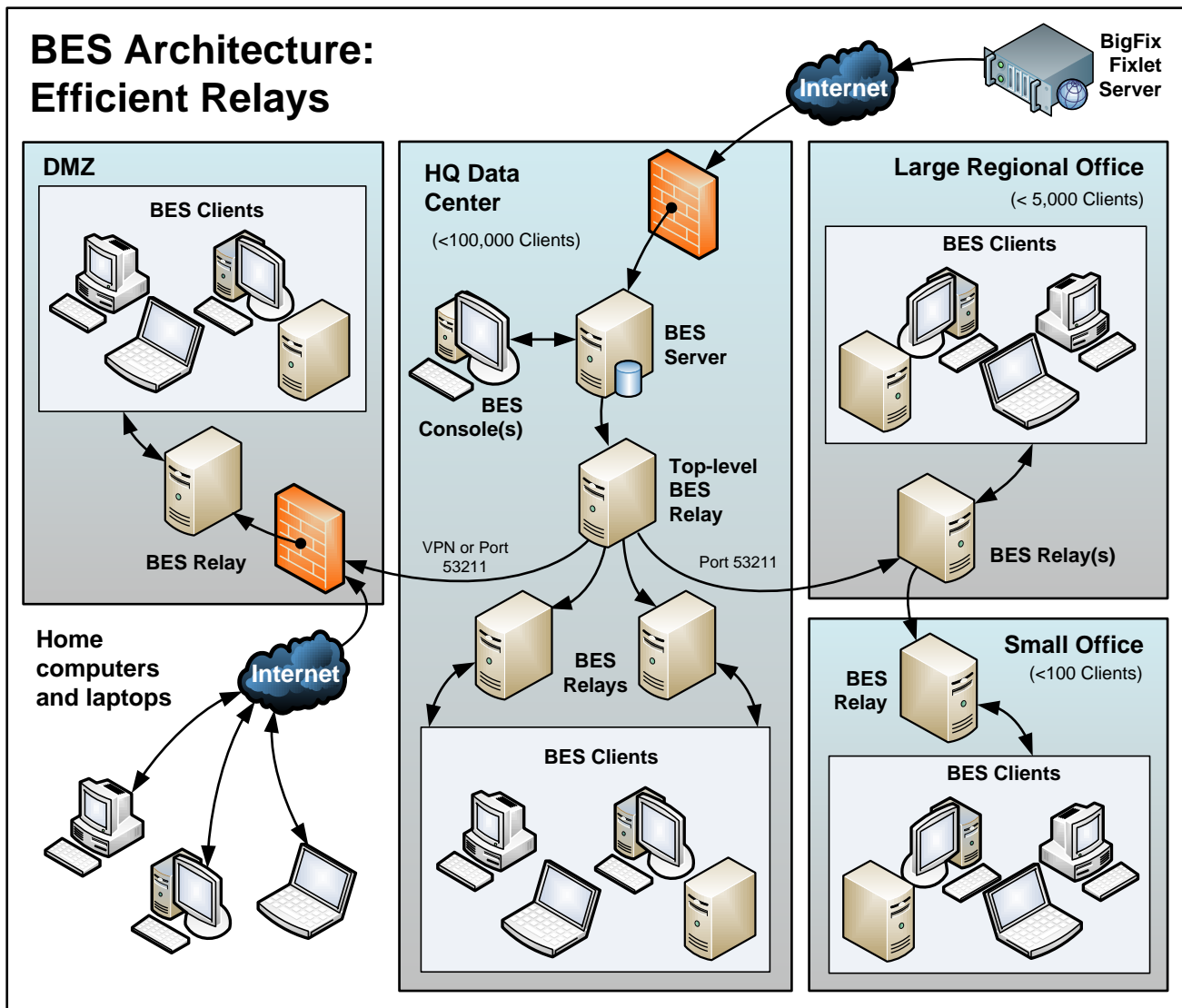
Note the following about the diagram:

- There is a dedicated server computer known as the Top-Level BES Relay that is used to take the load off of the BES Server computer.

- All BES Relays are manually configured to point to either the top level BES Relay or to another BES Relay that is closer. The general rule for configuring BES Relays is that you want as few levels as possible to the BES Relays unless there is a bandwidth bottleneck. Communications over thin pipes should be relay to relay. The top-level BES Relay will relieve the BES Server, and the secondary BES Relay can allow a single download to be distributed over hundreds of BES Clients.

- There is a BES Relay in the DMZ set up with a special trust relationship with the BES Server. This BES Relay will allow BES Clients in the DMZ or on the public Internet to be managed by BES. The DMZ places a security firewall between the BES Relay and the set of home computers and laptops reporting in from the Internet.

- This diagram shows a single BES Relay in the large regional office. However, for offices with more than a few hundred clients, there will typically be multiple BES Relays to effectively distribute the load.

- As a general rule, you should deploy at least one BES Relay per 500-1000 BES Clients to maximize the efficiency of the BES Relay. See http://support.bigfix.com/bes/misc/besrelays.html for more information.

Hub and Spoke

This scenario involves a main data center, a small number of large regional offices and many small regional offices. This configuration is common in large international organizations. The BES Clients are installed on computers in offices all around the world. Many of these locations have slow WAN connections (8 kbps-512 kbps), but there will be many offices with faster WAN connections (1mbps-45mbps).
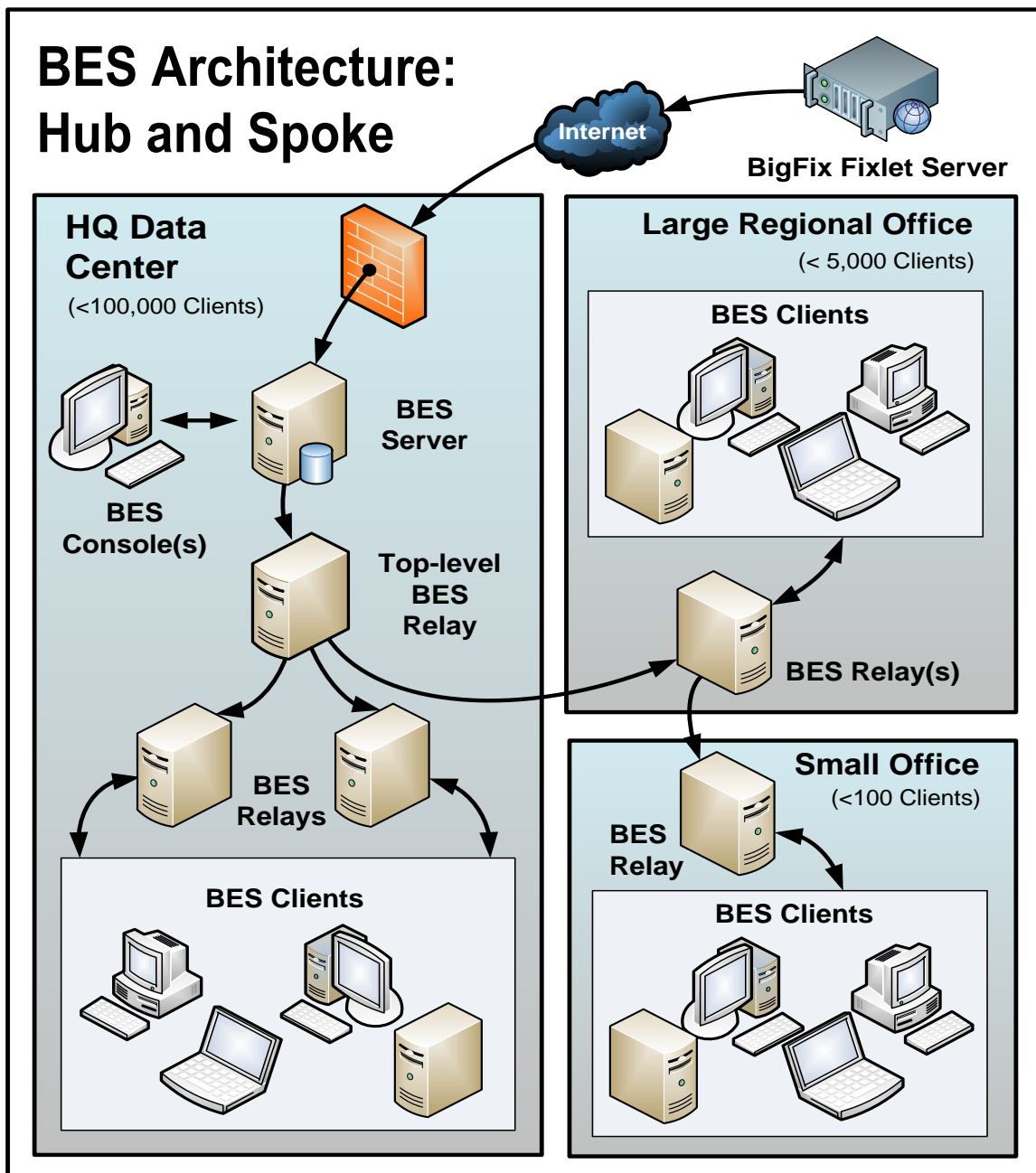
Often these locations are configured in a hub-and-spoke arrangement. This scenario builds on the previous one, but the hub-and-spoke configuration permits more levels in the BES Relay hierarchy.

Note the following about the diagram:

- In this scenario, the BES Relays are carefully deployed at the proper junctions within the WAN to optimize bandwidth. Poor placement of BES Relays can adversely impact your network performance.

- It is vital that at least one BES Relay is installed in every location with a slow WAN connection. Often a company will already have a server in just such a spot, acting as a file server, print server, AV distribution server, SMS distribution server or domain controller, or any other computer. The BES Relay is usually installed on these existing computers.

- To provide redundancy in a typical office, more than one BES Relay should be installed. In case a BES Relay fails for any reason (powered down, disconnected from the network, etc.), its attached BES Clients can then automatically switch-over to a different BES Relay. A redundant relay is less important in very small offices because fewer computers are affected by the failure of a BES Relay.

- When the BES Clients are set to **Automatically Locate Best BES Relays**, they will choose the closest one. If any BES Relay should fail, the BES Clients will automatically seek out another BES Relay. You should monitor the BES Relay configuration after the initial automated setup (and periodically after that) to ensure that the BES Clients are pointing to appropriate locations. Talk to your support technician for more details on how to protect against overloading WAN pipes with BES data.

- Bandwidth throttling at the BES Relay level is very helpful in this configuration. The BES Relays are set up to download slowly across the WAN pipes so as not to saturate the slow links. See http://support.bigfix.com/cgi for more information.

- Instead of pointing to the main BES Server, the BES Relays are configured to point to the top level BES Relay. This frees up the BES Server to couple more tightly to the BES Console and improves reporting efficiency.

The BES Relays will be configured to manually create the optimal hierarchy. The hierarchy will have three levels (from the top down):

1. The top-level BES Relay that connects directly to the BES Server.
2. The regional office BES Relays that connect to the top-level BES Relay.
3. Multiple branch office BES Relays that connect to specified regional office BES Relays.

Remote Citrix / Terminal Services Configuration

Although BES can efficiently deliver content even over slow connections, the BES Console itself is data intensive and can overwhelm a link slower than 256 kbps. Adding more BES Clients further increases the lag time. However, you can access the BES Console remotely from a Citrix, Terminal Services, VNC or Dameware-style presentation server and realize excellent performance. Here is what this configuration looks like:
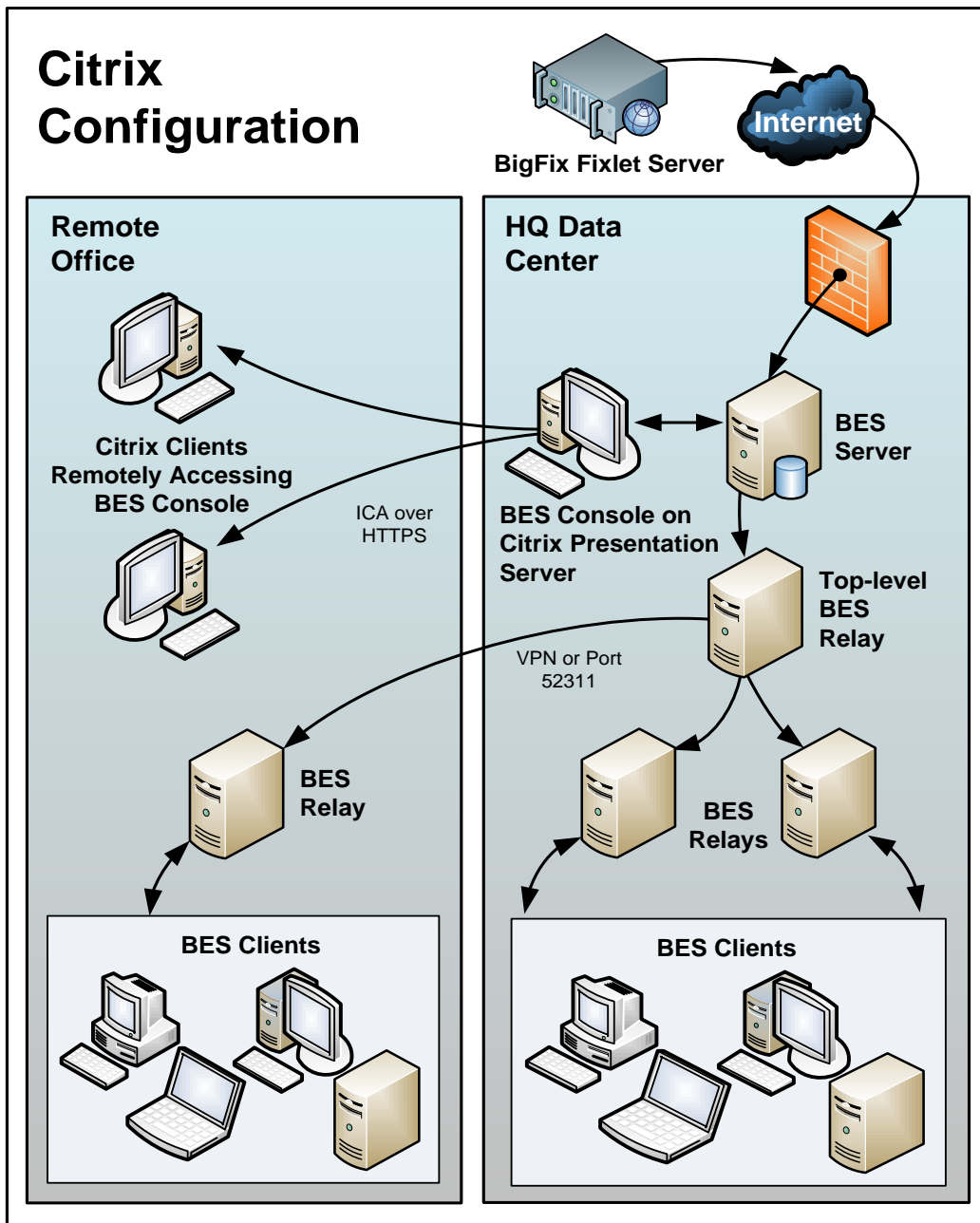
Note the following about the diagram:

- In the main office, the BES Console is set up on a computer that is close to the BES Server for fast data collection. This will be your Presentation Server.

- You must create user accounts for each remote user. These users will then be able to access the BES Console quickly because the time-critical data loading is done at the main office over a fast link.

- Your remote connection can be over HTTPS to improve security.

- Note that running a BES Console from a Presentation Server containing the private key is inherently less secure than if the key is stored on a removable drive.

- You may be able to benefit from load-balancing software to spread the remote accesses across multiple servers.

- The main bottleneck for a BES Console running on Citrix is memory size. If the BES Console runs out of memory, its performance will drop sharply. A good technique to determine the memory requirement is to open up the BES Console as a Master Operator. Check the memory used: this will indicate the maximum memory requirement per user. Then log in as a typical operator and use this as your average memory requirement. If your Citrix server can support all concurrent users with the maximum memory then a single box will suffice. If not, then use the average memory requirement per user to determine how many extra Citrix servers you may need.

- The second constraint is CPU power. During refreshes, the BES Console works best with a full CPU core. That means the Presentation server will be optimized with one CPU core running the BES Console for each concurrent user.

- The final concern is disk space for the BES Console cache. You can get a feel for the size of the cache by looking at an example on your local box: C:\Documents and Settings\<USERNAME>\Local Settings\Application Data\BigFix\Enterprise Console\BES_bfenterprise\Sites. There should be enough disk space to provide one cache file for each BES Console operator.

Glossary

action password—See BES signing password.

BDE—See BigFix Development Environment.

BES—See BigFix Enterprise Suite.

BES Client—Software installed on each networked computer to be managed under BES. The Client accesses a pool of Fixlet messages, checks the computer it is installed on for vulnerabilities, and sends the BES Server a message when such a condition occurs.

BES Console—A management program that provides an overview of the status of all the computers with the BES Client installed in the network, identifying which might be vulnerable and offering corrective actions.

BES database—A component of the BES system that stores data about individual computers and Fixlet messages. The BES Server's interactions primarily affect this database, which is a standard Microsoft product (MSDE 2000 or SQL Server 2000).

BES Generator Install folder—The directory on the installation computer where the Generator places the installation files for the BES system.

BES Installation Generator—An application that creates installers for the core BES system components.

BES Relay—This is a BES Client (Win 2k, 2k3 or XP) that is running special server software. Relays spare your server and the network by minimizing direct server-client downloads and by compressing upstream data. Relays are automatically discovered by BES Clients, which dynamically choose the best Relay to connect to.

BES Root Server—Refers to the HTTP or HTTPS services offered by the main BES Server as an alternative to IIS. The BES Root server is specially tuned to Fixlet traffic and is more efficient than IIS for this application.

BES Server—A collection of interacting applications (web server, CGI-BIN, and database server) that coordinates the relay of information to and from individual computers in the BES system. The server processes may be hosted by a single server computer or segmented to run on separate server computers or replicated on redundant servers.

BES signing password—The password (specified when the BES system was installed) used by a BES Console operator to sign an action for deployment. It is called the *action* password in the Console interface.

BES Site Administrator—The person in charge of installing BES and authorizing BES Console operators.

BES system install folder—The directory on the BES Server where the BES Server and related files (including Console and Client installers) will be installed.

BigFix technology—A process that enables knowledgeable computer technicians to disseminate information about the causes of computer problems to BES Clients across a network and provide automatic solutions for them.

BigFix Action Scripting Language—The language used for crafting action scripts. Action can be crafted in different scripting languages, including AppleScript and Unix shells.

BigFix Development Environment (BDE)—An integrated system for authoring and deploying, or publishing, Fixlet messages.

BigFix Enterprise Suite (BES)—A preventive maintenance tool for enterprises that monitors computers across networks to find and correct vulnerabilities with a few simple mouse-clicks.

BigFix Relevance Language—The language in which relevance clauses are written.

Custom Site—You can create your own custom content and host it in a custom site. This can only be done by a Master Operator that has been granted the rights to create custom content (use the BES Admin program to allocate these users).

DSA—Distributed Server Architecture. Multiple BES Servers are linked to provide full redundancy in case of failure.

Fixlet message—A mechanism for targeting and describing a problematic situation on a computer and providing an automatic fix for it.

Fixlet servers—Web servers offering Fixlet site subscriptions. They can be either internal to the enterprise network or external to the network (if direct external web access is allowed).

Fixlet site—A trusted source from which the BES Client obtains Fixlet messages.

installation computer—A secure computer (separate from the BES Server computer) that hosts and runs the BES Installation Generator.

Management Rights—Ordinary BES Console Operators can be limited to a specified group of computers. These limits represent the management rights for that user. Only a BES Site Administrator or a Master Operator can assign management rights.

Master Operator—A BES Console Operator with administrative rights. A Master Operator can do almost everything a BES Site Administrator can do, with the exception of creating new operators.

masthead—Files containing the parameters of the BES process, including URLs that point to where trusted Fixlet content is available. The BES Client brings content into the enterprise based on subscribed mastheads.

Microsoft Data Engine (MSDE)—A database engine that is included as part of the BES system and is useful for all the reporting and data storage needs. Sufficient for many needs, but may be upgraded to a full SQL implementation on larger networks.

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

MSDE—See Microsoft Data Engine.

Operator—A person who operates the BES Console. Ordinary operators can deploy Fixlet actions and edit certain computer settings. Master Operators have extra privileges, among them the ability to assign management rights to other operators.

signing password—See BES signing password.

Site Administrator —The only BES Console Operator with the right to create new Operators.

SQL server—A full-scale database engine from Microsoft that can be acquired and installed into the BES system to satisfy more than the basic reporting and data storage needs. A step up from MSDE.

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

VPN—Virtual Private Network. An encrypted channel (or tunnel) that allows companies to extend their local-area networks across the world by using an inexpensive Internet connection.

WAN—Wide-area network. Many offices are connected by WAN. The bandwidth of your WAN determines the placement of BES Relays in your deployment, with thin WANs requiring more relays to aggregate downloads and reduce overhead.

Index

Acknowledgements and Notices

We would like to acknowledge the individuals and organizations listed below whose software we have included in unmodified form for use with our proprietary software product. Where applicable, we have included notices applicable to such third parties' software and a link to the URL where you can obtain such third party software.

ALL THIRD PARTY SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, AND ALL WARRANTIES, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT, ARE HEREBY DISCLAIMED. FURTHER, BIGFIX, INC. DOES NOT WARRANT RESULTS OF USE OR FREEDOM FROM BUGS OR UNINTERRUPTED USE OR ACCESS. IN NO EVENT SHALL BIGFIX, INC. BE LIABLE OR OBLIGATED WITH RESPECT TO ANY THIRD PARTY SOFTWARE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION, PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY, SERVICES OR RIGHTS, INTERRUPTION OF USE, LOSS OR CORRUPTION OF DATA, LOST PROFITS OR BUSINESS INTERRUPTION) HOWEVER CAUSED, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The 'zlib' compression library written by Jean-loup Gailly (jloup@gzip.org) and Mark Adler (madler@alumni.caltech.edu) is included with this product. You can obtain the 'zlib' compression library code at http://www.gzip.org/zlib/.

This product uses cryptographic software written by Eric Young (eay@cryptsoft.com). This product uses software written by Tim Hudson (tjh@cryptsoft.com). The following notice applies only to such software, which together comprises the 'openSSL' library included with this product. You can obtain the 'openSSL' library code at http://www.openssl.org/.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following

acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you
must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

The following notice applies only to the 'gd' library software included with this product. You can obtain the 'gd' library code
at http://www.boutell.com/gd/.

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003 by Cold Spring Harbor Laboratory.
Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@graphviz.org).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@graphviz.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C)
1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work
of the Independent JPEG Group. See the file libjpeg-license.txt for more information.

See also libfreetype-license.txt, libpng-license.txt, zlib-license.txt, and libjpeg-license.txt, all of which are open
source licenses compatible with free commercial and noncommercial use, in some cases with minor documentation
requirements.

Portions relating to WBMP copyright 2000, 2001, 2002, 2003 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial
application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in this version of gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

The PNG Reference Library, 'libpng' is included with this product. You can obtain the libpng code at http://www.libpng.org/pub/png/libpng.html.

The following notice applies only to FreeType Project software included with this product. You can obtain the FreeType Project code at http://www.freetype.org/.

Portions of this software are copyright © 1996-2002 The FreeType Project (www.freetype.org). All rights reserved.

The following notice applies only to the H3 Library software included with this product. You can obtain the H3 Library code at http://software.bigfix.com/download/bes/misc/bigfixh3modifications.zip. The H3 Library software included in this product is redistributed to licensee free of charge and without a fee.

Copyright © 1998, Silicon Graphics, Inc. – ALL RIGHTS RESERVED

Permission is granted to copy, modify, use and distribute this software and accompanying documentation free of charge provided (i) you include the entirety of this reservation of rights notice in all such copies, (ii) you comply with any additional or different obligations and/or use restrictions specified by any third party owner or supplier of the software and accompanying documentation in other notices that may be included with the software, (iii) you do not charge any fee for the use or redistribution of the software or accompanying documentation, or modified versions thereof. Contact sitemgr@sgi.com for information on licensing this software for commercial use. Contact munzner@cs.stanford.edu for technical questions.

SILICON GRAPHICS DISCLAIMS ALL WARRANTIES WITH RESPECT TO THIS SOFTWARE, EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. SILICON GRAPHICS SHALL NOT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST REVENUES, LOST PROFITS, OR LOSS OF PROSPECTIVE ECONOMIC ADVANTAGE, RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the Government is subject to restrictions as set forth in FAR 52.227.19(c)(2) or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and/or in similar or successor clauses in the FAR, or the DOD or NASA FAR Supplement. Unpublished - rights reserved under the Copyright Laws of United States.

Contractor/manufacturer is Silicon Graphics, Inc., 2011 N. Shoreline Blvd. Mountain View, CA 94039-7311.

This software includes portions of geomview/OOGL. Copyright (c) 1992 The Geometry Center; University of Minnesota, 1300 South Second Street; Minneapolis, MN 55454, USA

geomview/OOGL is free software; you can redistribute it and/or modify it only under the terms given in the file COPYING, which you should have received along with this file. This and other related software may be obtained via anonymous ftp from geom.umn.edu; email: software@geom.umn.edu.

The incorporated portions of geomview/OOGL have been modified by Silicon Graphics, Inc. in 1998 for the purpose of the creation of this software.

Original Geometry Center Copyright Notice: Copyright (c) 1993

The National Science and Technology Research Center for Computation and Visualization of Geometric Structures (The Geometry Center): University of Minnesota, 1300 South Second Street
Minneapolis, MN 55454 USA email: software@geom.umn.edu

This software is copyrighted as noted above. It is free software and may be obtained via anonymous ftp from geom.umn.edu. It may be freely copied, modified, and redistributed under the following conditions:

1. All copyright notices must remain intact in all files.

2. A copy of this file (COPYING) must be distributed along with any copies which you redistribute; this includes copies which you have modified, or copies of programs or other software products which include this software.

3. If you modify this software, you must include a notice giving the name of the person performing the modification, the date of modification, and the reason for such modification.

4. When distributing modified versions of this software, or other software products which include this software, you must provide notice that the original source code may be obtained as noted above.

5. There is no warranty or other guarantee of fitness for this software, it is provided solely "as is". Bug reports or fixes may be sent to the email address above; the authors may or may not act on them as they desire.

If you use an image produced by this software in a publication or presentation, we request that you credit the Geometry Center with a notice such as the following: Figures 1, 2, and 5-300 were generated with software written at the Geometry Center, University of Minnesota.