BigFix Enterprise Suite (BES™)

Administrator's Guide

Version 4.1
Last Modified: March 23, 2004

BigFix, Inc.
Emeryville, California

All inquiries regarding the foregoing should be addressed to:

BigFix, Inc.
5915 Hollis Street
Emeryville, CA 94608-2017

Acknowledgements

We would like to acknowledge the following individuals and organizations whose software we have built upon:

Cryptographic software

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Compression software

This product uses the 'zlib' compression library written by Jean-loup Gailly (jloup@gzip.org) and Mark Adler (madler@alumni.caltech.edu).

Contents

Introduction

The **BigFix Enterprise Suite (BES)** solves the increasingly complex problem of keeping your critical systems updated, compatible and free of security holes. 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.

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'll find it easy to keep your networked computers updated and properly patched, all from a central BES Console. Rolling out a security 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 an issue are never bothered.

You'll be able to track the progress of each computer as updates 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 for audit trails and chart your overall activity with a convenient web-based reporting program.

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 BES. They access a collection of Fixlet messages that detects security holes and other vulnerabilities. The BES Client is then capable of implementing corrective actions received from the BES Console through the BES Server. In most cases, the BES Client operates silently, without any direct intervention from the end user. However, BES also allows the administrator to provide screen prompts for those actions that require user input.

- **The BES Server** is a collection of interacting services, including application services, a web server and a database server, forming the heart of the BES system. It coordinates the flow of information to and from individual computers and stores the results in the BES database. The BES Server components operate quietly in the background, without any direct intervention from the administrator.

- **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 or Windows XP computer that has network access to the BES Server.

- **Web Reports** let you produce charts and graphs of your data, providing you with hard copy and helping you to maintain an audit trail of all the Fixlet activity on your network. You can export this data for further manipulation in a spreadsheet or database. The Web Reports program also allows you to aggregate information from additional BES Servers that you may have installed in your organization. This important feature allows an organization with hundreds of thousands of computers to be quickly and easily visualized.

Using this Guide

The process of getting BES up and running varies, depending on your network environment and your security policies. This guide focuses on a standard BES deployment, which applies to workgroups and to enterprises within a single administrative domain. In addition, the standard deployment stipulates that:

- The organization has 75,000 or fewer computers. (More computers can be added with more BES servers – talk to your BigFix sales engineer for details).
- The BES Server is able to make direct connections to the Internet (the BES Server can be set up to use a proxy if necessary).
- The BES Site Administrator’s computer can make ODBC and HTTP connections to the BES Server.
- The computers must be on a single LAN, although separate sections may be connected through a VPN or leased line.
- Each BES Client computer in the network must be able to make an HTTP connection to the BES Server on the specified port (the default port is 52311).

Some larger enterprises may violate one or more of these conditions, but BES can still be deployed in these environments -- the section titled **Deployment Scenarios** (page 46) shows you how. If your network configuration doesn’t match any of the scenarios in that chapter, talk to a BigFix support technician for more options.

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

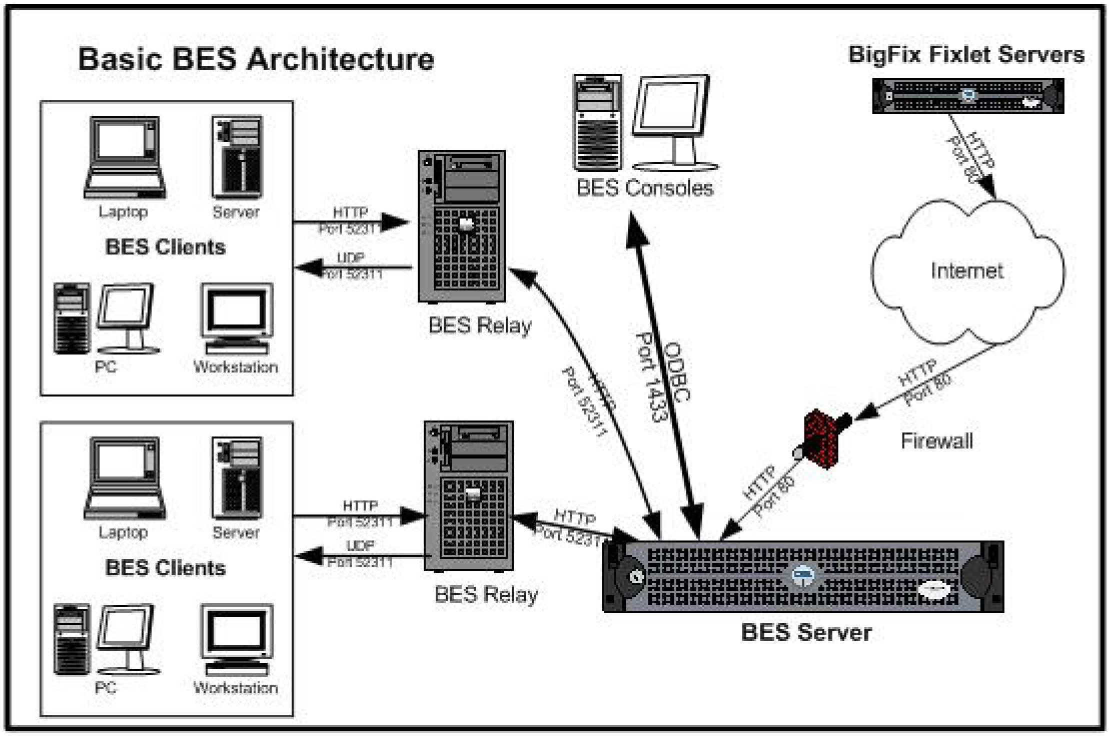
If you are installing the BES Evaluation version, be sure to read the **BES Quick Start Guide**. When you’re ready to install the full system, you'll want to pay extra attention to BES Client and BES Relay deployment, to ensure an efficient rollout.

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

A Typical Installation

A typical installation of BES resembles the diagram below. There is a single 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, so-called because they relay the data on to the BES Clients. Each BES Client inspects its local computer and reports any relevant Fixlet messages back to the BES Relay, which compresses the data and passes it back up to the servers.

The BES Console oversees all this activity. It connects to the BES Server and periodically updates its display to reflect changes or new knowledge about your network. When vulnerabilities are discovered, the BES Console operator can then target patches or other fixes to the appropriate computers. The progress of the fixes can be followed in near real-time as they spread to all the relevant computers and, one by one, eliminate their vulnerabilities.



Note: The arrows in this diagram are intended to illustrate the flow of information throughout the enterprise. BES Clients gather Fixlet messages and action information from BES Relays or directly from the BES Server. They then send small amounts of information back to the BES Server through the BES Relays. The arrow from the BigFix Fixlet Servers to the BES Server represents the flow of Fixlet messages into your network. This data transfer is strictly one-way; information never leaves your network. 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 BES to work properly. Please ask your support technician for more details.

BES Operating Requirements

BES has been designed to run efficiently using minimal server, network and client resources. This section describes the basic requirements for an organization with 75,000 or fewer computers. The requirements for the BES Client programs are not stringent. The power required by the BES Server and the BES Console will depend on the number of computers that are administered.

BES Server Requirements

The BES Server must be a Windows 2000 or Windows Server 2003 computer. The hardware requirements for the BES Server vary depending on how many BES Clients are attached. The latest BES Server recommendations can be found at http://support.bigfix.com/cgi-bin/redir.pl?page=serverreq. Note that the server requirements will vary for each organization depending on a number of factors. Consult with your support technician for more information about BES Server requirements.

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

- Your firewall should block port 52311 in and out of the organization so that all BES related traffic will not be able to flow into or out of your network

  Note: certain configurations of BES will require that this port be open at a firewall; specifically, if you wish to allow roaming BES Clients that are not connected through VPN to be administered by the system, you will need to open this port on your firewall.

- TCP/IP and UDP on port 52311 must be completely unblocked at all internal routers and internal firewalls.

These networking recommendations will be easy to satisfy for most organizations maintaining a moderate security posture. If these requirements can't be met in your organization, see **Configuring the BES Components** (page 30). For information on larger installations, see **Deployment Scenarios** (page 46).

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

- **BES Relays.** Designated BES Clients can be used as relays to significantly lighten the load on the BES Server(s).
- **The length of the Heartbeat Interval**, which controls how often BES Clients send the BES Server updated asset information. A proper setting balances responsiveness against acceptable network traffic. The default heartbeat is 15 minutes, but this can be changed in the BES Console from the **File > Preferences** menu.
- **The number and type of retrieved properties**. Retrieved Properties can provide extremely useful data points but, if poorly implemented, they can also create undue load on the system by requiring too much bandwidth or too many BES Client resources. Talk to your BigFix support technician for more information about retrieved properties.

- **Management rights.** By limiting Console Operator access to specific subsets of your network, you can lower the overall traffic between the BES Server and the BES Consoles.
- **The number of computers aggregating data for web reports.** Every BES Web Report server that is set to aggregate data from a BES Server will transfer a great deal of information. When using web reports aggregation, avoid aggregating data unnecessarily or make the aggregation less frequent (i.e., once per day).

For more information about these performance issues, please view http://support.bigfix.com/cgi-bin/redir.pl?page=besperformance or contact your BigFix support technician.

Note: The default installation of **Microsoft's URL Scan** and **IIS Lockdown Tool** will ***not*** allow the BES Server to function properly. For information on using these programs with BES, please view the knowledge-base articles at the BigFix support site, http://support.bigfix.com/. Search the knowledge base with the keyword **lockdown** to find relevant articles.

BES Console Requirements

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

Hardware	Software
Intel Pentium III–class processor	Windows 2000, XP Home, XP Pro
512 MB RAM	MDAC 2.7

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

BES Client Requirements

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

Hardware	Software
x86-based computers	Windows 95, 98, NT 4+, Me, 2000, Server 2003, XP, Red Hat Linux 7.1 & 8.0, Solaris 7, 8 & 9.
32 MB RAM	20 MB hard disk space

Versions of the BES Client are currently in development for several other operating systems, including Unix and the Macintosh OS variants. Please check with your support technician for more details. For Windows platforms, IE 4.01 or greater must be installed.

Database Requirements

BES requires SQL Server 2000 or Microsoft Data Engine (MSDE) 2000, 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's sufficient for some BES installations (especially evaluation installations), it isn't recommended for a full-blown deployment. 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 built-in restrictions -- 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 the 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 BES 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 BES, 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 actions to your BES Client computers.***

Treat your private key just like the physical key to your company's front door. Don't leave it lying around on a shared disk. Instead, store it on a removable disk in a safe place -- and ***don't 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'll need to do a fresh install of the entire system (including all the BES Clients).

As the BES 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 BES 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 an operator issues 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 BES 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 either IIS or SQL Server/MSDE (if you opt to use them) is secured with the latest security-related patches from Microsoft.
- Verify that your network firewall forbids inbound and outbound traffic on port **52311** so that BES-related traffic will not be able to flow into or out of your network

  Note: certain configurations of BES will require that this port be open at a firewall; specifically, if you wish to allow roaming BES Clients that are not connected through VPN to be administered by the system, you will need to open this port on your firewall. For more information, see **Modifying Port Number**s (page 43).
- Make sure that TCP/IP and UDP on port **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 BES 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 BES 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/.
- You should secure the database (SQL Server or MSDE) and web server (IIS) using company or industry-wide standards. Contact your network administrator or database administrator for more information. Note: certain lockdown procedures will cause the BES Server to not function properly. Contact your support technician if you have any specific questions about lockdown procedures.

Getting Started

Administrative Roles

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

- **The Network Administrator,** who 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 BES from working properly. The network administrator will also provide information about WAN link connection speeds and subnet addresses if necessary.

- **The Database Administrator,** who will be responsible for setting up and maintaining the SQL Server 2000 or MSDE 2000 database for the BES Server.
  Note: The BES Server installer will automatically set up and install MSDE 2000. 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 BES Site Administrator,** who will install and maintain the BES 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 grant administrative rights to 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,** who are operators 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 BES Site Administrator can create new operators.

- **BES Console Operators,** who will manage the day-to-day operation of BES, including Fixlet management and action deployment, subject to the management rights assigned by a BES 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 BES Site Administrator

This BES Site Administrator has the following primary responsibilities:

- **Obtaining and securing the Action Site Credentials.** In order to install BES, the BES administrator will need to generate a private key, receive a public key and a license certificate from BigFix, and create a masthead with the digital signature and configuration information.
- **Certifying Users.** The BES Site Administrator must authorize and set an initial password for each individual who intends to operate the BES Console.
- **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 BES database.
- **Installing the various BES Components.** The BES Site Administrator will install the BES Client, Server, Relay and Console modules. Installation takes less than a day. Depending on the network configuration, the one-time-only BES Client installation typically consumes the most time.
- **Assigning Management Rights.** The BES Site Administrator (along with the BES Master Operators) is responsible for assigning management rights to the BES Console operators. These rights constrain operators to specific subsets of the network, making their jobs easier and faster, while making the network more secure.
- **Maintaining the BES Server**. The BES Server runs a database (SQL Server 2000 or MSDE 2000) and a web server (IIS or BES Root Server). Standard maintenance tasks like upgrades or fixes will be managed using Fixlet technology or may be performed manually by the BES Site Administrator.
- **Maintaining security**. The BES system is protected by password-encrypted private keys. The BES Site Administrator controls access to these and can create new private publisher keys or revoke them as the need arises. BES 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 Certified

The BES system is powerful, so you'll want to limit access to trusted, authorized personnel only. BES operates from a central repository of Fixlet actions called the **Action site**, which is protected by public/private key encryption against spoofing and other unauthorized usage. The digital key creates a signing chain from the BES Site Administrator back up to BigFix, Inc., and is stored in a file called the **action site masthead**.

Before you perform the steps below, you must have purchased a license to use BES. If you have not yet purchased a license to use BES, please contact sales@bigfix.com or visit the BigFix Website at http://www.bigfix.com/.

Once you have your license from BigFix, you can use it to create your action site masthead. 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.

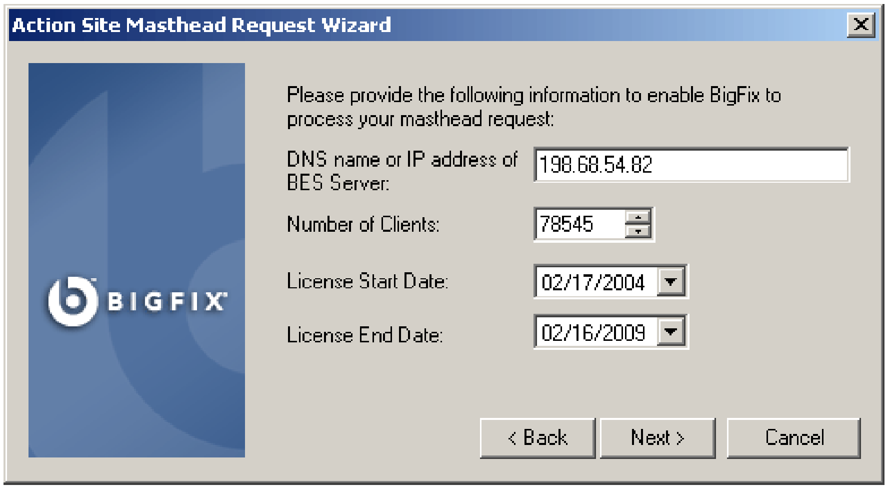
Note: If you are using an evaluation version of BES, you may skip the following section. During installation, the **BES Evaluation Generator** will create your signing keys through an expedited process, and the generation of separate publisher keys will not be necessary.

Obtaining a Site Certificate

The steps below will set up the various BES Installation programs and create a public/private key certificate that will allow you to deploy BES across your network. BigFix recommends that you don't use the BES Server computer for this; use a separate secure computer (such as the BES Site Administrator's desktop computer). For security reasons, private keys should never be stored on the BES Server itself.

1. Download **BES** at http://software.bigfix.com/bes/install/downloadbes.html. You will run this program twice: once to request a certificate and a second time to install the software.
2. Log in as an administrator and launch the downloaded program.
3. A **Welcome** dialog is displayed. Click **Next**.
4. The next screen presents you with a choice to install either the **Evaluation** or the **Production** version of the program. If you are interested in the Evaluation version, please consult the Quick Start Guide. For the purposes of this document, click the button marked Production, then click **Next**.
5. After reading the **License Agreement**, click **Yes** to accept it and continue.
6. A dialog box is displayed offering you three choices. Select the first choice to **request a production license from BigFix, Inc**., then click **Next**.
7. This choice launches the Action Site Masthead Request Wizard. Enter your **Name**, **Organization** and **Email address** in the appropriate boxes and click **Next**.

8 The next dialog asks for important information about your license.



Action Site Masthead Request Wizard

Please provide the following information to enable BigFix to process your masthead request:

DNS name or IP address of BES Server: 198.68.54.82

Number of Clients: 78545

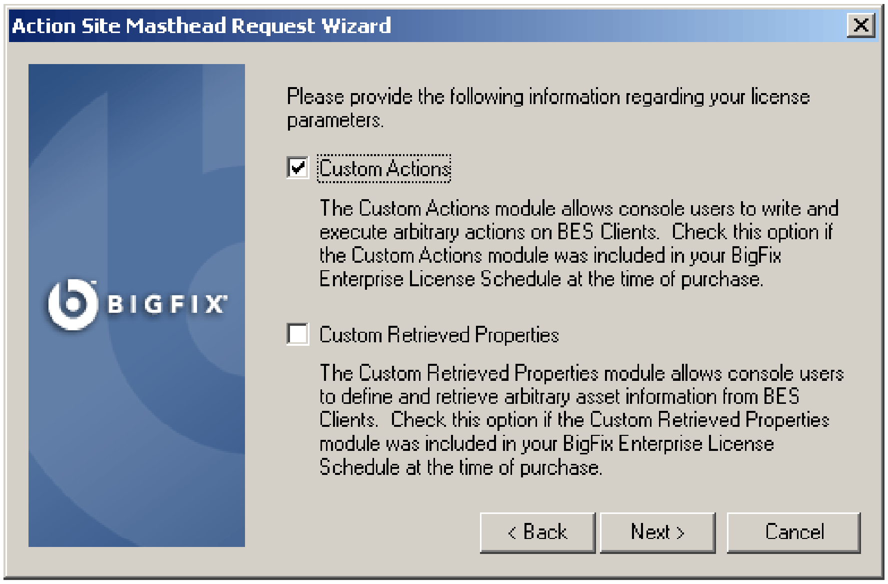
License Start Date: 02/17/2004

License End Date: 02/16/2009

Enter the dotted **IP address** or **DNS name** of the server computer that will host the BES Server. This address is at the core of your license agreement, and can't be changed later without reinstalling BES. If you use a hostname/dns name, it must be resolvable by all the BES Clients. Using a name like bes.companyname.com instead of the numbered IP address will allow you to easily change the BES Server's underlying IP address, should that become necessary. Enter the number of BES Clients that you wish to include and the desired licensing period, then click **Next**.

Note: Once a server IP or host name is registered with BigFix, Inc., it can't be changed without creating a completely new action site. Pick an IP address or host name that you can dedicate to BES.

9 The next screen presents you with two options to add custom features to your BES setup, **Custom Actions** and **Custom Retrieved Properties**. These optional features are purchased separately, and should be listed in your BigFix Enterprise License Schedule.



Action Site Masthead Request Wizard

Please provide the following information regarding your license parameters.

☑ Custom Actions

The Custom Actions module allows console users to write and execute arbitrary actions on BES Clients. Check this option if the Custom Actions module was included in your BigFix Enterprise License Schedule at the time of purchase.

☐ Custom Retrieved Properties

The Custom Retrieved Properties module allows console users to define and retrieve arbitrary asset information from BES Clients. Check this option if the Custom Retrieved Properties module was included in your BigFix Enterprise License Schedule at the time of purchase.

The **Custom Actions** option allows you to create your own Fixlet actions. The **Custom Retrieved Properties** option lets you query your client computers for specific custom properties. Depending on your license agreement with BigFix, you should check the boxes for the appropriate custom features. In general, the custom actions and custom retrieved properties are included with purchase of a BES license. Check with your sales engineer or reseller for more information. Click **Next** to continue.

10 The next dialog prompts you for a **password** that will add extra protection to your public/private key pair. Enter a password with at least six characters and verify it. Make sure you record it in a safe place. This Action password is used to encrypt your private site key (license.pvk), offering an extra level of protection. You may also select a different **key size** for encryption. In general, the greater the key length, the more secure it is (however, there is a small performance penalty for using a greater key length). The default length is 1024 bits, which should be more than adequate for most uses. However, it is possible to select up to 4096 bits. Click **Next** to continue.

11 The program prompts for a folder to hold the site credential. For maximum security, it is recommended that you use a removable or encrypted disk with a folder named **BES Credentials**. Click **OK** to continue. A private key (**license.pvk**) is written to your credential folder.

12 The final dialog of the Masthead Wizard is displayed, prompting you to submit your request for a certificate. Once you receive this certificate from BigFix, you will be able to install the BES software. There are two different ways to submit your request for a certificate. The first and fastest is to submit your request over the Internet. In the unlikely event that you don't have access to the Internet, the second choice saves the request in a file that can be submitted by other means to BigFix, Inc. Click **Next** to finish the wizard.

13 The data will be sent to BigFix, Inc. and your personalized site certificate will be returned by email, usually within 24 hours.

Keep in mind that a private key (**license.pvk**) to your action site has now been created for you and encrypted with your password. The key is in your **BES Credentials** folder and authorizes you, as the BES 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 BES Credentials folder to a removable or encrypted disk.

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 the BES Clients) with a freshly generated key.

Bookmark this Page.

**When you receive your license,
return here to continue the installation.**

Saving the License

When BigFix, Inc. receives your site request, a site certificate is created and digitally signed. The file is then sent as an attachment to the email account you specified in the previous step. The site certificate establishes a chain of authority from the BigFix root all the way down to the BES Console operators in your organization. This ensures that all administrative levels of BES are securely authorized.

Certain versions of email clients and email servers will not accept attachments that end in **.crt**. In order to circumvent this annoyance, BigFix sends you a compressed file (**license.zip**) containing your site certificate (**license.crt**). If your email client or email server blocks .zip files, please contact BigFix to request a compatible format.

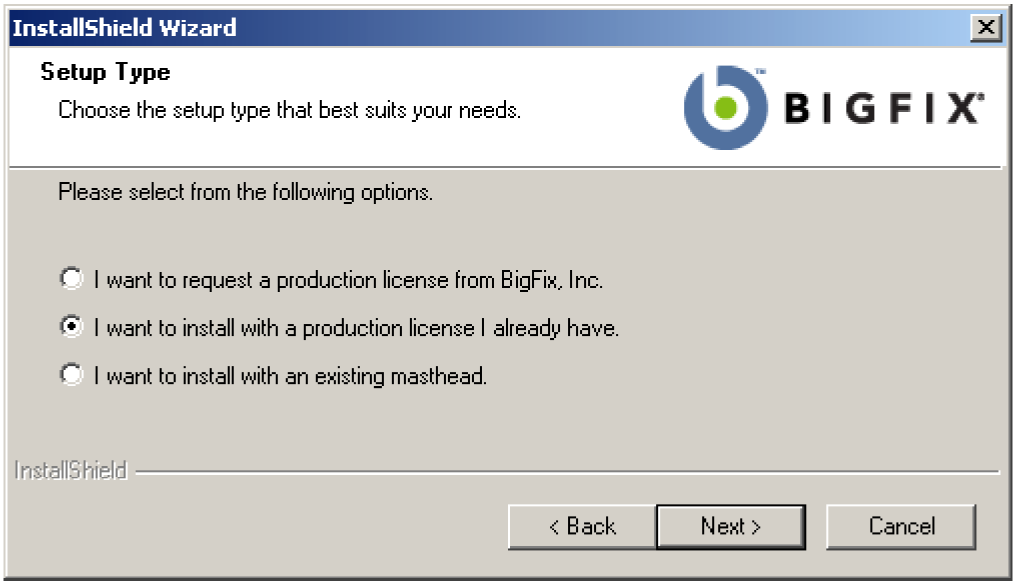
1. Unzip the **license.zip** file using WinZip or any other zip program.
2. Save **license.crt** to your hard drive or to the same disk with the **BES Credentials** folder. The file is in text format. If you're curious, you can open the file with WordPad. Notice that it is a signed file that includes your public key as well as your name, company, address and server IP address. This license authorizes you, as the BES Site Administrator, to create publisher certificates for your BES operators.

Creating the Action Site Masthead

Once you have your license, you're ready to create your personalized **action site masthead** that will, in turn, allow you to install and use BES. 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. Re-run the BES Installer that you downloaded from BigFix (as documented in the previous section).
2. At the welcome screen, click **Next**.
3. A dialog is displayed offering to install the **Evaluation** or **Production** version of BES. Select Production and click **Next**.
4. After reading the **License Agreement**, click **Yes** to accept it and continue.

5 The **Setup Type** dialog is displayed:



Please select from the following options.

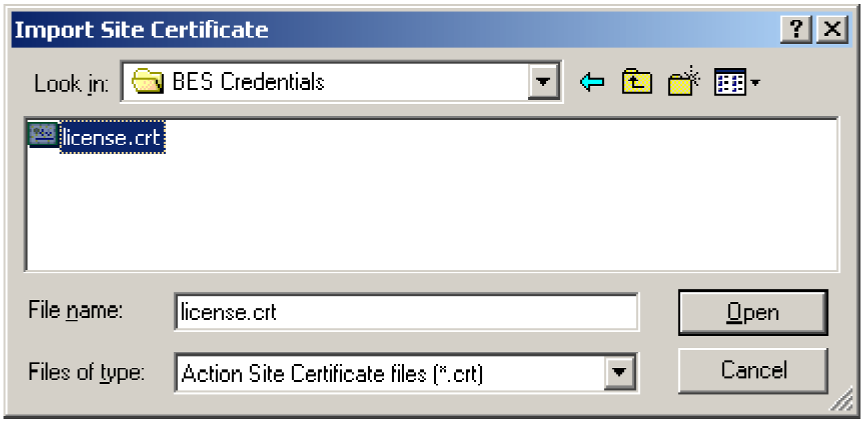
○ I want to request a production license from BigFix, Inc.

● I want to install with a production license I already have.

○ I want to install with an existing masthead.

Since you've already received your license certificate, select the choice to **install with a production license**, then click **Next**.

6 A standard Windows open-file dialog is displayed. Navigate to the site certificate file (**license.crt**) that you received from BigFix.



Look in: BES Credentials

license.crt

File name: license.crt

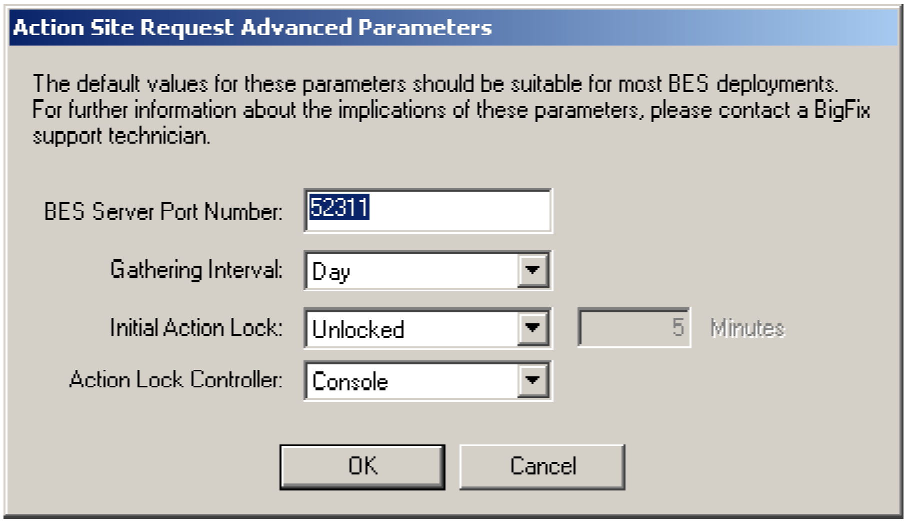
Files of type: Action Site Certificate files (*.crt)

Select the file and click **Open.** The program imports the certificate.

7 A dialog appears prompting you for the location of the **site level signing key**. This is your private key (**license.pvk**) that you created in the previous section. Select the default path (if specified) or click the **Browse** button to find the file.

8 Once the proper file is selected, click **OK**.

9 The program prompts for a server port number that BES will use for all its data transmissions. The default port is **52311**.



Action Site Request Advanced Parameters

The default values for these parameters should be suitable for most BES deployments. For further information about the implications of these parameters, please contact a BigFix support technician.

BES Server Port Number: 52311

Gathering Interval: Day

Initial Action Lock: Unlocked 5 Minutes

Action Lock Controller: Console

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). Make note of this number and make sure your firewall is configured to enable the use of this port internally while blocking access to it from outside the organization (see **Modifying Port Number**s, page 43). Click **Next**.

Note: Use caution when selecting a different BES Server port. If you later change your mind, you will need to completely re-install the BES System.

10 You will be prompted for the **Site Admin Private Key Password**. Enter the password you selected to protect your key (see the previous section) and click **OK**.

11 A standard Windows **Save As** dialog is displayed and you're prompted to save the **Masthead**. This is a public file that doesn't require protection. Navigate to the desired folder, name the file (e.g. actionsite.afxm), and click **Save**.

12 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**.

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

Installing the BES 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 BES installation components, including the BES Installation Guide. When the components have been saved, the **BES Installation Guide** is automatically executed. You may also run it at any time by selecting it from the Start Menu.

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

1. If it's 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 is displayed, prompting you to select a BES component to install. Click the buttons on the left, in order from top to bottom, to install the BES components. The three component installers include:
   - **Install BES Server**
   - **Install BES Console**
   - **Install BES Clients**
4. Each component has its own installer. Follow the instructions for each, as described below.

Installing the BES Server

The BES Server is the heart of the BES 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).

To install the BES Server, follow these steps:

1. If you haven't 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 is displayed. Click the top button labeled **Install BES Server.** This starts the installation process, which analyzes the server to ensure that it is properly prepared. If it finds that you don't have SQL Server 2000 or MSDE 2000 currently installed, the installer will offer to install a copy of MSDE 2000. Follow the on-screen instructions to install the database. Without a web server and a database, the BES Server cannot be successfully installed.
3. The BigFix Server Install Wizard presents a welcome screen. Click **Next** to continue.

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

5. 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've decided on the destination, click **Next**.

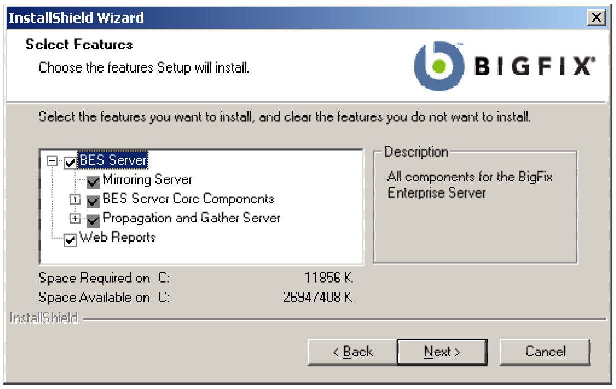
6. A dialog is displayed prompting you to select the **BigFix Server** or **IIS**. BigFix Server is more secure, more dedicated and more tuned to the task than IIS, and is thus the preferred selection (for more information, please contact your BigFix support technician). Select the server setup you desire, and click **Next**.

7. Next, you're prompted to enter a location for the BES Server web root folder. If you selected IIS, the installer will create a new IIS web server instance named **BigFix Enterprise Server Web Site** with the web root directory at **C:\inetpub\wwwrootbes\** (by default). If you opted to use the recommended BigFix Server, this folder will be used for the data files.

   The BES Server installer will configure the web server instance to use the appropriate port number (the default port is 52311) and will set the appropriate web server permissions. You may choose a different location for the BES Server web root folder by clicking the **Browse** button. Once you've selected the desired www root folder, click **Next.**

   Note: if you are installing the BES Server on a Windows 2000 *Professional* computer and using IIS (which is not recommended due to network connection limitations built into Windows 2000 Professional), the BES Server installer will not create another web server instance because multiple web server instances are not allowed on Windows 2000 Professional. Instead, the BES Server installer will configure the default web server to work with the BES Server. This may interfere with other programs using the web server on that computer.

8. A dialog is displayed with a list of the BES Server components about to be installed.



InstallShield Wizard

Select Features

Choose the features Setup will install.

Select the features you want to install, and clear the features you do not want to install.

- ☑ BES Server
  - ☑ Mirroring Server
  - ☑ BES Server Core Components
  - ☑ Propagation and Gather Server
- ☑ Web Reports

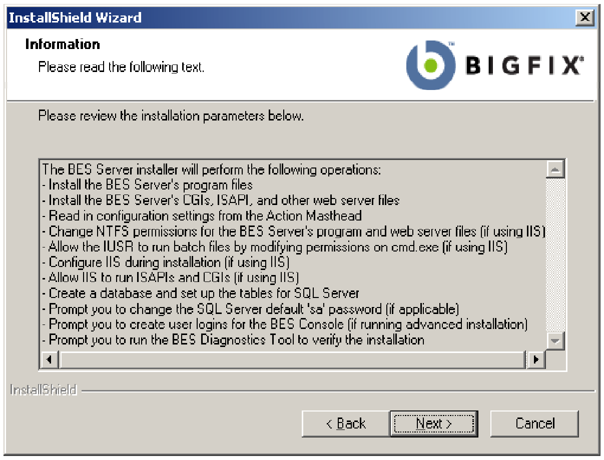
Description

All components for the BigFix Enterprise Server

Space Required on C: 11856 K
Space Available on C: 26947408 K

In general, you should accept the default components and click **Next**.

9 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 be run.



Information

Please read the following text.

Please review the installation parameters below.

The BES Server installer will perform the following operations:
- Install the BES Server's program files
- Install the BES Server's CGIs, ISAPI, and other web server files
- Read in configuration settings from the Action Masthead
- Change NTFS permissions for the BES Server's program and web server files (if using IIS)
- Allow the IUSR to run batch files by modifying permissions on cmd.exe (if using IIS)
- Configure IIS during installation (if using IIS)
- Allow IIS to run ISAPIs and CGIs (if using IIS)
- Create a database and set up the tables for SQL Server
- Prompt you to change the SQL Server default 'sa' password (if applicable)
- Prompt you to create user logins for the BES Console (if running advanced installation)
- Prompt you to run the BES Diagnostics Tool to verify the installation

Click **Next** to continue the installation.

10 When the files are properly installed, the program will prompt you for specific information, depending on your installation parameters. This 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).

11 You are then prompted to locate the **Action Site Masthead**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where your masthead is stored, select it and click **Open**.

12 You are prompted for the location of your **license certificate**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where your license is stored (license.crt), select it and click **Open**.

13 Next, you are prompted 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.

14 The program will then prompt you to create new user names and passwords for your console operators. Click **Add User** to start. You don't need to add all the users at this point; you will be able to add more users by running the BESAdmin program later. For more information on adding users, see **Adding BES Console Operators**, on page 28.

15 Enter the name of the BES operator (no spaces allowed), the email address and a password for this user. Indicate whether this user will be allowed to administer management rights or to create custom actions. Click **OK** when done.

16 When you're done entering users, click **Done**.

17 The BES Server installation is now complete. As the program exits, it provides you with the opportunity to run the **BES Diagnostics** (see below), to ensure that the installation is functioning properly. Make sure the box marked **Run the BES Diagnostic Tool** is checked, and click **Finish**.

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've 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 **CGI Scripts, Services, Web Permissions, Service Permissions** and **Web Reports.**
3. Click the different tabs to view the diagnostics.
4. 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.
5. 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.
6. If all the buttons are glowing green, click **Close** to exit the Diagnostic**.**

Understanding the BES Server Components

The BES Server is now successfully installed. It will respond to messages and requests from the BES 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:

- **Mirror Server Component.** Although it's possible to have the BES Clients communicate directly over the Internet to fetch Fixlet messages and downloads, that configuration can cause substantial wasted network traffic. Instead, in the default configuration of BES, a mirror server gathers content once from the Internet and then retransmits the content to the BES Clients directly (or through BES Relays). This solution provides significant bandwidth advantages, as well as removing the need to configure individual BES Clients to connect to the Internet directly.

- **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 then passed on to the BES database 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 rest of the components.

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's not a good idea to run the BES Console on the BES Server computer itself due to the 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. 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.
5. After the files are installed, click **Done** to complete the installation.

See the **BES Console Users Guide** for more details on using the 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 running the BES Server and the BES Console. That allows those computers to receive important Fixlet messages (like security patches or BES upgrades).

There are several different techniques for deploying the BES Client, 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 small networks (less than about 3,000 computers) connected to Active Directory or NT Directory domains, you can use the BES Client Deploy Tool to install BES Clients. 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 .
- 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 and you must be logged in as the domain administrator.
- 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 not intended for domains with more than about 3,000 computers. If you attempt to deploy more than 3,000 BES Clients with the tool, the program will become progressively less responsive.

The BES Client Deploy Tool starts by creating a share of the BES Client installer. It then gets a list of computers from the Active Directory server and, remotely connecting to the SCM, it accesses 100 computers at a time. It checks to see if the BES Client service is already installed on each computer. If so, it reports “Installed.” Otherwise it reports “Not Installed” – unless it can’t communicate with the computer at all, in which case it reports “Not Responding.”

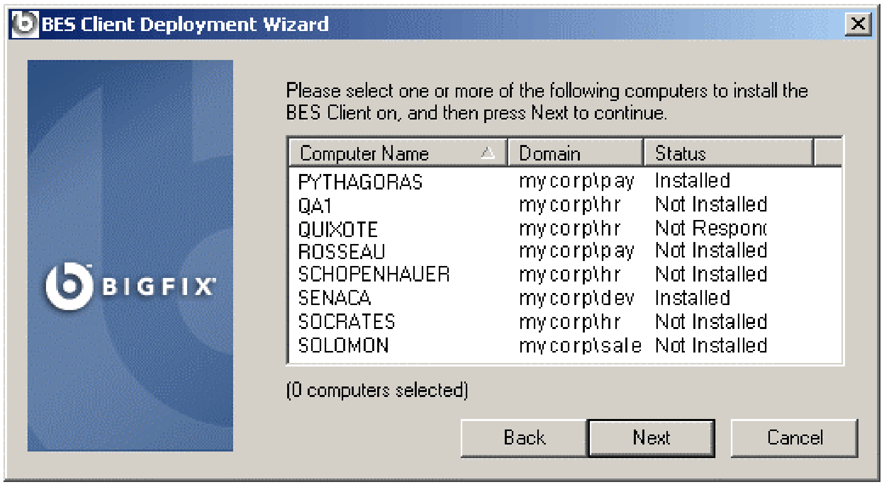
If the BES Client is not yet installed, the tool provides interfaces that allow you to issue a Remote Procedural Call that accesses the shared installer and -- with the proper domain administration credentials -- runs it silently, with no end user interaction. Here's how to use the tool:

1 The BES Client Deploy Tool is created by the BES Installation Generator. You can launch the tool from the BES Installation Guide or launch it directly from **Start > Programs >BigFix Enterprise > BES Client Deploy**.

  Note: You must be logged in as a domain administrator for the BES Client Deploy tool to work properly.

2 Select either **Active Directory** or **NT 4.0 Domains** to manage the BES Client rollout.

  - If you select **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 then checks each of the computers to see if the BES Client is already installed and displays them in a list.
  - If you select **NT 4.0 Domains**, all the computers in that domain are then listed, and each computer will have a status indicating whether the BES Client is already installed.



Please select one or more of the following computers to install the BES Client on, and then press Next to continue.

Computer Name	Domain	Status
PYTHAGORAS	mycorp\pay	Installed
QA1	mycorp\hr	Not Installed
QUIXOTE	mycorp\hr	Not Respon(
ROSSEAU	mycorp\pay	Not Installed
SCHOPENHAUER	mycorp\hr	Not Installed
SENACA	mycorp\dev	Installed
SOCRATES	mycorp\hr	Not Installed
SOLOMON	mycorp\sale	Not Installed

(0 computers selected)

3 When the list of computers is displayed, shift- and control-click to select the computers you want to administer with BES.

4 Click **Next**, type in your domain admin password and click **Next** again.

5 Using the supplied login credentials, the BES Client Deploy tool will copy the BES Client installer files to the computers you selected and then silently run the installer.

6 When completed, a log of successes and failures is displayed.

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've 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.

Using Software Distribution Tools

If you have access to a software distribution tool such as Microsoft SMS, IBM's Tivoli, 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. See the manufacturer's user manual for more information.

Using Remote NT Administration

Windows-based computers can be put under remote administration from a central NT/2000/XP computer, which allows direct execution of commands that can be used to install the BES Client on computers from a central location.

The only caveat is that any Windows 9x/Me computers on your network must first have remote administration enabled.

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. (Note: the BES Client does not come as a .msi package for GPO, but it can be packaged into a .msi using one of several third-party tools.)

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, do the following:

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).

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 user running setup.exe must have permission to install applications and write files, otherwise the installation will fail and a log file will not be created.

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.

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 a site administrator, you are in charge of each operator's domain and the specific rights they have over that domain.

There are two classes of operator: ordinary and master. As a site administrator, you will create a set of keys granting yourself master operator privileges. You will also create the keys for the other ordinary and master operators you want to appoint.

While ordinary operators are allowed to deploy actions and edit certain properties, master operators can also:

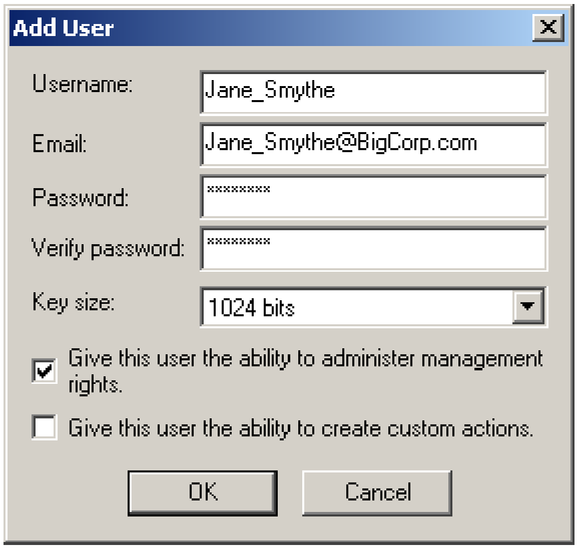
- Edit the management rights settings for other operators.
- Create new computer settings, which allow BES Clients to be labeled for various groupings.
- Create or edit retrieved properties, which are used to filter and sort computers.
- Change the BES Client heartbeat, to optimize BES performance.
- Subscribe or unsubscribe from Fixlet sites.
- Create Custom Actions (if that option is selected through BES Administration).

As a site administrator, you have the extra ability to authorize new operators. You can manage your team of operators and master operators by using the **BES Administration Tool**. This program is usually found in the start menu, under **Programs > BigFix Enterprise > BES Administration Tool**.

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:



Username: Jane_Smythe
Email: Jane_Smythe@BigCorp.com
Password: *********
Verify password: *********
Key size: 1024 bits

☑ Give this user the ability to administer management rights.
☐ Give this user the ability to create custom actions.

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 actions**. 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 actions across the entire network with just a few mouse clicks. This kind of power should not be delegated lightly. Use good judgment when granting these rights to operators.

9 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 (typically on a removable disk) and the name for the new folder (which will default to the operator's name). 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: 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:

- **license.crt:** the original action site certificate obtained from BigFix, Inc.
- **publisher.pvk:** 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.

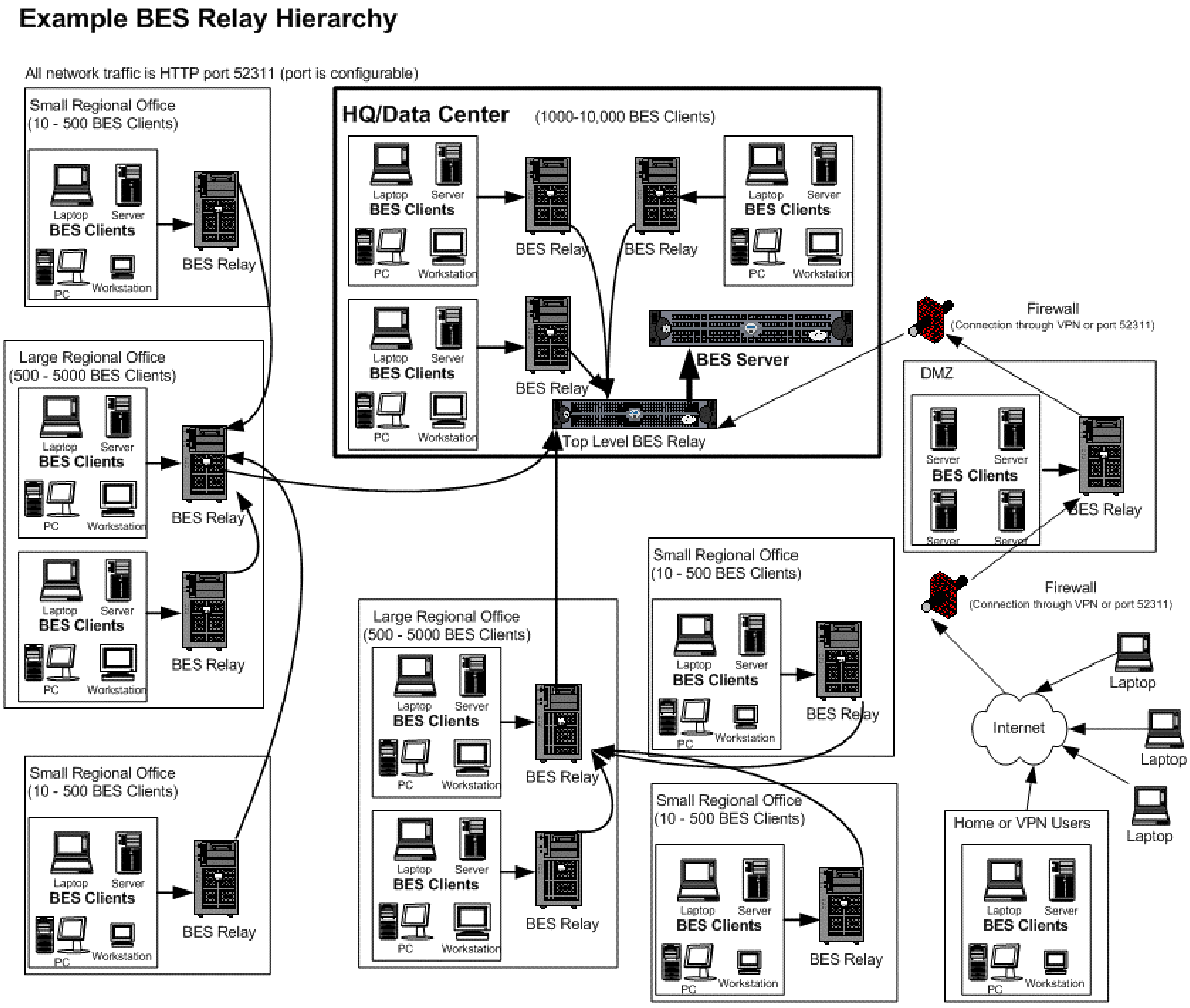
13 Once you've granted publishing rights to all your designated BES Console operators, click **OK**.

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.

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

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.



Example BES Relay Hierarchy

All network traffic is HTTP port 52311 (port is configurable)

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 patches 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. All the chores of a BES Server, including issuing action commands and pings, are taken over by the BES Relay.
- **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 VPN, designate one of those computers as a BES Relay. Then, instead of sending patches over the VPN 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 VPN bottleneck for remote groups on your network.

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 (Windows 2000 SP4 alone is more than 100MB) all at once. Without BES Relays, even network pipes as fast as T1 lines can be overwhelmed by such large requests.

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 *no significant WAN usage*.

BES Relays were designed to run on shared servers (file/print servers, domain controllers, SMS servers, AV distribution servers, etc.) with minimal impact. 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.

More information about BES Relays can be found by visiting http://support.bigfix.com/cgi-bin/redir.pl?page=besrelays, 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 from a BES Relay, a significant amount of the computer's resources (especially bandwidth) may be used to serve those files. Other than that, the duties of the BES Relay are not too demanding.

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, Norton/McAfee 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 2000, XP, or Server 2003 computers.
- More information about BES Relay requirements can be found at http://support.bigfix.com/cgi-bin/redir.pl?page=besrelays.

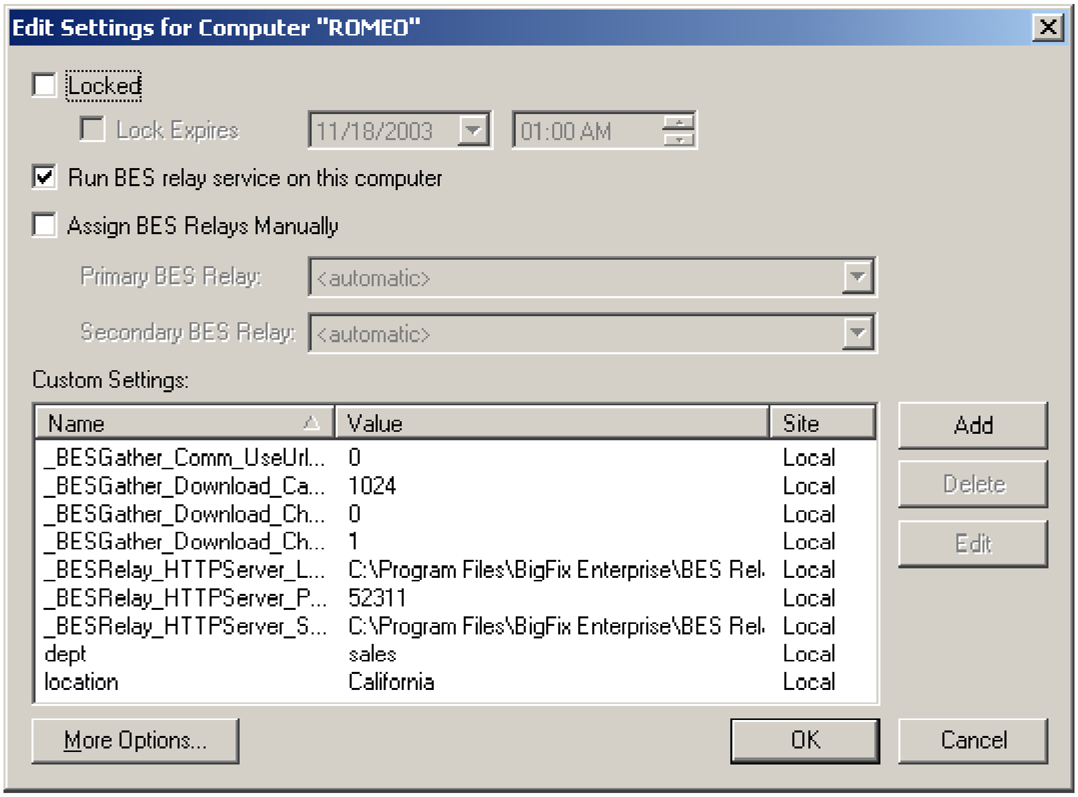
Designating a BES Relay

To set up a BES Relay, you need to designate a **Windows 2000, Server 2003,** or **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 **Computers** tab to bring up a tree/list of BES Clients.

2 From the computer list, right-click on the computer you want to designate as a BES Relay and select **Edit Computer Settings** from the pop-up menu (or select **Edit Computer Settings** from the **Edit** menu).

3 Check the box marked **Run relay service on this computer**.



Edit Settings for Computer "ROMEO"

□ Locked

□ Lock Expires 11/18/2003 01:00 AM

☑ Run BES relay service on this computer

□ Assign BES Relays Manually

Primary BES Relay: <automatic>

Secondary BES Relay: <automatic>

Custom Settings:

Name	Value	Site
_BESGather_Comm_UseUrl...	0	Local
_BESGather_Download_Ca...	1024	Local
_BESGather_Download_Ch...	0	Local
_BESGather_Download_Ch...	1	Local
_BESRelay_HTTPServer_L...	C:\Program Files\BigFix Enterprise\BES Rel.	Local
_BESRelay_HTTPServer_P...	52311	Local
_BESRelay_HTTPServer_S...	C:\Program Files\BigFix Enterprise\BES Rel.	Local
dept	sales	Local
location	California	Local

4 Click the **OK** button.

Note: If you would like to install the BES Relay in a non-default location, you must download the BES Relay installer and install it manually. Check http://support.bigfix.com/cgi-bin/redir.pl?page=besrelays for the latest download of the BES Relays. During the installation, you will be prompted for the installation path. Contact your support technician for more information.

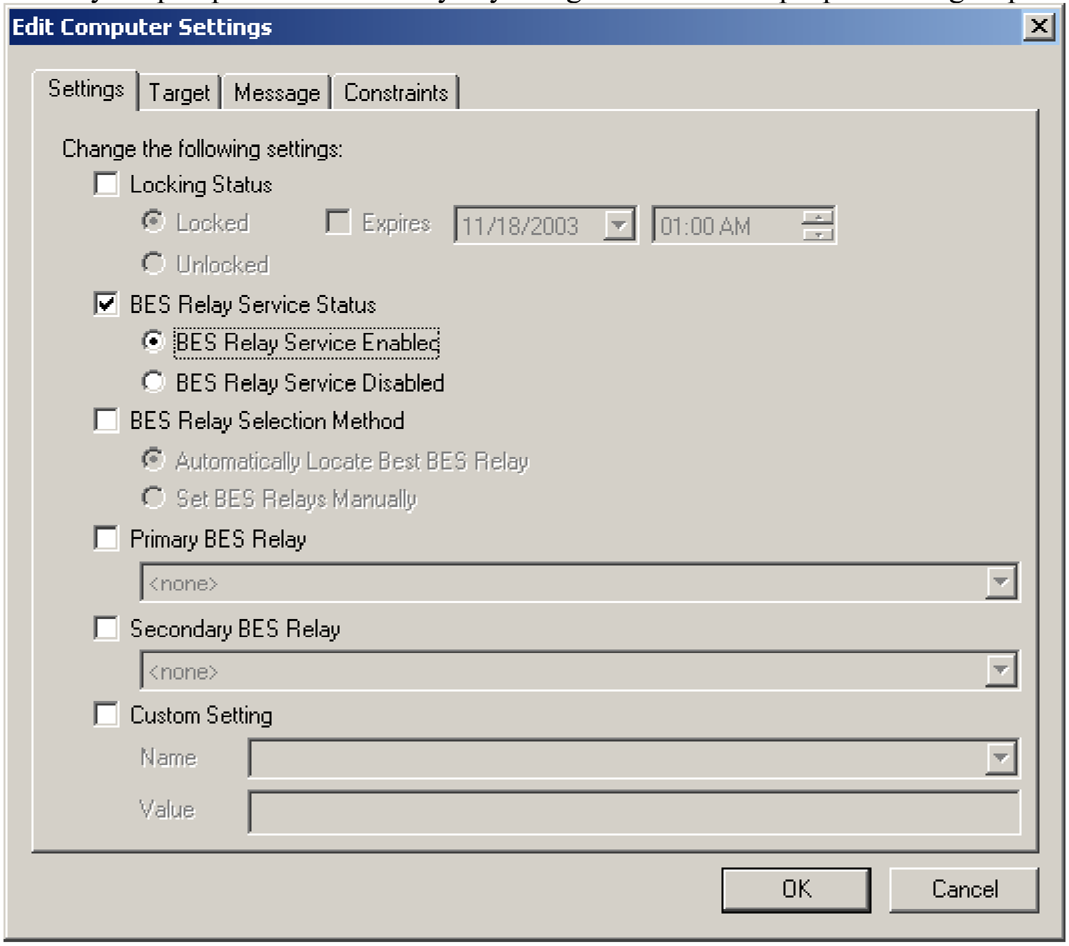
Designating multiple BES Relays

You can set up multiple BES Relays in a similar fashion. Follow these steps:

1 In the BES Console, click the **Computers** tab to bring up a filter/list of BES Clients.

2 From computer list, ctrl- or shift-click all the computers you want to designate as BES Relays.

3 Right-click on this highlighted set and select **Edit Computer Settings** from the pop-up menu (or select **Edit Computer Settings** from the **Edit** menu). If you want, you have a second chance to specify a group of computers by choosing the **Target** tab of this dialog. Select your prospective BES Relays by using their retrieved properties to group them.



Edit Computer Settings

Change the following settings:

□ Locking Status

● Locked □ Expires 11/18/2003 01:00 AM

○ Unlocked

☑ BES Relay Service Status

● BES Relay Service Enabled

○ BES Relay Service Disabled

□ BES Relay Selection Method

● Automatically Locate Best BES Relay

○ Set BES Relays Manually

□ Primary BES Relay

<none>

□ Secondary BES Relay

<none>

□ Custom Setting

Name

Value

4 Check the box marked **BES Relay Service Status**.

5 Click the button labeled **BES Relay Service Enabled** and click **OK**.

After the BES Relays have been created, the BES Clients can be configured to discover them automatically and connect to them. See the next sections for details.

Automatic Relay Discovery

Once you've set up your BES Relays, you're 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**.

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's 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 to enable **Manual Relay Selection**.
5. Then access the **Primary Relay Server**, and select a computer name from the drop-down list of available BES Relay servers.
6. Assign a **Secondary Relay Server**, which will be the backup whenever the Primary Relay Server is unavailable for any reason.
7. Click the **OK** button**.**

BES Relay Selection

To see which BES Clients are selecting which BES Relays, look in the BES Console under the "Relay" column (this column may be hidden so you will need to right-click on the column headings and make sure the "Relay" column is checked). The BES Relay column shows which BES Relay each computer is using. 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-bin/redir.pl?page=besrelays.

BES Relay Health

It is extremely important that the BES Relays and BES Clients in your network are properly configured. When everything is properly configured, even actions with large downloads can be successfully sent to tens of thousands of computers in just minutes. If not configured properly, even actions with small downloads can negatively impact your corporate WAN. Check http://support.bigfix.com/cgi-bin/redir.pl?page=besrelayshealth for more information about verifying the health of your BES Relay configuration.

Optimizing the BES Server

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 optimizations available from the BES Console (**File > Preferences**):

- 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).

- Slow down the **BES Client heartbeat**. 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. 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 you're 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.

Managing Bandwidth

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

The BES download manager can throttle the data stream. For more information About BES Relay/BES Client throttling, please visit http://support.bigfix.com/cgi-bin/redir.pl?page=besthrottling.

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**.

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 **Settings** tab, then click on the **Add new Database** link (under **Database Settings**).
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. Choose the option labeled **Use Username and Password to login**.
6. 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. Repeat steps 3-6 for each BES Server you wish to include.

Using an NT Authenticated Account

If you have access to the Microsoft SQL Server Enterprise Manager, and the servers are in the same domain, you can connect using NT authentication. Contact tech support for more information on how this can be accomplished.

Managing and Maintaining BES

Now that you've 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 user for the BES Console: operators and master operators.

- **Operators** can access the database and are authorized to issue actions across the network, according to their management rights.
- **Master Operators** are operators who can also assign management rights to other operators. A master operator therefore has a lot of power, and should be well-versed in corporate policy and security issues.

To add new operators and master operators to the BES system, simply repeat the steps outlined in **Adding BES Console Operators** (page 28).

Assigning Management Rights

In a typical BES deployment, there will be tens of thousands of computers sharing a centralized Fixlet database. Sometimes it is important to separate out which computers can be controlled by different BES Console operators for organizational, security or performance reasons.

A better way to organize a network of this size is to break it down into separate sections based upon geography, department, computer type (servers vs. workstations), etc. Each BES Console operator can be assigned management rights to the appropriate computers. For even larger networks, these departments can be broken down again. Because different managers 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's how to **Add** or **Delete** management rights:

1. Log in to the BES Console as an master operator with management rights (this must be a properly-authorized user name created with the BES Administration Tool). If you don't have the proper authorization, you will not be allowed to edit management rights.
2. Click on the **Console Operators** tab. 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. (If this choice is not available, you may not have the proper authorization to perform this command.)
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** folder, you can select a set of computers that share common properties or settings. For instance, you might assign all server computers to the server group. Or you might want to assign computers in a certain subnet to a local administrator. As new computers are added to the network, they will automatically be classified by their retrieved properties, 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.

Changing a BES Database Password

You can change your database password from the BES Console.

1 Select **Change Database Password** from the **File** menu.

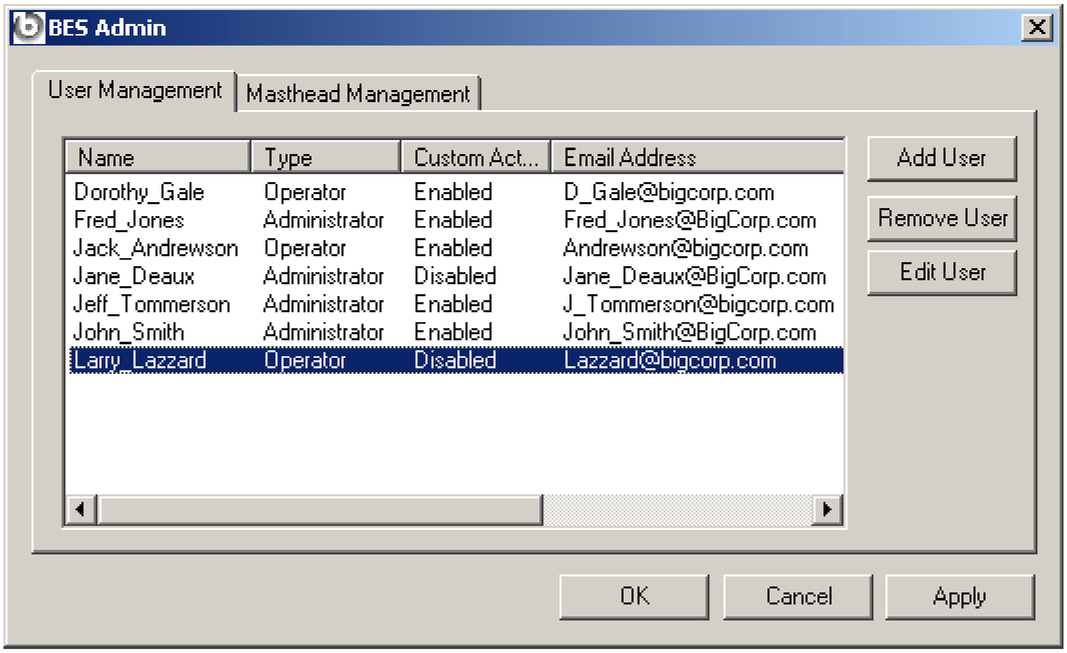
2 Type in your old password to authenticate yourself, then enter your new password and confirmation.

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**.



Name	Type	Custom Act...	Email Address
Dorothy_Gale	Operator	Enabled	D_Gale@bigcorp.com
Fred_Jones	Administrator	Enabled	Fred_Jones@BigCorp.com
Jack_Andrewson	Operator	Enabled	Andrewson@bigcorp.com
Jane_Deaux	Administrator	Disabled	Jane_Deaux@BigCorp.com
Jeff_Tommerson	Administrator	Enabled	J_Tommerson@bigcorp.com
John_Smith	Administrator	Enabled	John_Smith@BigCorp.com
Larry_Lazzard	Operator	Disabled	Lazzard@bigcorp.com

3 When you've 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**.

Editing the Masthead

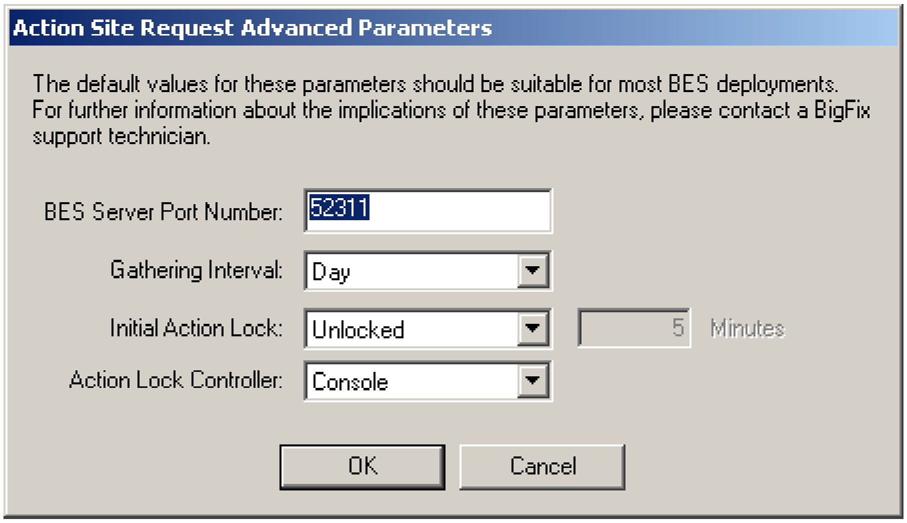
You can change certain default parameters stored in the masthead for the BES system by using the **BES Administration Tool**. Here's how:

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.



Action Site Request Advanced Parameters

The default values for these parameters should be suitable for most BES deployments. For further information about the implications of these parameters, please contact a BigFix support technician.

BES Server Port Number: 52311

Gathering Interval: Day

Initial Action Lock: Unlocked 5 Minutes

Action Lock Controller: Console

The parameters are:

- **The BES Server Port Number.** In general, you won't want to change this number.

  Note: If you decide to change this number after deploying the BES Clients, BES will not work correctly. See **Modifying Port Numbers**, below.

- **The 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 doesn't gather information it already has.

- **The 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).

- **The 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.

5. Click **OK** to enter the changes.
6. Enter your site password at the prompt, allowing the new configuration changes to be sent to the BES Clients across your network.

Modifying Port Numbers

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

The BES Server uses port **52311** to communicate with the BES Clients. It's highly unlikely, but should you have a conflict you can change this port number as well. Choose a custom port from the IANA pool of unassigned, dynamically allocated IP port numbers.

These ports are for internal use only – for security reasons, be sure that they're opened on internal firewalls/routers within your enterprise and blocked against inbound or outbound 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.***

1. Launch the BES Administration program from **Start > Programs > BigFix Enterprise > BES Administration Tool**. (If you don't find the program listed there, do a Find File for BESAdmin.exe).
2. Browse to the location of your site license and click **OK**.
3. Select the **Masthead Management** tab.
4. Click the **Edit Masthead** button.
5. Enter the desired **BES Server Port Number** and click **OK**.
6. Enter your site password at the prompt, allowing the new masthead to be propagated across your network.

WARNING! If you change the port number that BES uses to communicate, you will have to re-deploy all of your BES components. Consult with your network administrator to make sure that you choose an appropriate port ***before*** installation.

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 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) and re-create all the users. If this happens, please contact your support technician. To protect your site certificate, obey these important rules:

- **Don’t lose the private key for your site** (saved in the file named **license.pvk**). Follow your standard procedures for duplicating and securing infrastructure-critical confidential information.
- **Don’t change the IP address/hostname or port number of the BES Server**, because it’s the primary identifier for your site certificate. Any change to the IP address/hostname 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.
- **Don’t forget your password.** Follow your corporate standards for noting and storing your 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're 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 is 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 update the BES components, you can also 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.

Maintaining and Troubleshooting BES

If you're 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 20.
- Check the BigFix Knowledge Base at http://support.bigfix.com/. This site is continually updated, and if you can't 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.

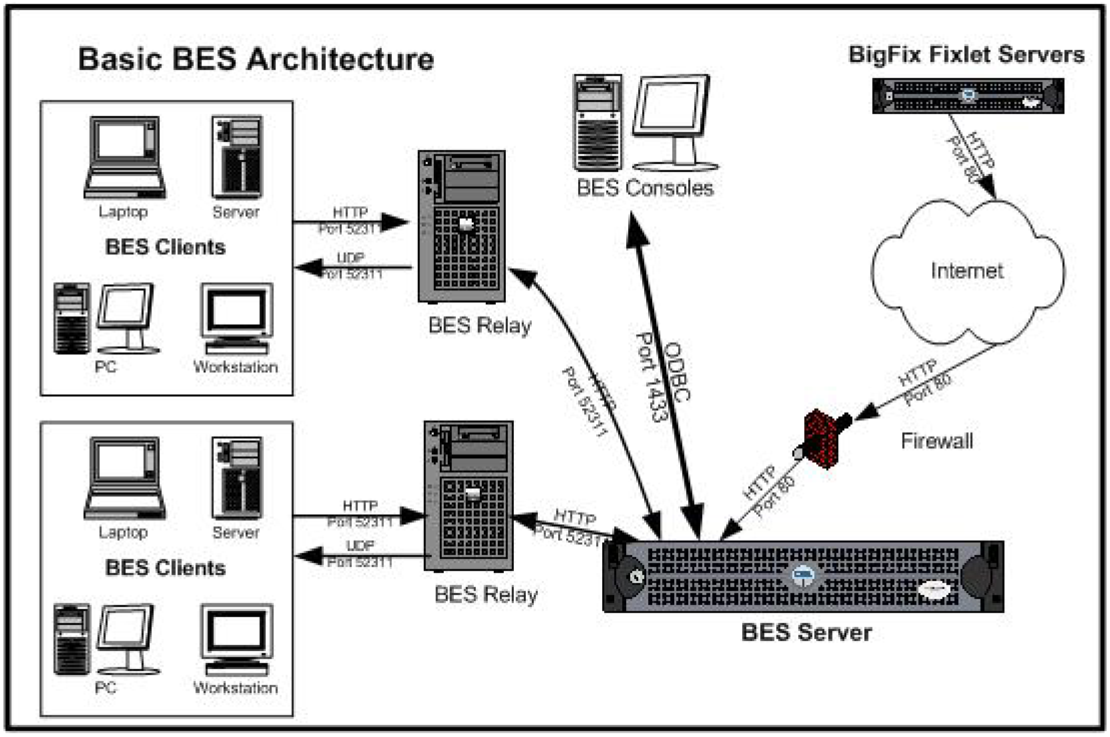
Deployment Scenarios

The following deployment scenarios illustrate optimal configurations, taken from actual case studies. Pay careful attention to the BES Relay distribution in each scenario.

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

Standard Deployment

For the sake of clarity and brevity, this guide has concentrated on a typical deployment: an organization with a central BES Server and fewer than 75,000 BES Clients (see **A Typical Installation**, page 4). Here's a diagram of a standard BES deployment:



Note the following about the diagram:

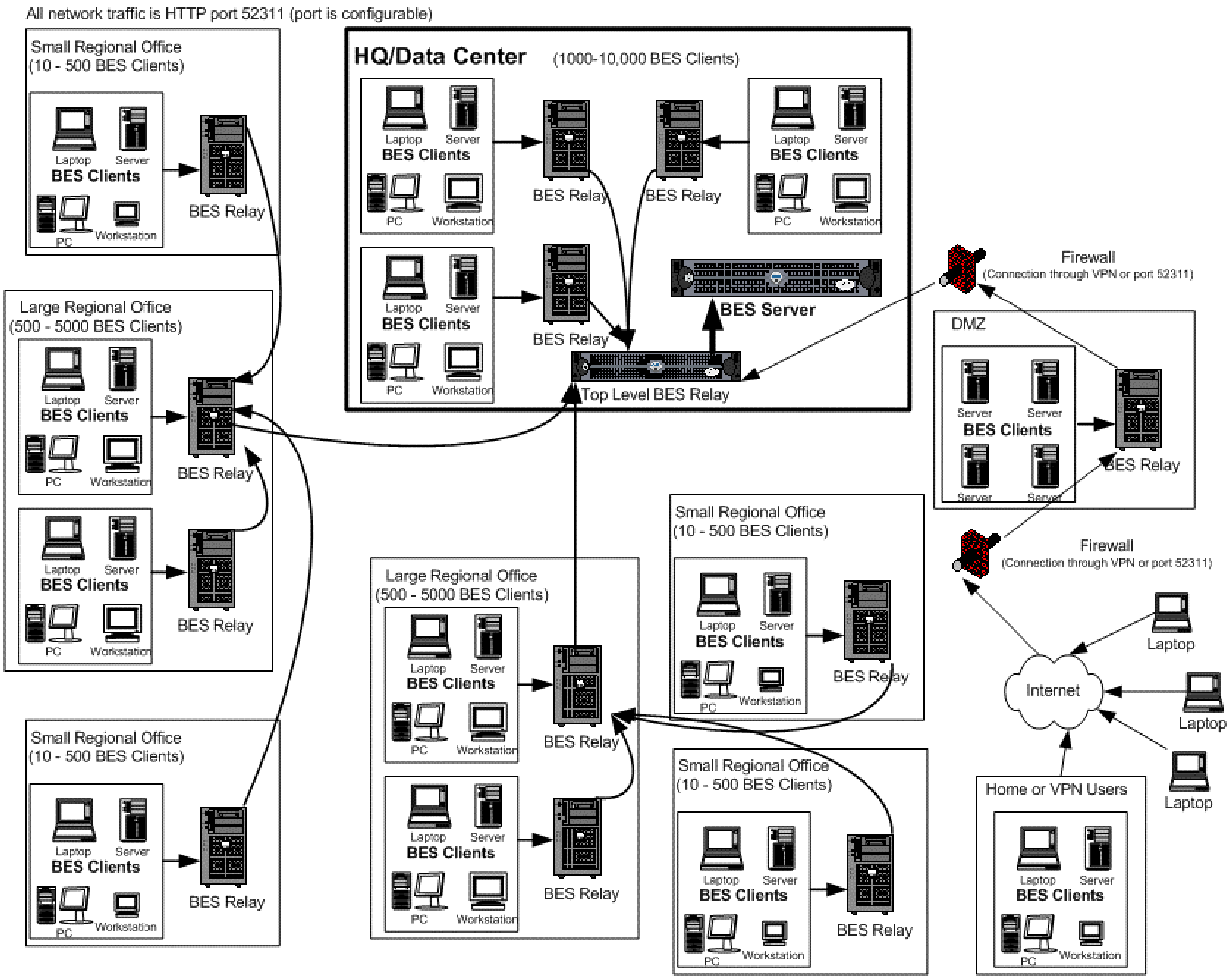
- BES Relays are used to share the server load. Typically a BES Relay is deployed for every 500-1,000 computers.
- Information comes in from the Internet (across the firewall), but never goes out.

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.

Efficient BES Relay Setup

To increase efficiency and reduce latency, this company has set up BES Relay computers to help relieve the server load. Each BES Relay they add takes an extra burden off the 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.

Example BES Relay Hierarchy


All network traffic is HTTP port 52311 (port is configurable)
HQ/Data Center (1000-10,000 BES Clients)
Small Regional Office (10 - 500 BES Clients)
Large Regional Office (500 - 5000 BES Clients)
Laptop
Server
BES Clients
PC
Workstation
BES Relay
BES Server
Top Level BES Relay
Firewall (Connection through VPN or port 52311)
DMZ
Internet
Home or VPN Users

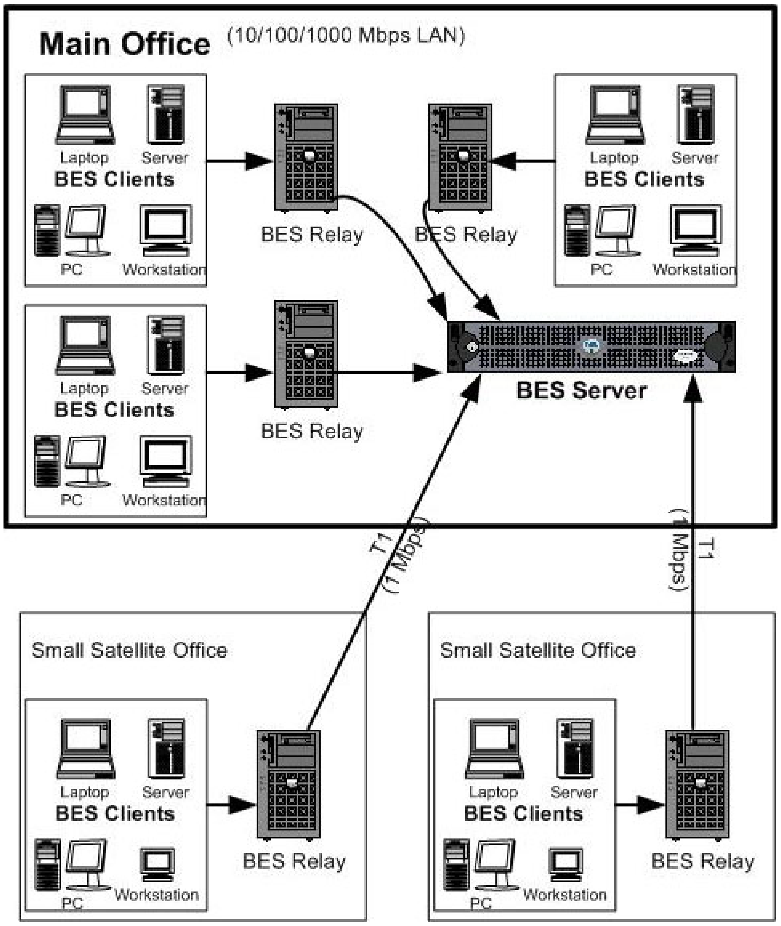
Note the following about the diagram:

- 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.* If there is a bandwidth bottleneck, then the BES Relays should be configured to point to other BES Relays nearby. In the picture above, there is limited bandwidth between offices so the BES Relays in the regional offices all go through a single BES Relay for downloads and to post their data.

- There is a BES Relay in the DMZ set up with a special trust relationship with the BES Server. This BES Relay will allow connections to computers in the DMZ or outside the LAN.
- As a general rule, you should deploy at least one BES Relay per 500-1000 BES Clients to optimize bandwidth.
- See http://support.bigfix.com/bes/misc/besrelays.html for more information.

One Main Office

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.



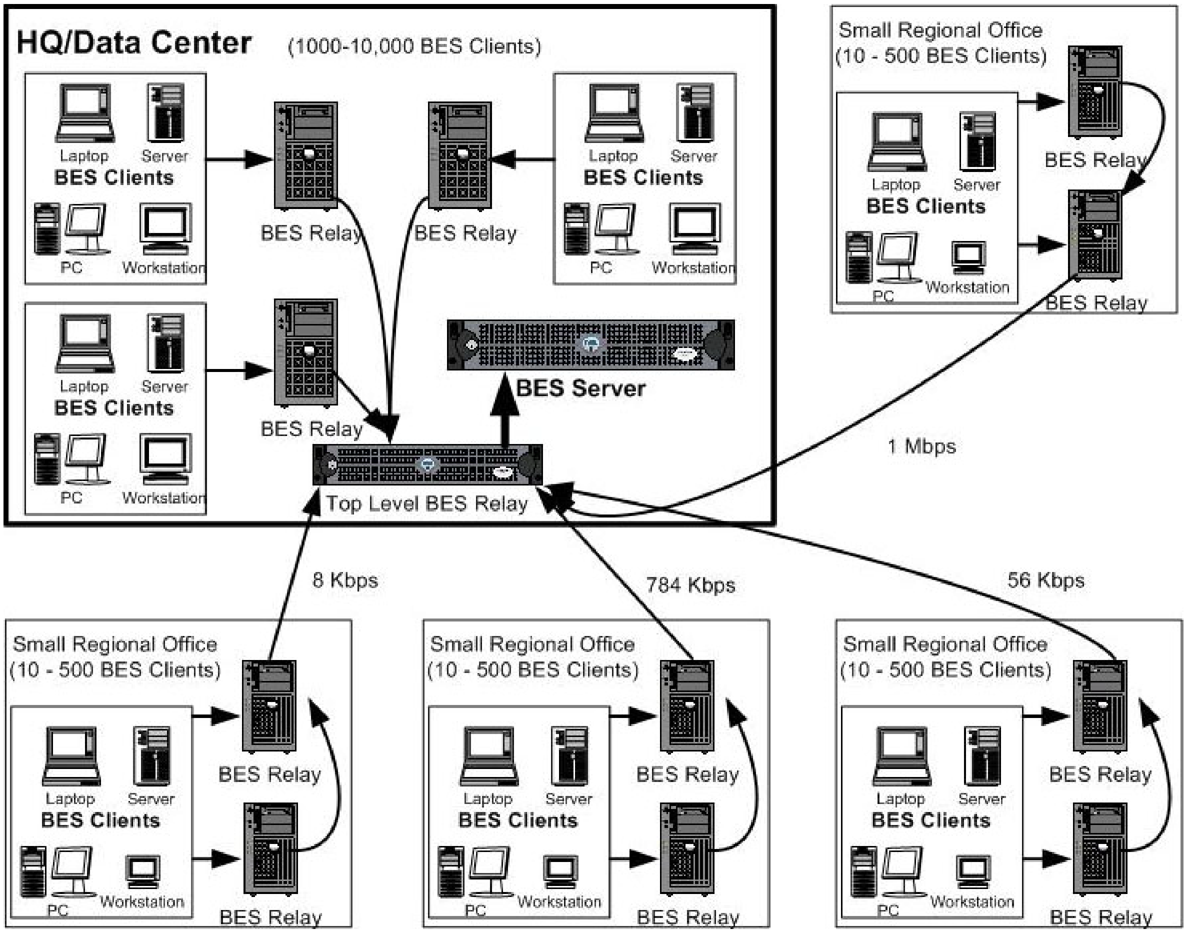
Note the following about the diagram:

- 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 fat WAN pipes. A thin WAN could force a change in the layout of the BES Relays (see the scenarios 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. Since any BES Relay is thus equally beneficial, the BES Clients simply choose one at random. Despite this seeming arbitrariness, there are still great benefits to automatic relay selection: the load gets efficiently distributed across all the BES Relays and you don't need to manually assign each individual BES Client.
- 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 any single office has over 20,000 BES Clients, another level of BES Relays should be considered.

One Main Office, Smaller Regional Offices

This configuration is common in many mid-size and large companies that have many small offices, but do not have large regional centers. Small WAN pipes are common in the remote offices. The BES Clients are installed on computers in offices all around the world. Many of these locations have slow WAN connections (8 kbps-128kbps), but there will be many offices with faster WAN connections (1mbps-45mbps).



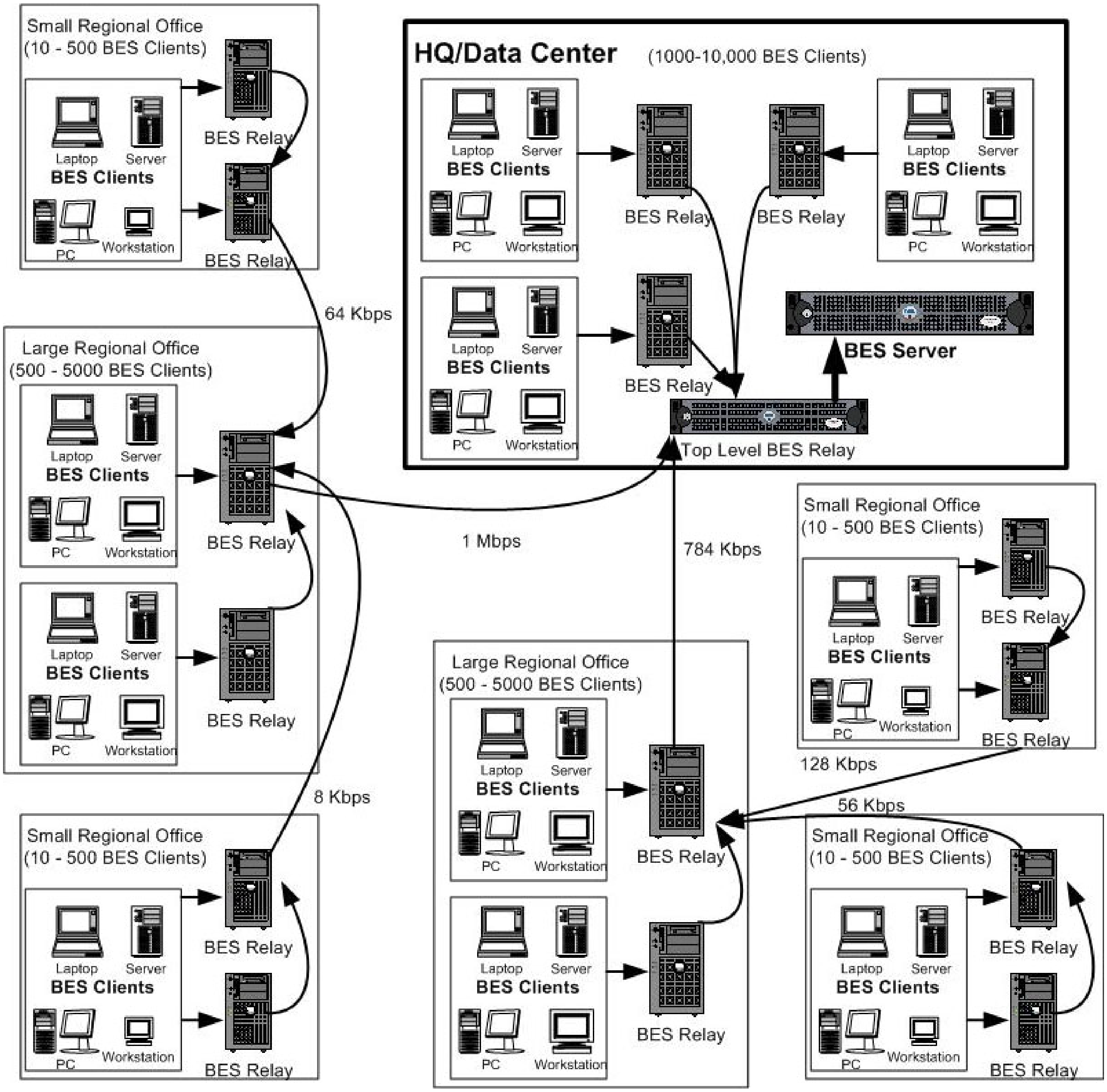
Note the following about the diagram:

- 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. The BES Relay can usually be installed on these existing computers.
- To provide redundancy, more than one BES Relay should be installed in each of these locations. In case one of the BES Relays fail for any reason (it is turned off, the network connection is lost, etc.), its attached BES Clients can then automatically fail-over to a different 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. Use **Web Reports** to verify your BES Relay connections. Talk to your support technician for more details on how to protect against overutilizing WAN pipes with BES.
- 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-bin/redir.pl?page=besthrottling 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.
- All BES Relays are manually configured to point to either a BES Relay in the same office or the top-level BES Relay.

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-128kbps), 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. The BES Relay is usually installed on these existing computers.
- To provide redundancy, more than one BES Relay should be installed in each of these locations. In case one of the BES Relays fail for any reason (it is turned off, the network connection is lost, etc.), its attached BES Clients can then automatically fail-over to a different 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. Use **Web Reports** to verify your BES Relay connections. Talk to your support technician for more details on how to protect against overutilizing WAN pipes with BES.
- 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-bin/redir.pl?page=besthrottling 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.

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's 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 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.

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.

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 BigFix Client obtains Fixlet messages.

IIS—See Internet Information Services.

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

Internet Information Services (IIS)—BES is optimized to be used with a Windows 2000 Server computer running IIS.

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's 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 doesn't 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.

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's 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.

Index