Tivoli. Endpoint Manager
Version 8.1

Administrator's Guide

IBM®

Note: Before using this information and the product it supports, read the information in Notices.

Contents

Part One

Introduction

Tivoli® Endpoint Manager aims to solve the increasingly complex problem of keeping your critical systems updated, compatible, and free of security issues. It uses patented Fixlet® technology to identify vulnerable computers in your enterprise. With just a few mouse-clicks you can remediate them across your entire network from a central Console. Fixlet messages are powerful, flexible, and easily customized. Utilizing Fixlet technology, you can:

- Analyze vulnerabilities (patched or insecure configurations)
- Easily and automatically remediate all your networked endpoints
- Establish and enforce configuration policies across your entire network
- Distribute and update software packages
- View, modify, and audit properties of your networked client computers

Fixlet technology allows you to analyze the status of configurations, vulnerabilities, and inventories across your entire enterprise and then enforce policies automatically in near real-time. In addition, administrators can create or customize their own Fixlet solutions and Tasks to suit their specific network needs.

Tivoli Endpoint Manager is easy to install and has built-in public/private-key encryption technology to ensure the authenticity of Fixlet messages and actions. It grants you maximum power as the administrator, with a minimal impact on network traffic and computer resources. Tivoli Endpoint Manager can handle hundreds of thousands of computers in networks spanning the globe.

When installed, you can easily keep your networked computers correctly configured, updated, and patched, all from a central Console. You can track the progress of each computer as updates or configuration policies are applied, making it easy to see the level of compliance across your entire enterprise. In addition to downloads and security patches, you can also examine your managed computers by specific attributes, allowing you to group them for action deployments, ongoing policies, or asset management. You can log the results to keep an audit trail and chart your overall activity with a convenient web-based reporting program.

Audience

This guide is for administrators and IT managers who want to install and administer Tivoli Endpoint Manager. It details the system requirements for each of the components and provides licensing and installation instructions that allow you to deploy the program in your environment. It also includes information about configuring and maintaining Tivoli Endpoint Manager. See the *Tivoli Endpoint Manager Console Operator’s Guide* for operating instructions and further information about the performance of the various product components, including Tivoli Endpoint Manager Servers, Relays and Clients.

Versions

The guide includes the functions introduced in Tivoli Endpoint Manager, Version 8.1.

Terms used in this guide

The following terms are all Tivoli Endpoint Manager terms, but are used throughout the guide without being labeled every time with Tivoli Endpoint Manager:

- **Console** always means Tivoli Endpoint Manager Console
- **Client** always means Tivoli Endpoint Manager Client
- **Server** always means Tivoli Endpoint Manager Server
- **Relay** always means Tivoli Endpoint Manager Relay

In addition, you might see these components labeled with "BigFix" or "BigFix Enterprise Suite" (BES), which is legacy terminology, now superseded by "Tivoli Endpoint Manager".

Overview of the Tivoli Endpoint Manager System

The Tivoli Endpoint Manager system has the following main components:

- **Tivoli Endpoint Manager Clients**, also called Agents, are installed on every computer that you want to manage under Tivoli Endpoint Manager. They access a collection of Fixlet messages that detects security holes, improper configurations, and other vulnerabilities. The Client can then implement corrective actions received from the Console through the Server. The Tivoli Endpoint Manager Client runs undetected by users using a minimum of system resources. However, the Tivoli Endpoint Manager also allows the administrator to provide screen prompts for those actions that require user input. Tivoli Endpoint Manager Clients can encrypt their upstream communications, protecting sensitive information. Tivoli Endpoint Manager Client software can run under Windows®, Linux®, Solaris, HP-UX®, AIX®, and Macintosh operating systems.

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

- **Tivoli Endpoint Manager Relays** increase the efficiency of the system. Instead of forcing each networked computer to directly access the Tivoli Endpoint Manager Server, relays spread the load. Hundreds to thousands of Tivoli Endpoint Manager Clients can point to a single Tivoli Endpoint Manager Relay for downloads, which in turn makes only a single request of the server. Tivoli Endpoint Manager Relays can connect to other relays as well, further increasing efficiency. A Tivoli Endpoint Manager Relay does not need to be a dedicated computer; the software can be installed on any Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Red Hat Enterprise Linux 4/5/6, or Solaris 10, computer with the Tivoli Endpoint Manager Client installed. As soon as you install a Tivoli Endpoint Manager Relay, the Clients on your network have the ability to automatically discover and connect to them.

- **Tivoli Endpoint Manager Consoles** join all these components together to provide a system-wide view of all the computers in your network, along with their vulnerabilities and suggested remedies. The Tivoli Endpoint Manager Console allows an authorized user to quickly and simply distribute fixes to each computer that needs them without impacting any other networked computers. The Tivoli Endpoint Manager Console can be run on any Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2 computer that has network access to the Tivoli Endpoint Manager Server. Consoles for large deployments are often hosted from Terminal Servers or Citrix® Servers.

Using this Guide

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

- The Tivoli Endpoint Manager Servers are able to make connections to the Internet on port 80. The Tivoli Endpoint Manager Server can be set up to use a proxy, which is a common configuration. Alternatively, an air-gap can be used to physically separate the Tivoli Endpoint Manager Server from the Internet Fixlet Server (for more information, see the article on air-gaps at the Tivoli Endpoint Manager support site).
- Each Tivoli Endpoint Manager Server must have access to the SQL server, located locally on the Server machine or remotely on a separate SQL Server.
- Each Console operator can make an ODBC connection to the database and an HTTP connection to the Tivoli Endpoint Manager Server.
- Each Tivoli Endpoint Manager Client computer in the network must be able to make an HTTP connection to a Server or a Relay on the specified port (the default port is 52311, but any available port will serve).

Some enterprises will violate one or more of these conditions, but the Tivoli Endpoint Manager can still be deployed in these environments; see **Deployment Scenarios** (page 88) for more information. If your network configuration does not match any of the scenarios in that chapter, contact a support technician for more options.

The initial deployment of a minimal Tivoli Endpoint Manager system (Server, Console, and a few Clients) should take about an hour to complete.

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

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

Tivoli Endpoint Manager Operating Requirements

Tivoli Endpoint Manager runs efficiently using minimal server, network, and client resources. The requirements for the Client programs are not stringent. The hardware required by the Server and the Console depends on the number of computers that are administered and the total number of Consoles. The distributed architecture of Tivoli Endpoint Manager allows a single Server to support hundreds of thousands of computers.

Tivoli Endpoint Manager Server Requirements

The Tivoli Endpoint Manager Server is supported on Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2. The supported versions of SQL Server are SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.

SQL 2005 Express Edition is not recommended for use in production deployments. For more information, see the knowledge-base article on MSDE at the Tivoli Endpoint Manager support site.

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

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

The exact hardware requirements for the Tivoli Endpoint Manager Servers vary depending on how many Clients are attached. The latest references on Tivoli Endpoint Manager Servers can be found at the Tivoli Endpoint Manager support site. Consult your support technician for more information about Tivoli Endpoint Manager Server requirements.

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

- All internal network communication will be on one specified port (52311 is the default) to allow for simplicity and flexibility of deployment. TCP/IP and UDP on this port must be completely unblocked at all internal routers and internal firewalls (you can optionally disable UDP but that might negatively affect performance).
- The Tivoli Endpoint Manager Server should connect to the network at 100 mbps or higher.
- The Tivoli Endpoint Manager Consoles must be able to make connection to the SQL Server database using ODBC. Consoles should have high speed connections to the Tivoli Endpoint Manager Server (100 mbps or higher)
- The Windows Firewall must be turned off on the Tivoli Endpoint Manager Server machine.
- The Tivoli Endpoint Manager Client must be installed on the Tivoli Endpoint Manager Server machine.

These networking recommendations are typically easy to satisfy for most organizations maintaining a moderate security posture. If these requirements cannot be met in your organization, see **Configuring the Tivoli Endpoint Manager Components** (page 52). For information about larger installations, see **Deployment Scenarios** (page 88).

The Tivoli Endpoint Manager Server requirements and performance can also be affected by other factors in addition to the number of Clients. These include:

- **The number of Console Operators.** Multiple Console operators can connect to the Servers at the same time to manage subsets of the networked computers. Some deployments can have hundreds of operators. If you plan on having more than 30 operators, you might want to have a more powerful Server to support the additional load.
- **Relays.** Relays should be used to lighten the load on the Servers by accepting connections from Clients and then forwarding the data to a Server. In most deployments, very few Clients report directly to the main Server.
- **The number and type of Retrieved Properties and Analyses.** Custom-Retrieved Properties and Analyses can provide extremely useful data, but if custom properties are poorly implemented or overused, they can also create undue load on the system by requiring too much bandwidth or too many Client resources. For example, it would be unwise to create a custom-retrieved property that returned the names of every file on every computer, due to the load on the client computers and the network.

For more information about these performance issues, consult the Tivoli Endpoint Manager support site.

Console Requirements

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

- **Hardware:** Intel Pentium III–class processor with 512 MB RAM. Larger deployments require more capable computers.
- **Software:** Windows XP, 2003 Vista, 2008, 7, or 2008 R2 with Internet Explorer version 7.0 or later.

The Tivoli Endpoint Manager Console can be installed on a laptop or any moderately-powerful computer. However, as the number of computers that you are managing with the Console grows, you might need a more powerful computer. The latest Console recommendations can be found at the Tivoli Endpoint Manager support site.

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

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

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

Client Requirements

The Tivoli Endpoint Manager Client can run on computers that meet the following minimum requirements:

- **Hardware:** x86-based computers, Mac or SPARC with 32 MB RAM and 20 MB free hard disk space. Extra temporary disk space might be required for some patches.
- **Software:** Windows 2000, Server 2003, XP, Vista, 2008, 7, 2008 R2 Red Hat® Linux 8.0, & 9.0, Red Hat Linux Enterprise 3/4/5/6, Red Hat Fedora Core 3.0, 4.0 and 5.0, Solaris 8, 9, and 10, HP-UX 11.00 and 11.11, AIX 5.1, 5.2 and 5.3, SUSE® 8, 9, and 10, Mac® OS X 10.3 and 10.4.

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

You can find the latest Client at the Tivoli Endpoint Manager support site.

Database Requirements

Tivoli Endpoint Manager requires SQL Server 2005, 2008, or 2008 R2, which will store all of the data retrieved from the Clients.

Security Requirements

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

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

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

Whenever operators issue an action, it must be signed by their private publisher key. Then when the Client receives the action, it validates the signature using the public key information. If the signature validation fails on the Client, the operator's action is discarded. This prevents unauthorized personnel from using the 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 Tivoli Endpoint Manager root for authentication. This signature must match the Fixlet site's masthead, which is placed in the Client install folder when 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 Tivoli Endpoint Manager in your organization:

- Make sure the Server computer is running Windows Server 2003+ with the latest Service Pack available from Microsoft.
- Make sure that the SQL Server is secured with the latest security-related patches.
- Verify that your network firewall forbids inbound and outbound traffic on the specified port (default 52311) so that Tivoli Endpoint Manager-related traffic will be unable to flow into or out of your network.

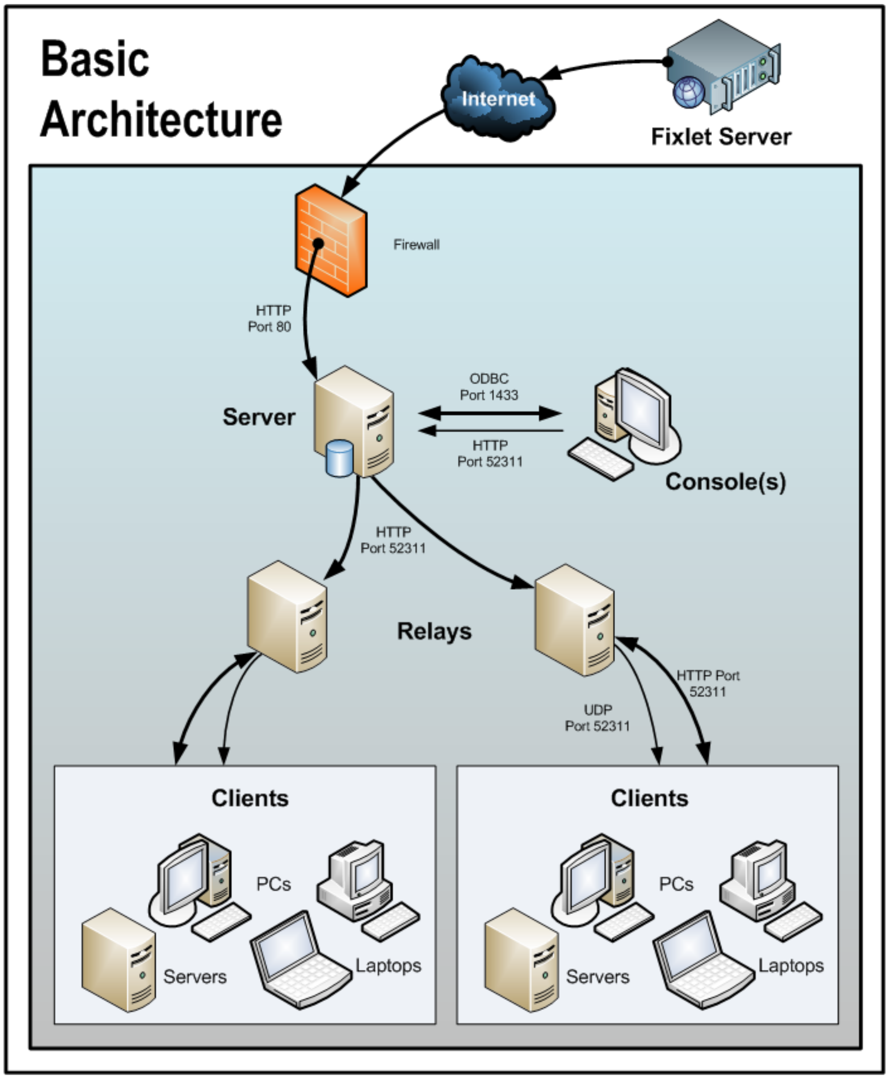
  It is possible to administer roaming laptops by opening this port on your firewall. However, a better technique is to use message-level encryption to route the relay through a non-default port and avoid opening this port altogether.
- Make sure that TCP/IP and UDP on the specified port (default 52311) is completely unblocked at all internal routers and internal firewalls.
- Verify with your network administrator that you can allow the Server to access the Internet via port **80**. The Tivoli Endpoint Manager Gather service is the only component of the 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 must set the Tivoli Endpoint Manager Gather service to log on as a user with Internet and administrative access on the Server computer. Detailed instructions about how to configure the server are available from the knowledge base at the Tivoli Endpoint Manager support site.

  It is also possible to maintain a physical disconnect from the Internet with an air-gapped implementation as described in the KB article at the Tivoli Endpoint Manager support site.
- Secure the Server computers and the SQL or SQLite database using company or industry-wide standards. Contact your network administrator or database administrator for more information.

Note: Certain rare lockdown procedures might cause the Servers to function imcorrectly. Contact your IBM software support if you have any specific questions about lockdown procedures.

A Basic Installation

A simplified Tivoli Endpoint Manager deployment resembles the diagram below. There is at least one Server that gathers Fixlet messages from the Internet where they can be viewed by the Console operator and distributed to the Relays. Each Client inspects its local computer environment and reports any relevant Fixlet messages back to the Relay, which compresses the data and passes it back up to the servers.



The Tivoli Endpoint Manager Console oversees all this activity. It connects to the Servers and periodically updates its displays to reflect changes or new knowledge about your network.

The Tivoli Endpoint Manager Console operator can then target actions to the appropriate computers to fix vulnerabilities, apply configuration policies, deploy software, and soon. The progress of the actions can be followed in near real-time as they spread to all the relevant computers and, one by one, address these critical issues.

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

Note: The arrows in the diagram illustrate the flow of information throughout the enterprise. The arrows from the Fixlet Server to the Servers represent the flow of Fixlet messages into your network. Clients gather Fixlet messages and action information from Relays. They then send small amounts of information back to the Servers through the Relays. The UDP packets from the Relay to the Clients are small packets sent to each Client to inform them that there is new information to be gathered. The UDP messages are not strictly necessary for the Tivoli Endpoint Manager to work correctly. View the article on network traffic at the Tivoli Endpoint Manager support site, or ask your support technician for more details.

Message Level Encryption (MLE) Overview

Message Level Encryption (MLE) allows your Clients to encrypt upstream data using a combination of an RSA public/private key-pair and an AES session key.

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

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

There are three levels of report encryption:

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

A Typical Installation

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

A Multiple Server Installation

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

- Continued service availability on both sides of a network split (automatic failover).
- Continued availability in the event of a server outage.
- Distribution of Console database load during normal operation.
- Automatic failback upon reconnection.

To take advantage of this function, you need one or more additional servers with a capability at least equal to your primary server. All Tivoli Endpoint Manager servers in your deployment must run the same version of SQL Server. If your existing Server is running SQL 2005, your new servers must run SQL 2005 as well.

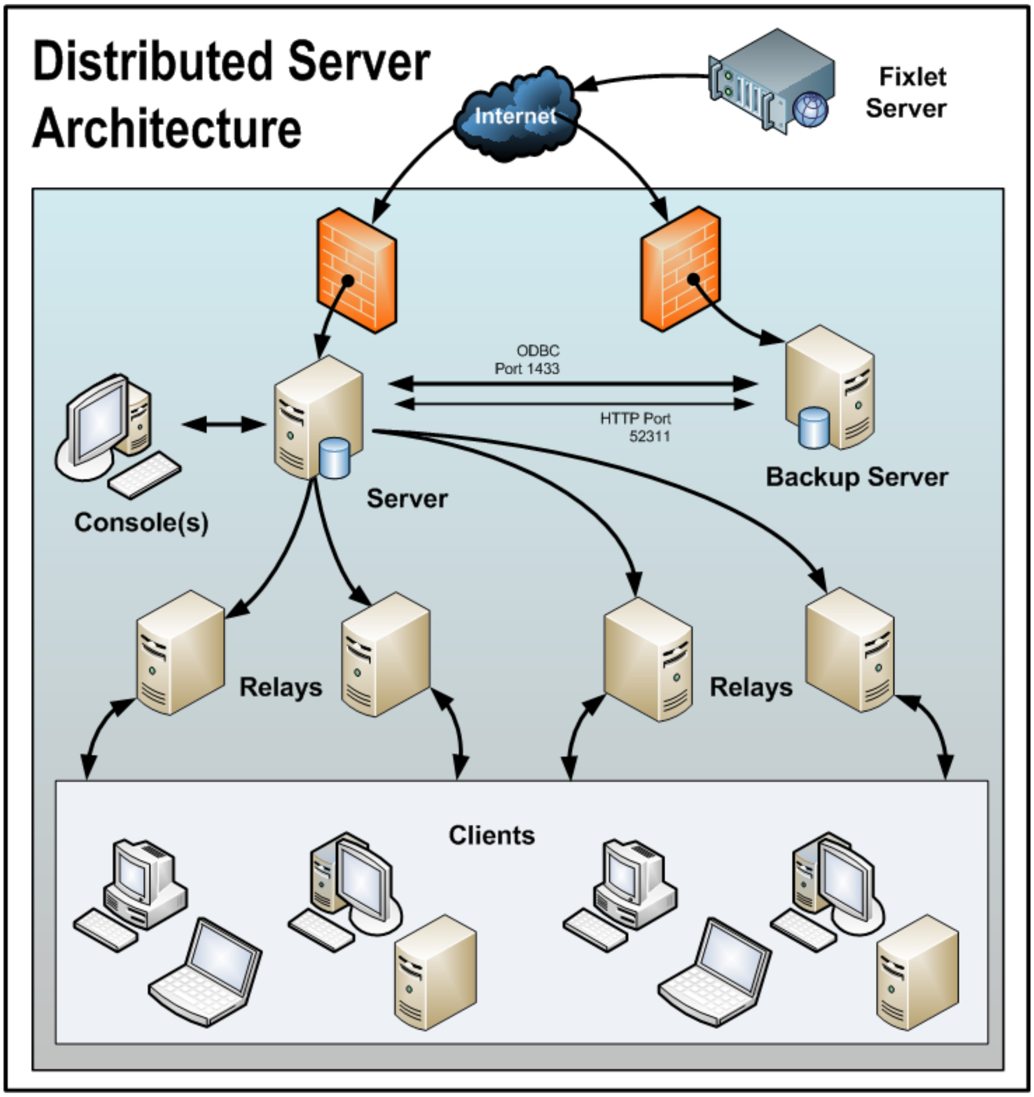
Understanding Replication

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

- Servers communicate on a regular schedule to replicate their data. You review the current status and adjust the replication interval through **Tivoli Endpoint Manager Administration Tool > Replication**.
- When each server is ready to replicate from the other servers in the deployment, it calculates the shortest path to every other server in the deployment. Primary links are assigned a length of 1, secondary links 100, and tertiary links 10,000. Links which resulted in a connection failure the last time they were used are considered to be non-connected.
- When an outage or other problem causes a network split, it is possible for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected, precedence goes to the version on the server with the lowest Server ID.
- If multiple copies of **Web Reports** are installed, they operate independently. Each Web Report Server can connect to the Server that is most convenient, because they all contain equivalent views of the database.
- By default, server 0 (zero) is the master server. The **Tivoli Endpoint Manager Administration Tool** only allows you to perform certain administrative tasks (such as creating and deleting users) when connected to the master server.
- If you want to switch the master to another server, you can do so with a setting. For more information, see the section on **Managing Replication** (page 63).

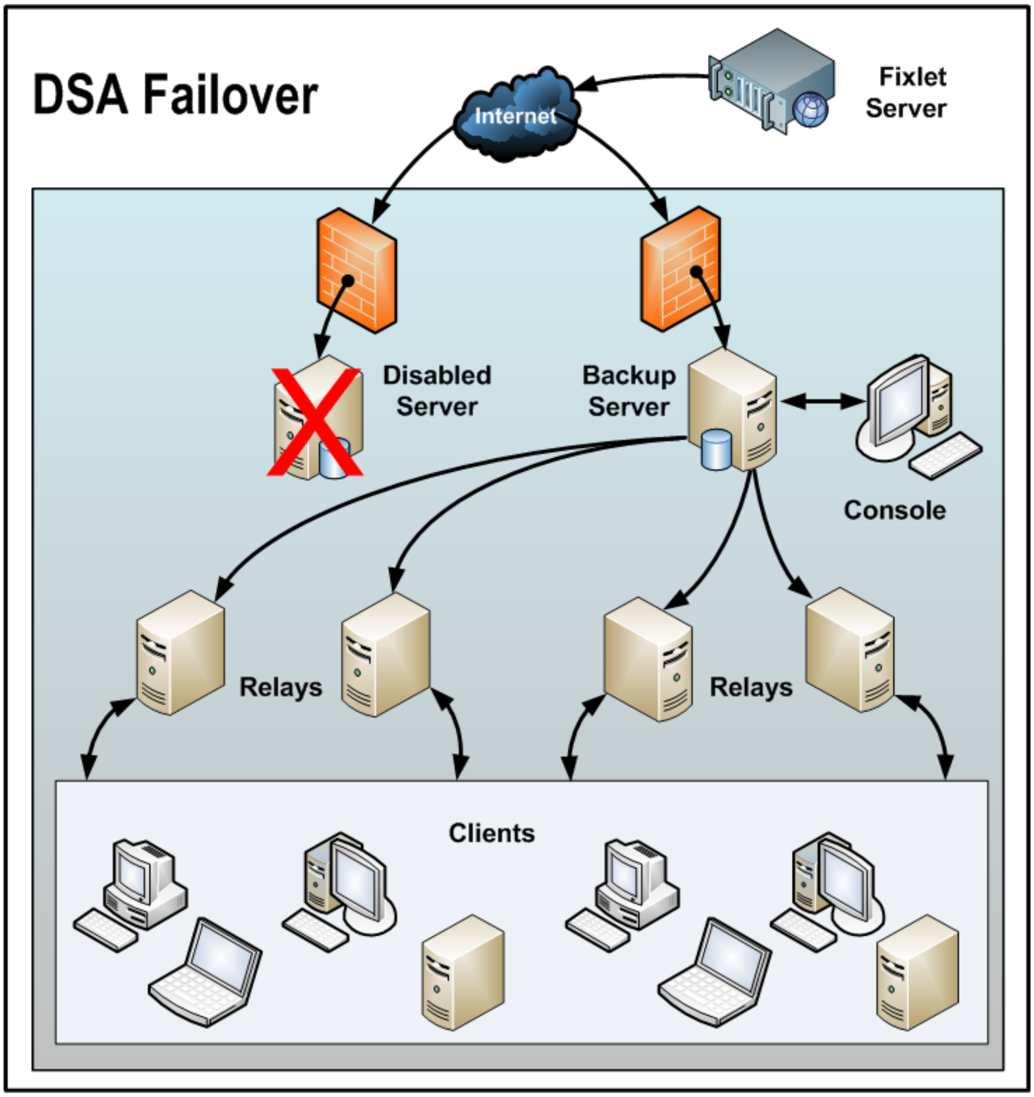
Distributed Server Architecture (DSA)

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



Automating Failover and Failback

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



Administrative Roles

To install and maintain Tivoli Endpoint Manager typically requires the cooperation of several administrators and operators:

- **The Network Administrator.** This person needs to allow the Server to connect to the Internet through the existing proxy server (if applicable) as well as resolve any network-specific issues that might prevent Tivoli Endpoint Manager from working correctly. The network administrator also provides information about WAN link connection speeds and subnet addresses if necessary. When starting a deployment of Tivoli Endpoint Manager, it is best to make the Network Administrator aware of how the Tivoli Endpoint Manager uses the network by reviewing the page on network traffic at the Tivoli Endpoint Manager support site.
- **The Database Administrator.** This person is responsible for setting up and maintaining the SQL Server 2005+ database for the Server.
- **The Site Administrator.** This person installs and maintains the software, including the Tivoli Endpoint Manager Server, Console, and Client programs. The Site Administrator is also responsible for creating, distributing, and revoking publisher keys and management rights that allow Console operators to deploy actions. The Site Administrator is the only person in an organization who can authorize new Console Operators or Master Operators (see next bullet). A Site Administrator holds this position by virtue of having administrative access to the Server computer as well as access and the password to the site-level signing keys.
- **Console Master Operators.** These people are operators with access to all the Tivoli Endpoint Manager computers with the added authority to assign management rights to other 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 Tivoli Endpoint Manager Site Administrator can create new operators and a Master Operator can only create custom content with permission from the Site Administrator.
- **Console Operators.** These people manage the day-to-day operation of the Tivoli Endpoint Manager, including Fixlet management and action deployment, typically on a subset of computers subject to the management rights assigned by a Site Administrator or Master Operator.

Often these administrative roles overlap and one person might be assigned multiple tasks. The network and database tasks are limited to minimal setup procedures, which are described in this document. The Tivoli Endpoint Manager Console Operators (including Master Operators) should read the separate ***TIVOLI ENDPOINT MANAGER Console Operator’s Guide***.

Tasks of the Tivoli Endpoint Manager Site Administrator

The Site Administrator has the following primary responsibilities:

- **Obtaining and securing the Action Site Credentials.** To install Tivoli Endpoint Manager, the Administrator must generate a private key, receive a license certificate from IBM, and create a masthead with the digital signature and configuration information.
- **Certifying Users.** The Site Administrator must create an account and private key files for each operator. Avoid using the same login information for site-level and user-level accounts. This practice increases confusion about context and can lead to errors.
- **Preparing the Server**. The Tivoli Endpoint Manager Server must be correctly set up to communicate externally with the Internet and internally with the Clients. The Tivoli Endpoint Manager Server also needs to be configured to host the Tivoli Endpoint Manager database (or another computer can be used as the SQL Server database).
- **Installing the various Components**. The Site Administrator installs the Tivoli Endpoint Manager Client, Server, Relay, and Console modules.
- **Assigning Management Rights.** Master Operators can assign management rights to the Console operators. These rights constrain operators to specific computers. You can also grant or revoke the right to make custom content or to view unmanaged assets.
- **Maintaining the Server**. The Tivoli Endpoint Manager Server runs a SQL Server database and several specific services. Standard maintenance tasks like upgrades or fixes are managed using Fixlet technology or can be performed manually by the Tivoli Endpoint Manager Site Administrator.
- **Maintaining security**. The Tivoli Endpoint Manager system is protected by password-encrypted private keys. The Site Administrator controls access to these and can create new private publisher keys or revoke them as the need arises. Authentication uses public key infrastructure (PKI) technology with key lengths of up to 4096 bits.

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

Part Two

Getting Started

Now that you understand the terms and the administrative roles, you are ready to actually get authorized and install the programs. This guide describes each step in detail, but the process is typically straightforward and fast.

Getting Authorized

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

If you have not yet purchased a license, contact sales@bigfix.com or visit the Tivoli Endpoint Manager website at http://www.bigfix.com.

The sales agent will want to know how many Clients you intend to install. Based on this, the agent will create, sign, and email you a **License Authorization** file, which will have a name like “CompanyName.BESLicenseAuthorization”.

The Installer program collect sfurther information about your deployment and then creates a file called the **action site masthead**. This file establishes a chain of authority from the Tivoli Endpoint Manager root all the way down to the Console operators in your organization. The masthead combines configuration information (IP addresses, ports, and so on) and license information (how many 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 use the **Tivoli Endpoint Manager Installer**, which you can download from IBM.

Note: If you are using an evaluation version of the Tivoli Endpoint Manager, you can skip the following section. During installation, the Tivoli Endpoint Manager Evaluation Generator create syour signing keys through an expedited process, and the generation of separate publisher keys is not necessary.

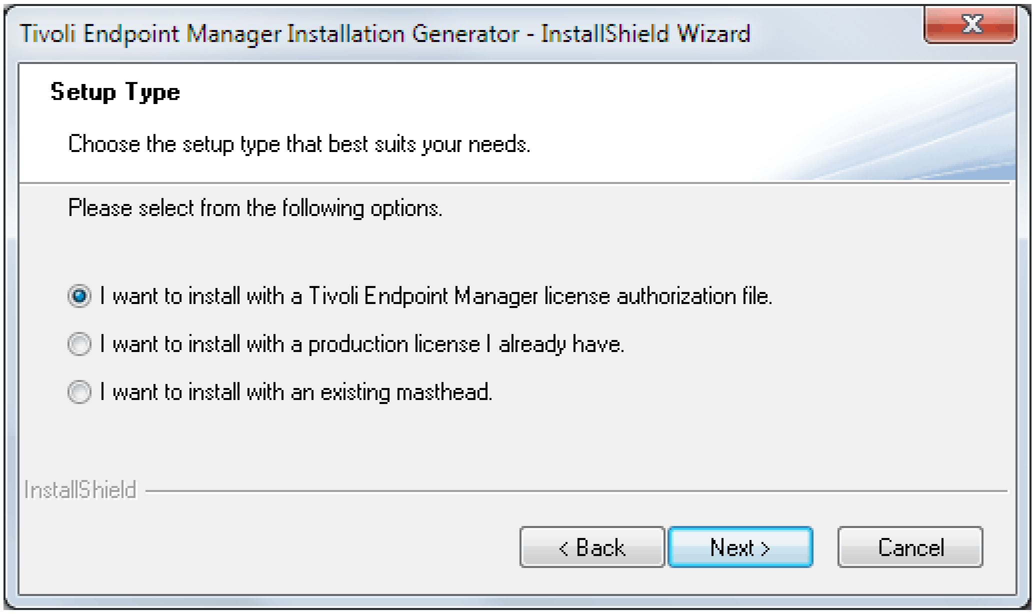
Creating the Action Site Masthead

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

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

1. Run the Tivoli Endpoint Manager Installer that you downloaded from the Tivoli Endpoint Manager site (www.BigFix.com). At the welcome screen, click **Next**.
2. In the dialog offering to install the Evaluation or Production version of Tivoli Endpoint Manager, select **Production** and click **Next**.

3. After reading the License Agreement, click **Yes** to accept it and continue. The **Setup Type** dialog opens.



Tivoli Endpoint Manager Installation Generator - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select from the following options.

● I want to install with a Tivoli Endpoint Manager license authorization file.

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

○ I want to install with an existing masthead.

Select the choice to **install using the License Authorization file from IBM**, then click **Next**.

4. The Action Site Masthead Creation Wizard launches. It asks you for the location of your license authorization file. Click the **Browse** button to bring up a standard Windows open-file dialog. Navigate to your license authorization file, which has a name like CompanyName.BESLicenseAuthorization. Select the file and click **Open.**
5. A dialog opens displaying the current contents of your license authorization. Click **Next**.
6. The next panel in the Wizard prompts you for the **DNS name** or **IP address** of your Server. Type this in and click **Next**.
7. Note: The DNS/IP address that you choose becomes a permanent part of your deployment and must never change. For the sake of flexibility, it is strongly recommended that you use a DNS name instead of a static IP address.
8. The next panel in the Wizard prompts you for a site-level **password** to allow you to create a site admin key for your deployment. Type in your password twice (for verification), and specify a key size (from 2K to 4Kbits) for the public/private key pair. Click **Next**.
9. From the **Save As** dialog, find a folder to save your private key file (license.pvk) to a secure location, such as a PGPDisk on a USB drive. Click **Save**.
10. The next panel in the Wizard prompts you to submit your masthead request to IBM. This request consists of your original authorization, your server DSN name, and your public key, all packaged into a single file. Typically, you select the first choice, **submit request**, to post the request via the Internet. Click **Next**. The Wizard retrieves your certificate (license.crt) from the Tivoli Endpoint Manager License Server.

    (Alternatively, the Wizard allows you to save the request as a file named request.BESLicenseRequest. Then you can visit the Tivoli Endpoint Manager website, post your request, and download your certificate.)
11. Upon a successful request submission, the Wizard retrieves your license (license.crt) and prompts you to save it. Click **Save**. This action completes the Wizard, returning you to the

Setup Type dialog. You are now ready to install the programs with your new production license.

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

Warning!

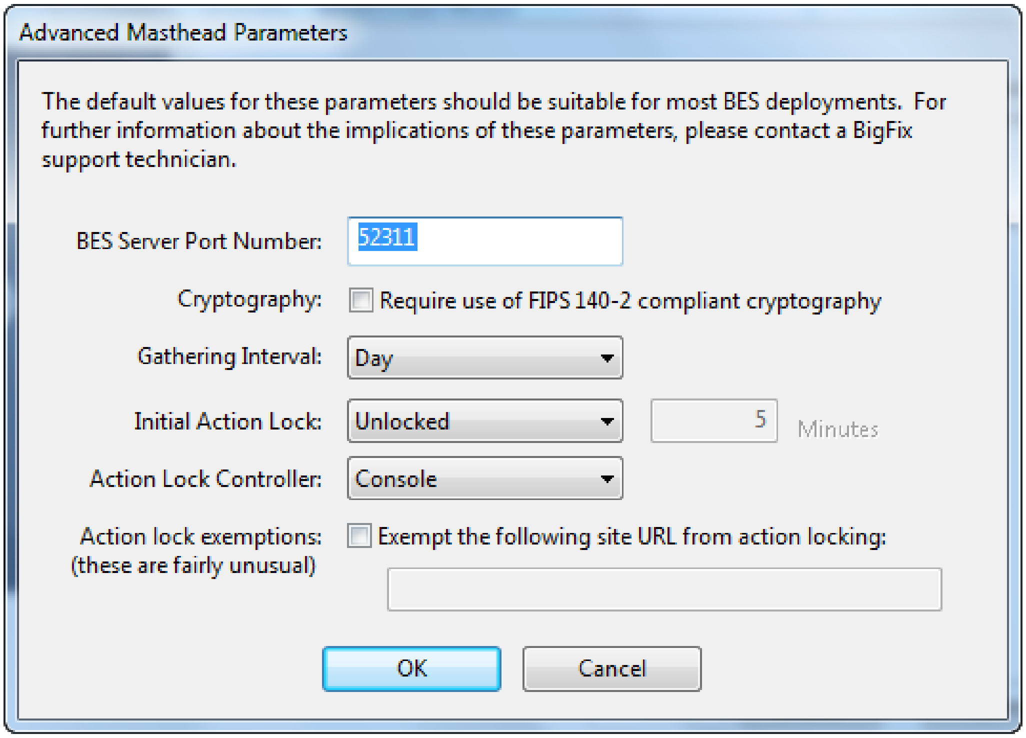
If you lose your site credential files or password, then no one – not even IBM – can recover your keys or your password. You will need to *reinstall the entire system*, including all the Clients, with a freshly-generated key.

If the main Server is lost, you might also lose your encryption key file. For disaster recovery, you have two options: you can back up your encryption key now, so you can restore it after re-creating the Server, or you can generate a new encryption key after re-creating the Server.

Installing the Programs

When you have your license or your action site masthead, you are ready to install the programs. Perform the following steps:

1. If the installer is not already running, launch it. From the **Setup Type** dialog, select the second choice to **Install with a production license**. Click **Next**.
2. Browse to the location of your license key and click **Open**.
3. A dialog opens, prompting you for your private **site signing key** (license.pvk). This is typically stored in the same folder as the license.crt file. Browse to it and click **Open**.
4. A dialog prompts you for the **Site Admin Private Key Password**. Enter the password you selected to protect your private key (see the previous section) and click **OK**.
5. The program prompts for a server port number that Tivoli Endpoint Manager will use for all its data transmissions. The default port is **52311**.



Advanced Masthead 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

Cryptography: □ Require use of FIPS 140-2 compliant cryptography

Gathering Interval: Day

Initial Action Lock: Unlocked 5 Minutes

Action Lock Controller: Console

Action lock exemptions: (these are fairly unusual) □ Exempt the following site URL from action locking:

This is the recommended port number, but you can choose a different port if that is more convenient for your particular network. Typically, you choose a port from the IANA range of private ports (49152 through 65535). You could use a reserved port number (ports 1-1024), but it is not considered best practice because it inhibits the ability to monitor or restrict traffic correctly and it prevents you from using port numbers for specific applications. The lock options in this dialog typically do not need to be changed unless you want a computer to automatically be locked after installation. There is also a checkbox if you want to apply FIPS 140-2 Cryptography. Click **OK** when you are finished.

Accept the default settings on this page unless you have a specific reason to change them. Incorrect settings can cause Tivoli Endpoint Manager to work in a sub-optimal way. Consult with a support technician for more details.

6. A standard Windows **Save As** dialog prompts you to save the **Masthead**. This is a public file that does not require protection. Navigate to a folder of your choice, name the file (for example, actionsite.afxm), and click **Save**.
7. You are now ready to generate the Tivoli Endpoint Manager installation components. Select the default directory (Tivoli Endpoint Manager Installers) or click **Browse** to choose a different folder. Click **Next**.
8. The Install Wizard then generates and saves various installation components. After saving the files, a dialog opens confirming the installation and reminding you of their location. Click **Finish** to exit and start the **Tivoli Endpoint Manager Installation Guide**.

Running the Component Installers

You have now created a private key, requested and received a certificate, used the certificate to create a masthead, and then generated the various installation components, including the **Tivoli Endpoint Manager Installation Guide**. When the components have been saved, the **Tivoli Endpoint Manager Installation Guide** automatically launches. You can also run it at any time by selecting it from the Start Menu.

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

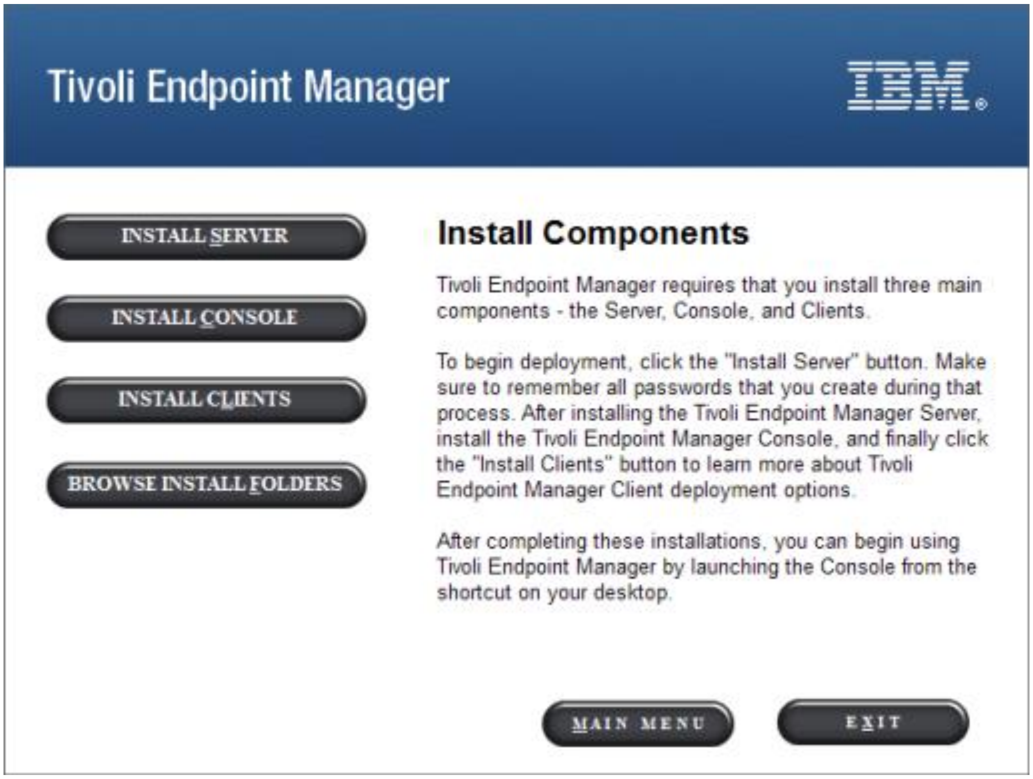
1. If it is not already running, launch the Installation Guide (**Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Installation Guide**).
2. Select the button labeled **Install Components**.
3. A dialog box opens, prompting you to select a component to install. Click the buttons on the left, in order from top to bottom, to install the Tivoli Endpoint Manager components. The component installers include:
   - Install the Tivoli Endpoint Manager Server
   - Install the Tivoli Endpoint Manager Console
   - Install the Tivoli Endpoint Manager Clients
   - Browse Install Folders
4. The Tivoli Endpoint Manager Server, Console, and Clients all have their own installers. Follow the instructions for each, as described in the following sections.

Installing the Primary Server

The Tivoli Endpoint Manager Server is the heart of the System. It runs on a server-class computer on your network, which must have direct Internet access as well as direct access to all the Client computers in your network. Make sure your server meets the requirements outlined in the **Server Requirements** section (page 4). Also, you can consult the knowledge-base article on server requirements at the Tivoli Endpoint Manager support site.

To install the Server, follow these steps:

1. If you have not already done so, run the Installation Guide (**Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Installation Guide**). Click the button labeled **Install Components**.
2. A new panel opens.



Install Components

Tivoli Endpoint Manager requires that you install three main components - the Server, Console, and Clients.

To begin deployment, click the "Install Server" button. Make sure to remember all passwords that you create during that process. After installing the Tivoli Endpoint Manager Server, install the Tivoli Endpoint Manager Console, and finally click the "Install Clients" button to learn more about Tivoli Endpoint Manager Client deployment options.

After completing these installations, you can begin using Tivoli Endpoint Manager by launching the Console from the shortcut on your desktop.

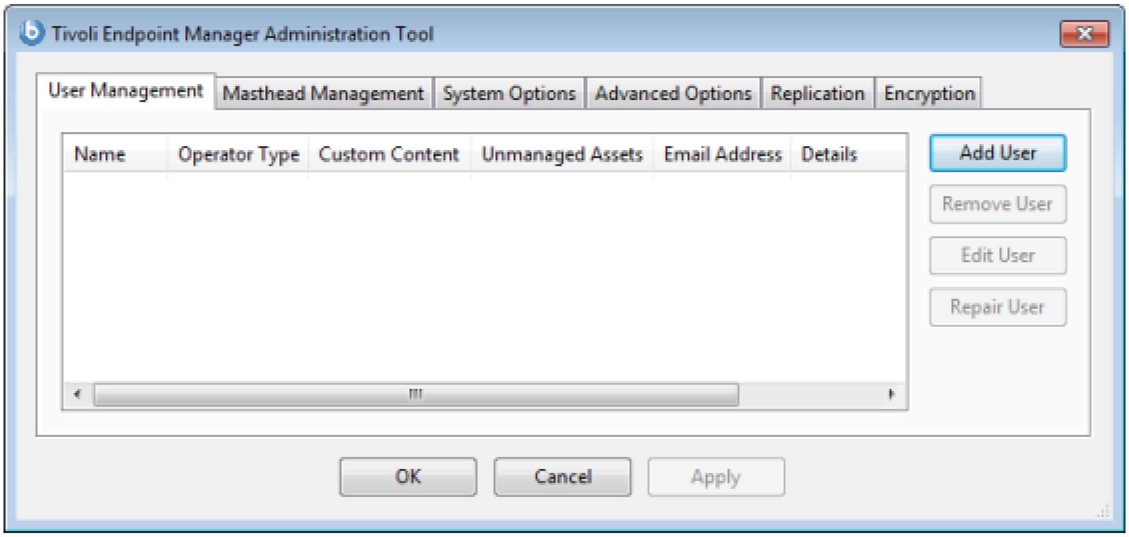
Click the top button labeled **Install Server.** The Tivoli Endpoint Manager Server Install Wizard presents a welcome panel. Click **Next** to continue.

3. After reading the **License Agreement**, click **Yes** to accept it and continue.
4. A dialog prompts you to choose a **Master** or **Replicated** database. Click the first button to create a Master database for later replication or if you only need a **Single** database in your deployment. Click the second button to create a Replica of an existing Master. If this is your initial installation, click the top button.
5. A dialog prompts you to select a **Local** or **Remote** database. If you want to use another computer to host the Tivoli Endpoint Manager Database, it must have a SQL Server already installed. The most common choice is to use the local database.

6. A dialog displays a list of the Server components about to be installed. In general, you should accept the default components and click **Next**.
7. The installer prompts you for the desired destination of the 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. When you have decided on the destination, click **Next**.
8. The Server Properties dialog prompts you to enter a location for the Server web root folder (if different from the default). This is where downloaded files for the Clients will be stored. The default URL is also available for editing, if you want to change it.

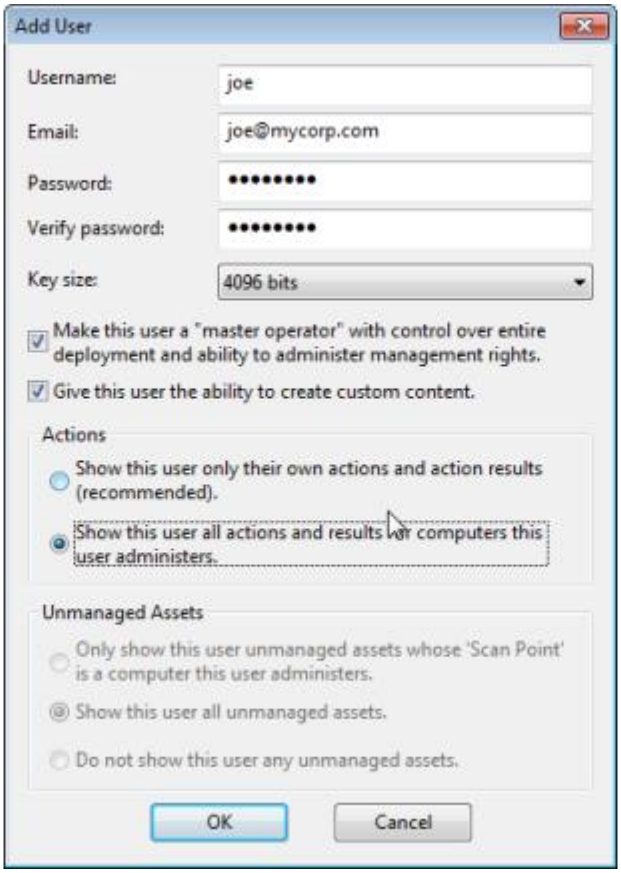
Note: No other application can be listening on the Tivoli Endpoint Manager port or errors will occur.

9. A dialog prompts you for a location and port number for Web Reports. By default, it uses port 80. If IIS is installed, it chooses port 52312 instead.
10. The Tivoli Endpoint Manager Server installer then presents a window displaying the selected inventory of server components to be installed as well as some other installation programs to run. Click **Next** to continue the installation.
11. When the files have been correctly installed, the program prompts you for specific information, depending on your installation parameters. The program asks you to set a default 'sa' password if the 'sa' password for the SQL Server database is currently blank (this is done for security reasons).
12. The program then prompts you to locate the **Action Site Masthead**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where you stored your masthead, select it, and click **Open**.
13. The program might prompt you for the location of your **license certificate**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where you stored your license (license.crt), select it, and click **Open**.
14. The program might prompt you for the location of your private key (license.pvk). Accept the default path (if specified) or click the **Browse** button to find a different location. Finally, enter your password to initialize the database.
15. The program then prompts you to create an administrative user. Click **OK** to open the **Tivoli Endpoint Manager User Management** dialog.



Click **Add User** to enter each user.

For each user, enter the name, email, password, and various permissions.



Add User

Username: joe

Email: joe@mycorp.com

Password: •••••••••

Verify password: ••••••••

Key size: 4096 bits

☑ Make this user a "master operator" with control over entire deployment and ability to administer management rights.

☑ Give this user the ability to create custom content.

Actions

○ Show this user only their own actions and action results (recommended).

● Show this user all actions and results for computers this user administers.

Unmanaged Assets

○ Only show this user unmanaged assets whose 'Scan Point' is a computer this user administers.

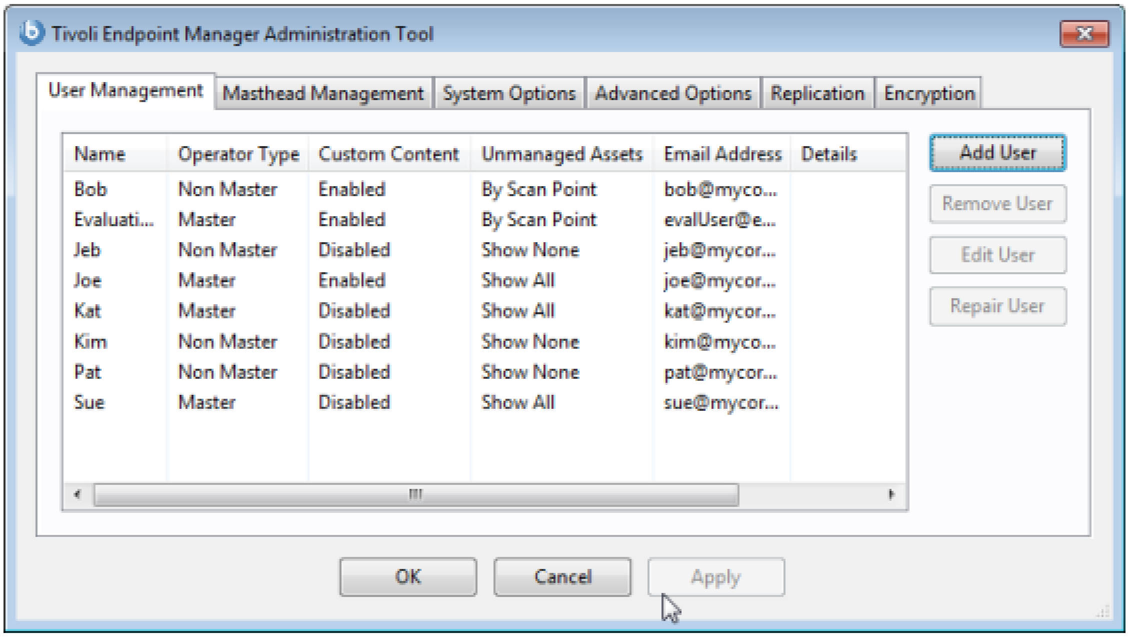
● Show this user all unmanaged assets.

○ Do not show this user any unmanaged assets.

You do not need to add all your users now; you will be able to add more users by running the **Tivoli Endpoint Manager Administration Tool** later. Enter the name of the Tivoli Endpoint Manager operator (no spaces allowed), the email address, and a password for this user. Indicate whether you want to allow this user to **administer management rights** or to **create custom content**.

You must grant administrative rights to at least one user, typically yourself. You can limit user rights to view **unmanaged assets**. You can also limit users to their specific domain (using Scan Point), allow unfettered access, or disallow all access. Click **OK** when done.

16. When you have finished entering users, click **Done**.



Name	Operator Type	Custom Content	Unmanaged Assets	Email Address	Details
Bob	Non Master	Enabled	By Scan Point	bob@myco...	
Evaluati...	Master	Enabled	By Scan Point	evalUser@e...	
Jeb	Non Master	Disabled	Show None	jeb@mycor...	
Joe	Master	Enabled	Show All	joe@mycor...	
Kat	Master	Disabled	Show All	kat@mycor...	
Kim	Non Master	Disabled	Show None	kim@myco...	
Pat	Non Master	Disabled	Show None	pat@mycor...	
Sue	Master	Disabled	Show All	sue@mycor...	

The program prompts you for your site admin password to propagate the Tivoli Endpoint Manager Operator information.

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

Authenticating Additional Servers (DSA)

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

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

Using NT Authentication with Domain Users and User Groups

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

1. Create a service account user or user group in your domain. For a user group, add authorized domain users to your Servers. You might need to have domain administration privileges to do this.
2. On the Master Server, use SQL Server Management Studio to create a login for the domain service account user or user group, with a default database of **BFEnterprise**, and give this login System Admin (sa) authority or the DBO (DataBase Owner) role on the BFEnterprise and master databases.
3. On the Master Server, change the **LogOn** settings for the FillDB service to the domain user or member of the user group created above, and restart the service.

Using NT Authentication with Domain Computer Groups

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

1. Create a Global Security Group in your domain containing each desired Server. You might need to have domain administration privileges to do this.
2. After creating the group, each server must be rebooted to update its domain credentials.
3. On the Master Server, use SQL Server Management Studio to create a login for the domain group, with a default database of BFEnterprise, and give this login System Admin (sa) authority or the DBO (DataBase Owner) role on the BFEnterprise and master databases.

Using SQL Authentication

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

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

2. On the Master Server, use SQL Server Management Studio to create a SQL Server login with this name. Chose SQL Server Authentication as the authentication option and specify the password. Change the default database to BFEnterprise and grant it System Admin (sa) authority or the db_owner role for the BFEnterprise and master databases.
3. On the Master Server, add the following String values under the key:

   HKLM\Software\BigFix\Enterprise Server\FillDB:
   ReplicationUser = <login name>
   ReplicationPassword = <password>
4. Restart the FillDB service.

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

Installing Additional Servers (DSA)

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

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

1. Install the same SQL Server version being used by the Master Server.
2. Run the **Server installer** on each machine that you want to configure as an additional Server. Use the same domain administration that you used for the local SQL Server install (so you have sa authority).
3. If you are extracting the server installer from the Installation Generator, select **Production Deployment**, and **I want to install with an existing masthead**. Specify the masthead.afxm file from the Master Server. Otherwise, use the Server install package from the BESInstallers folder on the Master Server.
4. On the **Select Database Replication** page of the server installer, select **Replicated Database**.
5. On the **Select Database** page, select **Local Database** to host the database on the server (typical for most applications).
6. Proceed through the installer screens as usual until the installer gets to **Configuring your new installation** and prompts you with a **Database Connection** dialog box. Enter the hostname of your master server, and the credentials for an account that can log in to the master server with DBO permissions on the BFEnterprise database.
7. The Replication Servers window shows you the Server configuration for your current deployment. By default, your newly-installed Server should be configured to replicate directly from the master server every 5 minutes. You can adjust this as necessary.
8. For large installations, the initial database replication can take several minutes and might get interrupted. If you experience this problem, you can discuss it with your IBM Software Support.
9. Use SQL Server Management Studio to create the same SQL Server login you created earlier on the Master Server with BFEnterprise as the default database and System Admin (sa) authority or the DBO role on the BFEnterprise and master databases.
10. For NT Authentication via Domain User and User Group, change the LogOn settings for the FillDB service to the domain user or member of the user group created above, and restart the service.

11. For SQL Authentication, add the following string values to the FillDB registry keys, and restart the FillDB Service.
12. HKLM\Software\BigFix\Enterprise Server\FillDB:
    ReplicationUser = <login name>
    ReplicationPassword = <password>
13. On the newly-installed server, run the **Tivoli Endpoint Manager Administration Tool** and select the **Replication** tab to see the current list of servers and their replication periods. Select the newly-installed server from the pull-down menu, and verify in the list below that it is successfully connected to the master server. Then select the master server in the server dropdown, and verify that it is correctly connected to the new server. You might need to wait for the next replication period before both servers show a successful connection.

    Note: The initial replication can take several hours depending on the size of your database. Wait for the replication to complete before taking any actions from a Console connected to the replica Server.
14. You can see a graph of the servers and their connections by clicking the **Edit Replication Graph** button. You can change the connections between servers by simply dragging the connecting arrows around.

Connecting the Console to a different Server

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

1. From **Control Panel > Administrative Tools > Data Sources (ODBC)**, select the **System DSN** tab, and click Add.
2. Select the **SQL Server** driver, and click **Finish**.
3. Specify the following information on the subsequent dialog:

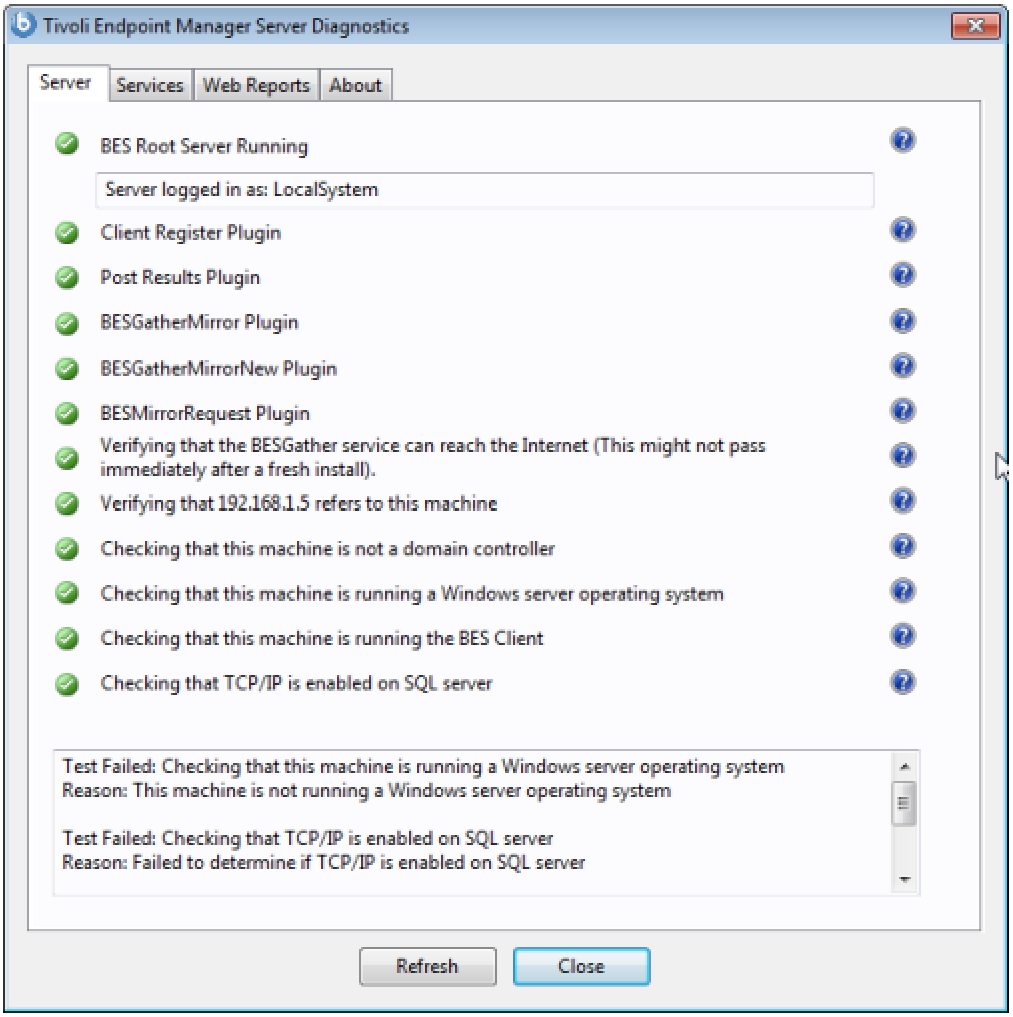
   Enter bes_<servername> for the Name, and <servername> for the Server, where <servername> is the hostname of the new replica Server. Click **Next**.
4. On the following dialog, specify **NT Authentication** or **SQL Authentication** as appropriate for your deployment. If unsure, use SQL Authentication. Clear the box to **Connect to SQL Server** to obtain default settings. Click **Next**.
5. Check the top box and change the default database to **BFEnterprise**. Click **Next**, and on the following panel, click **Finish**.

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

Running the Tivoli Endpoint Manager Diagnostics Tool

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

1. If you have just installed the Server, the Diagnostics Tool should already be running. Otherwise, log on to the Server as an administrator and launch the program (**Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Diagnostics Tool**). The program analyzes the server components and creates a report.
2. For more in-depth information, click the **Full Interface** button. The Tivoli Endpoint Manager Diagnostic control panel is displayed. This window has tabs corresponding to the categories of server diagnostics, including **Services** and **Web Reports.**



BES Root Server Running

Server logged in as: LocalSystem

Client Register Plugin

Post Results Plugin

BESGatherMirror Plugin

BESGatherMirrorNew Plugin

BESMirrorRequest Plugin

Verifying that the BESGather service can reach the Internet (This might not pass immediately after a fresh install).

Verifying that 192.168.1.5 refers to this machine

Checking that this machine is not a domain controller

Checking that this machine is running a Windows server operating system

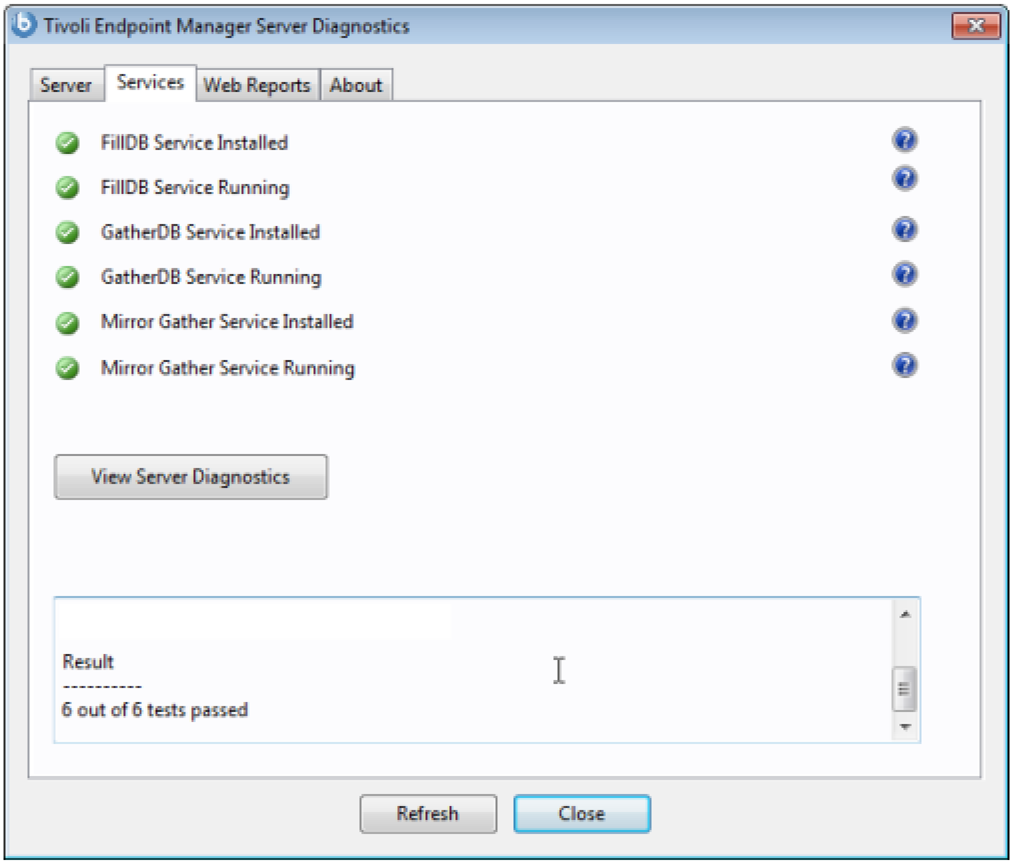
Checking that this machine is running the BES Client

Checking that TCP/IP is enabled on SQL server

```
Test Failed: Checking that this machine is running a Windows server operating system
Reason: This machine is not running a Windows server operating system

Test Failed: Checking that TCP/IP is enabled on SQL server
Reason: Failed to determine if TCP/IP is enabled on SQL server
```

Note that if you have not yet installed the Client, a warning light is shown. It becomes green as soon as you install the Client.

3. The **Services** tab shows you if the database and gathering services are correctly installed and running.



✓ FillDB Service Installed
✓ FillDB Service Running
✓ GatherDB Service Installed
✓ GatherDB Service Running
✓ Mirror Gather Service Installed
✓ Mirror Gather Service Running

```
Result
----------
6 out of 6 tests passed
```

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 Server is functioning correctly. Similarly, there is a tab to diagnose the **Web Reports** Server.

4. To find out more information, click the question mark button to the right of any item. These buttons link to knowledge-base articles at the Tivoli Endpoint Manager Support Site.
5. If all the buttons are glowing green, click **Close** to exit the Diagnostic**.**

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

Understanding the Server Components

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

- **Client Registration Component.** When the Client is installed on a new computer, it registers itself with the client registration component of the Server and the Client is given a unique ID. If the computer's IP address changes, the Client automatically registers the new IP address with the client registration component.
- **Post Results Server Component.** When a 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 together with the registered ID of the Client computer. This information is passed on to the Tivoli Endpoint Manager database through the FillDB service and then becomes viewable in the Console. Also, other state changes are periodically reported by the clients to the server directly or through Relays.
- **Gather Server Component.** This component watches for changes in Fixlet content for all the Fixlet sites to which you are subscribed. It downloads these changes to the Server and makes them available to the GatherDB Component.
- **FillDB Component.** This component posts Client results into the database.
- **GatherDB Component.** This component gathers and stores Fixlet downloads from the Internet into the database.
- **Download Mirror Server Component.** The Download Mirror Server Component hosts Fixlet site data for the Relays and Clients. This component functions as a simplified download server for Tivoli Endpoint Manager traffic.

Installing the Console

The Tivoli Endpoint Manager 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 Server. Except in testing or evaluation environments, it is not a good idea to run the Console on the Server computer itself due to the performance and security implications of having the publisher key credentials on a computer that is running a database or web server.

To install the Console, follow these steps:

1. Run the Installation Guide (**Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Installation Guide**). Click the button labeled Install Tivoli Endpoint Manager Components.

2. From the next panel, click **Install Console**.

3. After a welcome panel, you are shown the Console license agreement. Read the agreement and click **Yes** to accept the terms and continue the installation.

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

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

6. After the files are installed, click **Finish** to complete the installation. You can now choose to launch the Console, or continue to the next section to install the Clients.

See the ***Tivoli Endpoint Manager Console Users Guide*** for more details about using the Console program.

Installing the Clients

Install the Tivoli Endpoint Manager Client on every computer in your network that you want to administer – including those computers running the Server and the Console. This allows those computers to receive important Fixlet messages (like security patches, configuration files, or upgrades).

If you are running the Installer, select **Install Tivoli Endpoint Manager Components > Install Clients > Install Locally** to install the Client on your local machine in the directory you specify.

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

Using the Client Deploy Tool

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

- You must have an Active Directory or NT Directory domain (there is also an option to deploy to a list of computers if you have an administrator account on the computer).
- The Tivoli Endpoint Manager Client Deploy Tool can only target computers running Windows 2000, XP, Server 2003, Vista, Server 2008, 7, or Server 2008 R2.
- The computer running the Client Deploy Tool must be connected to the domain, but must not be the domain controller itself.
- The Service Control Manager (SCM) and the Remote Procedural Call (RPC) services must be running on the target machines.
- There must be no security policy on the computer that would prevent either a remote connection to the SCM or the issuance of a Remote Procedural Call.
- The dnsName property of every target computer in the Active Directory must be correctly defined.

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

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

If the 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 user interaction. Use the tool by performing the following steps:

1. The Tivoli Endpoint Manager Client Deploy Tool is created by the Installation Generator. You can launch the tool from the Installation Guide (click the **Install Tivoli Endpoint Manager Components > Install Tivoli Endpoint Manager Clients > Install Remotely**

button) or launch it directly from **Start > Programs >Tivoli Endpoint Manager > Tivoli Endpoint Manager Client Deploy**.

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

   - **Find computers using Active Directory**. The Tivoli Endpoint Manager Client Deploy tool contacts the Active Directory server to get a list of all of the computers in the domain. It checks each of the computers to see if the Client is already installed and displays this information in a list.
   - **Find computers using NT 4.0 Domains**. All the computers in the domain are listed with a status flag indicating whether or not the Client has been installed.
   - **Find computers specified in a list**. Based on how your network resolves computer addresses, you must provide a list of computer names, IP address ranges, or hostnames. The list must have one name / IP address range / hostname per line. Using this option, the Client Deploy Tool does not attempt to discover any computers, but instead attempts to install directly to all the listed computers.

3. Type in a **username** and **password** that has administrative access to the computers. In most cases, this is a domain administrator account. If you are using the computer list option, you can specify a local account on the remote computers (such as the local administrator account) that have administrative privileges. The rest of the client deployment process uses this username/password, so if the account does not have the appropriate access on the remote computers, you receive access denied errors.

4. When the list of computers is displayed, shift- and control-click to select the computers you want to administer with Tivoli Endpoint Manager. Click **Next.**

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

   - **File Transfer:** You can choose to **push** the files out to the remote server for installation or to have the files **pulled** from the local computer. Unless there are security policies in place to prevent it, for most cases pushing the files to the remote computer works best.
   - **Connection Method:** There are two ways to connect to the remote computers. Using the **Service Control Manager** (SCM) is recommended, but you might also use the **task scheduler** if the SCM does not work.
   - **Installation Path:** Specify a path for the Client, or accept the default (recommended).
   - **Verification:** Check this box to verify that the Client service is running after waiting for the installation to finish, to know if the installation completed successfully.
   - **Custom Setting:** Add a Custom Setting to each Client deployed, in the form of a Name / Value pair.

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

7. When completed, a log of successes and failures is displayed. Simply retrying can resolve some failures; use advanced options if that does not work. For more information, see the article on Client deployment at the Tivoli Endpoint Manager support site.

Installing the Client Manually

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

1. There are at least two ways to install the client:

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

   - Alternatively, run the Installation Guide (available at **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Installation Guide**) and click the button marked **Browse Install Folders**. It opens the **Tivoli Endpoint Manager Installers** folder and displays the **Client** folder.

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

3. After the welcome panel, you are prompted for a location to install the software. You can accept the default, or click **Browse** to select a different location.

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

5. Repeat this process on every computer in your network that you want to place under Tivoli Endpoint Manager administration.

Installing the Client with MSI

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

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

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

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

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

Using Software Distribution Tools

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

Using Group Policies

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

Using Login Scripts

In an NT or AD domain, login scripts can be written that check for the presence of the Client. When the computer logs in and finds the Client missing, it can automatically access the Client installer from a specified location on a global file share. The Support Site 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 Client.

If your network will be adding new computers from time-to-time, this approach can be very convenient, ensuring that the Server discovers and manage snew 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 Windows Installer based setup. For more information about command line options for setup.exe, see InstallShield's support website at http://kb.flexerasoftware.com/doc/Helpnet/isxhelp12/IHelpSetup_EXECmdLine.htm. Here are some examples of command line switches for the Client installer that can be used in a login script:

- To install the Client silently while writing a log to the C:\, execute a DOS command of the form:

  ```
  setup.exe /s /v/l*voicewarmup \"C:\besclientinstall.log\"
  SETUPEXE=1 /qn”
  ```

- To change the default installation location, the appropriate form of the command is:

  ```
  setup.exe /s /v/l*voicewarmup \"C:\besclientinstall.log\"
  INSTALLDIR=\”<InstallPath\” SETUPEXE=1 /qn”
  ```

  Where <InstallPath> is the full windows path to the folder where the Client is to be installed.

Note: The Windows user running setup.exe must have Administrative privileges on the computer and must be able to write a log file to the same folder that contains the “setup.exe” file, otherwise the installation failsand a log file is not created.

Embedding in a Common Build

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

For Windows

1. Install the Client on the computer to be imaged.
2. The Tivoli Endpoint Manager Client immediately attempts to connect to the Server. If it successfully connects to the Server, it is 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 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 Tivoli Endpoint Manager Client is now ready to be imaged.

Note: If the Client is started again for any reason (*including a system restart*), it re-registers with the server and **you will need to perform steps 3 to 4 again.** The Server has built-in conflict detection and resolution so if for any reason you fail to delete the ID, the Server notice s that there are multiple Clients with the same ComputerID and forces the Client to re-register and everything will work normally. However, it is advisable to perform the steps above to avoid having a grayed-out Client (the first imaged computer) in the computer list in the Console.

For Macintosh and Linux

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

Note: If the Client is started again for any reason (*including a system restart*), it re-registers with the server and **you will need to perform steps 2 to 4 again.** On a Windows system, the data in the folder simply overwrites the old installation. On UNIX systems, however, the BESData folder acts as a registry and must be deleted before imaging.

Using email

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

Enabling encryption on Clients

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

Note: You must have encryption enabled for your deployment before enabling it for your Clients. In particular, for the required option, your clients will go silent if you enable them without first setting up your deployment.
To enable encryption, follow these steps:

1. From the **BigFix Management** Domain, open the **Computer Management** folder and click the **Computers** node.
2. Select the computer or set of computers that you want to employ encryption.
3. From the right-click context menu, select **Edit Computer Settings**.
4. From the **Edit Settings** dialog, click **Add**.
5. In the **Add Custom Setting** dialog, enter the setting name as

   _BESClient_Report_Encryption (note the underline starting the name).

   There are three possible values for this setting:

   - **required:** causes the Client to always encrypt. If there is no encryption certificate available in the masthead or if the target computer (Relay or Server) cannot accept encryption, the Client will not send reports.
   - **optional:** the Client encrypts if it can, otherwise it sends its reports in clear-text.
   - **none:** No encryption is done, even if an encryption certificate is present. This allows you to turn off encryption after you enable it.

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

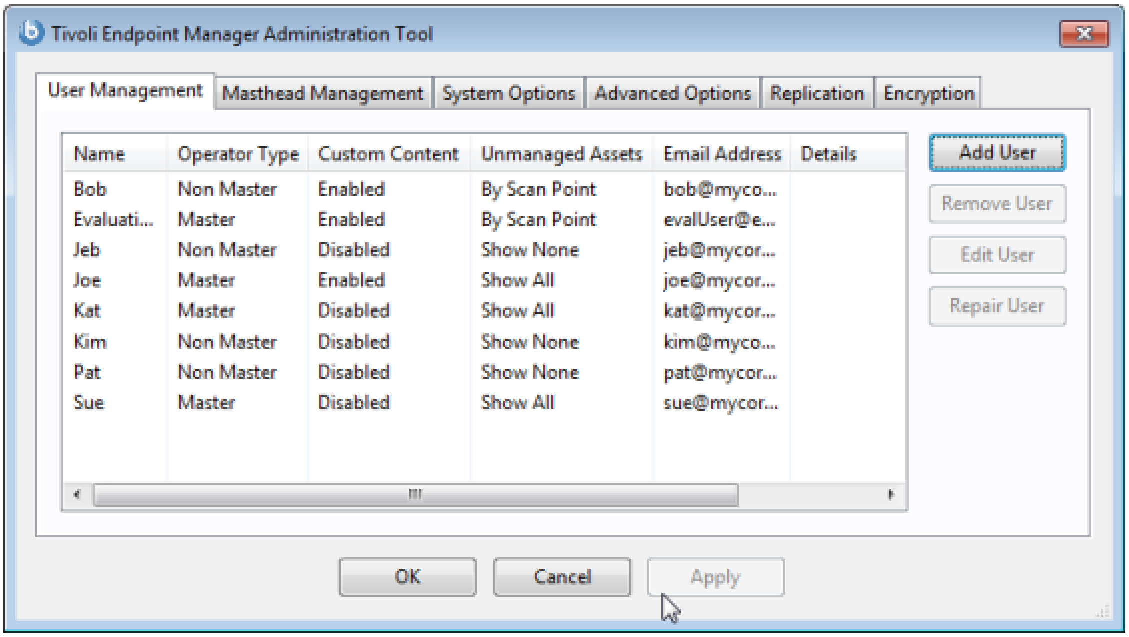
Running the Tivoli Endpoint Manager Administration Tool

The Installer automatically creates the Tivoli Endpoint Manager Administration Tool when it installs the other components of the Console program. This program operates independently of the Console and is intended for Administrative Operators only. You can find it from the Start menu: **Start > All Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool.** To run the program, you must first browse to the signing key (license.pvk).

Note that you can also change your administrative password through this interface. After you have selected the signing license, click OK to continue. You must supply your private key password to proceed.

User Management

If this is the first time you run the program, the Administration Tool provides you with a blank slate of users. Click **Add User** to include new Operators. This is where you return when you want to add, remove, or edit the management rights of your users.

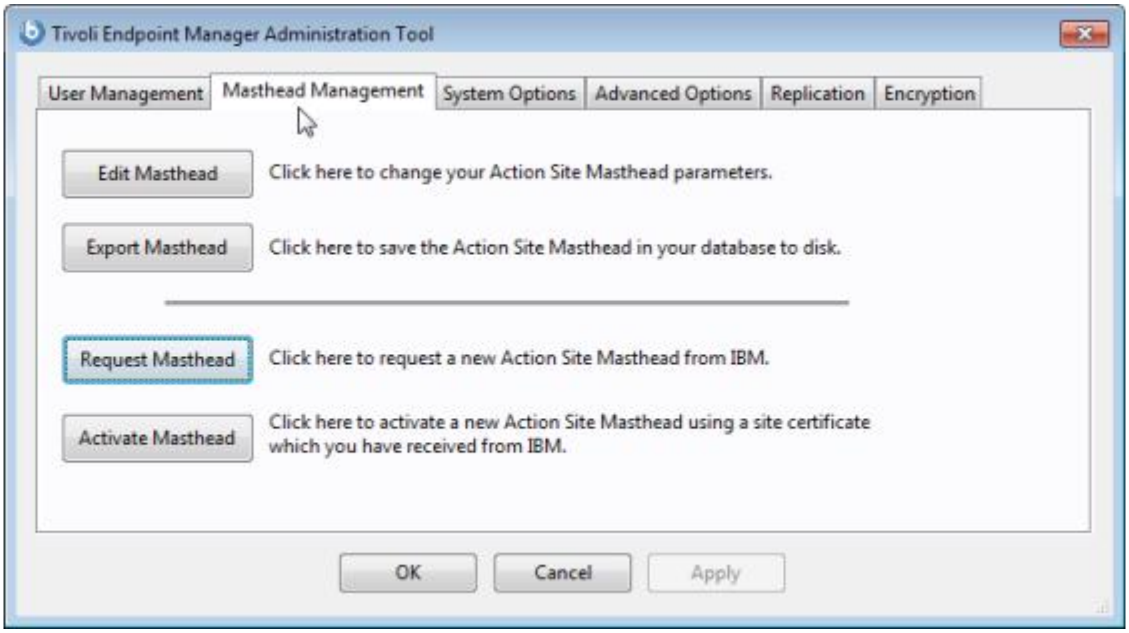


Name	Operator Type	Custom Content	Unmanaged Assets	Email Address	Details
Bob	Non Master	Enabled	By Scan Point	bob@myco...	
Evaluati...	Master	Enabled	By Scan Point	evalUser@e...	
Jeb	Non Master	Disabled	Show None	jeb@mycor...	
Joe	Master	Enabled	Show All	joe@mycor...	
Kat	Master	Disabled	Show All	kat@mycor...	
Kim	Non Master	Disabled	Show None	kim@myco...	
Pat	Non Master	Disabled	Show None	pat@mycor...	
Sue	Master	Disabled	Show All	sue@mycor...	

You can find out more about how to assign management rights in the section titled **Adding New Operators and Master Operators** (page 72).

Masthead Management

Click the second tab to view the **Masthead Management** dialog.



Click here to change your Action Site Masthead parameters.

Click here to save the Action Site Masthead in your database to disk.

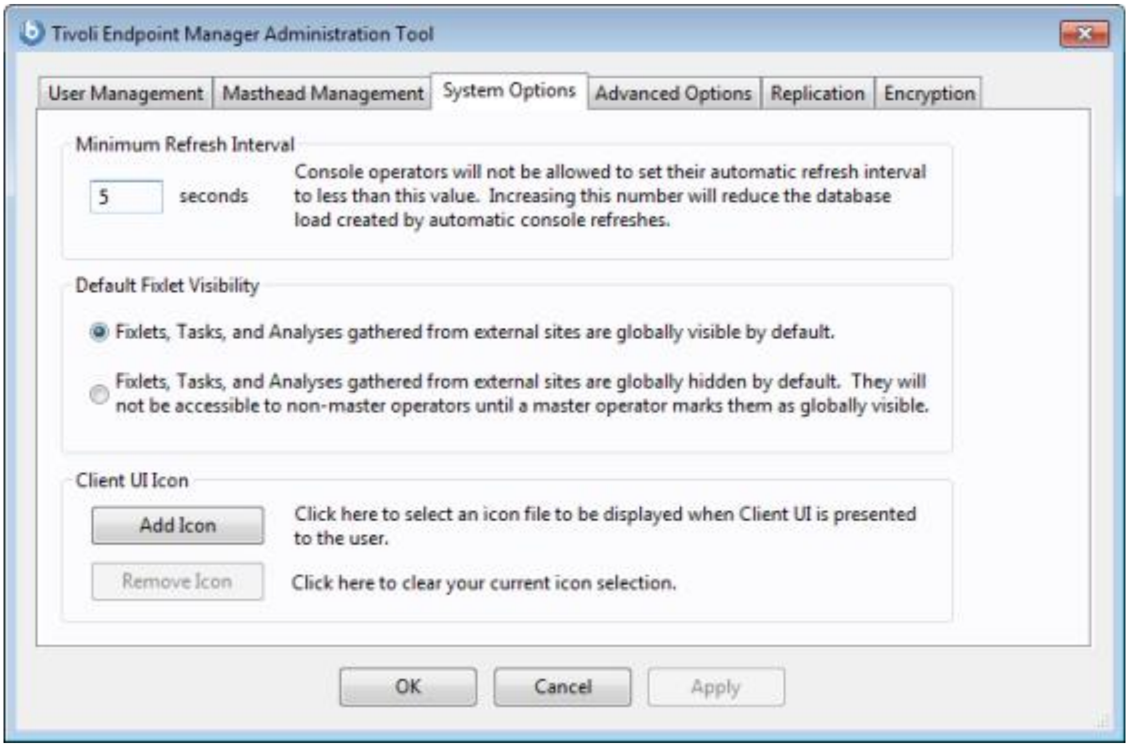
Click here to request a new Action Site Masthead from IBM.

Click here to activate a new Action Site Masthead using a site certificate which you have received from IBM.

If you do not yet have a masthead, which is required to run the Console, this dialog provides an interface to **Request** and subsequently **Activate** a new masthead. If you have an existing masthead, you can edit it to change gathering intervals and locking. For more information about managing your masthead, see the section named **Editing the Masthead** (page 80). You can also export your masthead, which can be useful if you want to extend your Tivoli Endpoint Manager network to other servers.

System Options

The third tab opens the **System Options** dialog. The first option sets a baseline minimum for refresh intervals. This refers to the Fixlet list refresh period specified in the Preferences dialog of the Console. The default period is 15 seconds, but if your network can handle the bandwidth, you can lower this number to make the Console more responsive. Conversely, if your network is strained, you might want to increase this minimum.



Minimum Refresh Interval

5 seconds

Console operators will not be allowed to set their automatic refresh interval to less than this value. Increasing this number will reduce the database load created by automatic console refreshes.

Default Fixlet Visibility

● Fixlets, Tasks, and Analyses gathered from external sites are globally visible by default.

○ Fixlets, Tasks, and Analyses gathered from external sites are globally hidden by default. They will not be accessible to non-master operators until a master operator marks them as globally visible.

Client UI Icon

Add Icon — Click here to select an icon file to be displayed when Client UI is presented to the user.

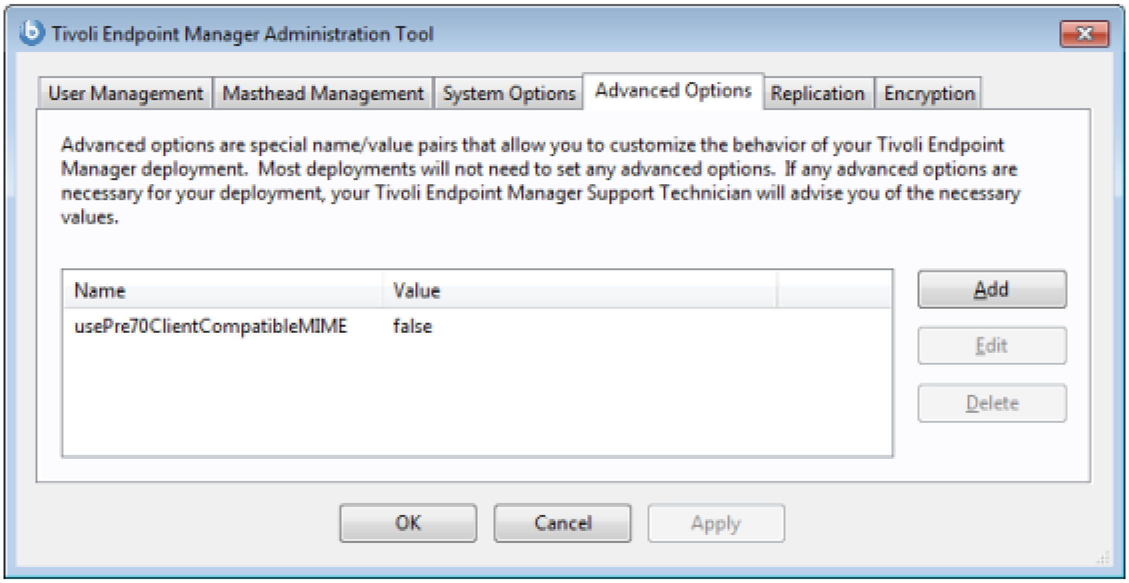
Remove Icon — Click here to clear your current icon selection.

This dialog also lets you set the default visibility of external sites. These are, by default, globally visible to all Console operators. To give you extra control, you can set the visibility to hidden, and then adjust them individually through the Console. You must be an administrator or a master operator to make these hidden sites become visible.

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

Advanced Options

The fourth tab opens the **Advanced Options** dialog. This dialog lists any global settings that apply to your particular installation.



Advanced options are special name/value pairs that allow you to customize the behavior of your Tivoli Endpoint Manager deployment. Most deployments will not need to set any advanced options. If any advanced options are necessary for your deployment, your Tivoli Endpoint Manager Support Technician will advise you of the necessary values.

Name	Value
usePre70ClientCompatibleMIME	false

These options are name/value pairs, and are typically supplied by your IBM Software Support. As an example, if you are subscribed to the Power Management site, one of these options allows you to enable the WakeOnLAN function.

Replication

The fifth tab opens the **Replication** dialog. This dialog helps you to visualize your replication servers. For more information, see the section titled **Managing Replication** (page 63).

Encryption

The final tab opens the **Encryption** dialog. This dialog allows you to generate a new encryption key or to disable encryption altogether. For more information, see the section titled **Managing Client Encryption** (page 75).

Understanding Operator Rights

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

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

Site Administrators

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

- **Creating/Modifying/Deleting** users with the Tivoli Endpoint Manager Administration Tool.
- **Setting global system options** including the Minimum Refresh Interval, Default Fixlet Visibility, and the Client UI Icon with the Tivoli Endpoint Manager Administration Tool.
- **Editing Mastheads.**
- **Administering Distributed Server Architecture** (DSA) configurations. This includes setting the replication rate and the linkage between Replication Servers.

Master Operators

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

- **Edit the management rights** settings for other operators. This allows you to divide up the computers in your network among various operators to have them each see a smaller subset of client computers.
- **Create new computer settings**, which monitor and control Client behavior and hold various labeled values for filtering. For more information, see the article on configuring settings at the support site.
- **Create or edit global retrieved properties**, which are used to filter and sort computers and can be used to create reports.
- View all unmanaged assets.
- Change the Client heartbeat, to optimize performance.
- Subscribe or unsubscribe from Fixlet sites.
- Create new custom Fixlet sites.
- **Designate operators** to be custom site owners, writers, and readers.
- **Globally hide or unhide** Fixlet messages.
- **Audit all Actions** taken in the Console.

- Manage External Fixlet Site subscriptions.

Operators

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

- **Deploy Actions.**
- **Create custom content**, including Fixlet messages, Tasks, Baselines, and Analyses. The Site Administrator can grant or revoke this right from the Tivoli Endpoint Manager Administration Tool.
- **Change or delete computer settings**, which monitor and control Client behavior and hold various labeled values that can be used for sorting and filtering.
- **View unmanaged assets** according to each Operator's scope (as defined by Scan Points). The Site Administrator can grant or revoke this right from the Tivoli Endpoint Manager Administration Tool.
- **Be custom site owners**, writers, and readers if granted the privilege by Master Operators.

Operators and Analyses

Operators have various rights and restrictions when activating and deactivating analyses:

- Ordinary operators cannot deactivate an analysis activated by other operators on computers they administer.
- Master Operators cannot directly activate custom analyses authored by ordinary operators. They can, however, make a copy of an analysis and activate the copy.

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

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

Administered: The operator must own or have permissions

Requires Custom Authoring: Granted by the Site Administrator through the Administration Tool

Administered by Admin Tool: Granted by the Site Administrator through the Administrator Tool

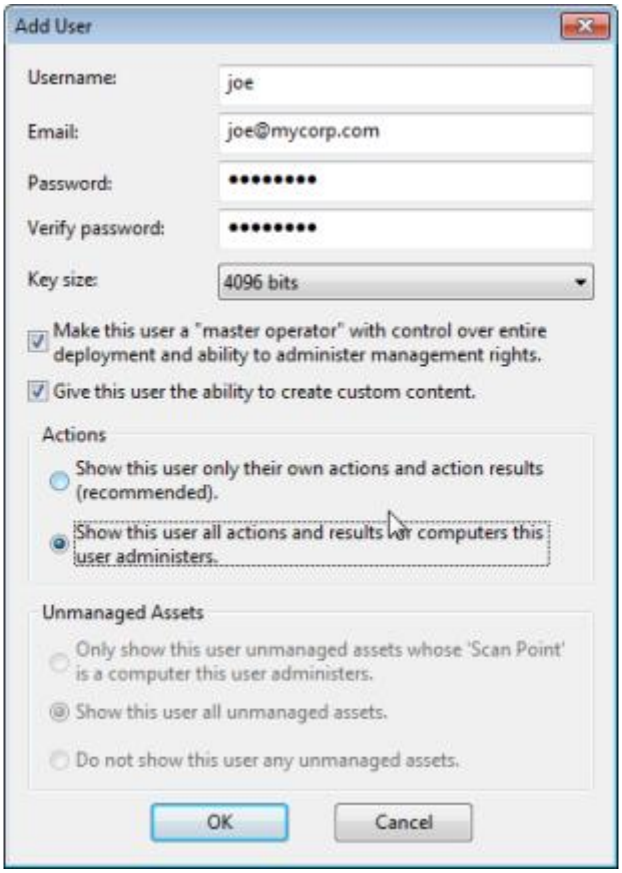
Adding Console Operators

As the Site Administrator, you must create accounts for each new Console operator, allowing them to view the database using the 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 Tivoli Endpoint Manager Administration Tool.

1. When you install the Server, the Tivoli Endpoint Manager Administrator Tool is automatically run so you can add new operators. However, you can add operators at any time by launching **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager 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 Console operators with publishing credentials. For each operator/publisher you add, you fill out data in the **Add Publisher** dialog:



Add User

Username: joe

Email: joe@mycorp.com

Password: •••••••••

Verify password: •••••••••

Key size: 4096 bits

☑ Make this user a "master operator" with control over entire deployment and ability to administer management rights.

☑ Give this user the ability to create custom content.

Actions

○ Show this user only their own actions and action results (recommended).

● Show this user all actions and results for computers this user administers.

Unmanaged Assets

○ Only show this user unmanaged assets whose 'Scan Point' is a computer this user administers.

● Show this user all unmanaged assets.

○ Do not show this user any unmanaged assets.

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. When you give the keys to your operators, they can change their passwords if they want.

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 have **administer management rights**, making them a Master Operator. As the Tivoli Endpoint Manager Administrator, check this box when you add yourself to the user list.

8. Check the second box if you want this operator to be able to **create custom content** such as custom Fixlet messages, Tasks, and Baselines. The availability of this feature depends on the license granted to you by IBM. By default, operators only see actions and action results for actions that they have issued. This is recommended for better Console performance. However, you can also choose to have the operator see all actions and action results that were taken against computers that the operator administers.

WARNING!

Custom actions grant the user the ability to create and deploy custom actions to any computer the operator manages with just a few mouse clicks. Use good judgment when granting these rights to operators.

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

10. A dialog opens prompting you to choose a location in which to create a new folder to contain the operator’s credentials. Choose both the parent folder and the name for the new folder, which defaults to the operator’s name. Consider using a removable disk for additional security. Give this folder, together with the password, to the designated Console operator.

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

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

    - **publisher.pv**k: the private key created for each authorized operator/publisher. As with the key to the front door, the operator must understand the responsibility of caring for this file.
    - **publisher.crt:** the signed certificate authorizing each operator/publisher to issue actions. This file is also stored in the database.

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

14. The Tivoli Endpoint Manager 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 Clients. At any time, you can add new authorized operators by running the Tivoli Endpoint Manager Administration Tool again.

Notes on Operators:

- Propagate the action site whenever you change any operator information, especially when you revoke operators.
- If two operators were created prior to Version 7.0 with the same email address, their signing certificates might conflict with each other and they will not be able to use the custom site functions until one of them is deleted and reissued. Such users are highlighted in red in the Tivoli Endpoint Manager Administration Tool .Click **repair** to see a pop-up a message box explaining the problem.
- A user’s status as Operator or Master Operator is permanently associated with the username and cannot be changed.
- For security. Site Administrators shouldo create users with a default password and store a backup copy of the console key files with those default passwords. Console operators who forget their password can be provided with the saved copy.

Subscribing to Fixlet Sites

Sites are collections of Fixlet messages that are created internally by you, by IBM, or by other vendors. You subscribe to a Site and agree on a schedule for downloading the latest batch of Fixlet messages.

You can add a new Site subscription by acquiring a Masthead file from a vendor or from IBM. Sites are generally devoted to a single topic, such as security or the maintenance of a particular piece of software or hardware. However, several sites can share characteristics and are then grouped into Domains, which are designed to be in accordance with the typical job tasks of your various Console managers. For example, the person responsible for patching and maintaining a common operating environment can find Support sites and Patching sites for various operating systems all bundled in the Patch Management Domain.

You can also set up your own custom site and populate it with Fixlets that you have developed specifically for your own network. You and other operators can then send and receive the latest in-house patches and quickly deploy them to the appropriate locations and departments.

Upon installation, the program is automatically set up to subscribe to certain management and maintenance sites. Depending on the terms of your license, you might have subscriptions to other sites as well. This means that content from those Sites automatically flows into your enterprise and is evaluated for relevance on all computers running the Tivoli Endpoint Manager Client. These sites, in turn automatically register with an appropriate Domain, providing a simple way to divide the content into functional sections.

To subscribe to a site, follow these steps:

1. Find an appropriate Site. Finding a Site is equivalent to finding a Site masthead file, which has an extension of .efxm. There are several ways to do this:
    - **Fixlet Sites:** IBM might post a links list to new Sites as they become available.
    - **Fixlet Subscriptions:** Sometimes a Fixlet message might offer a subscription. Click the Fixlet action to initiate the subscription.
    - **Download Mastheads:** You can also subscribe to a Site by downloading a masthead file from a vendor's website. After the masthead is saved to your computer, you can activate it in one of the ways described below.
2. Double-click the masthead, or select **Add External Site Masthead** from the **Tools** menu and browse to the folder containing the masthead.

3. You are prompted for your private key password. Type it in and click **OK**.
4. The masthead is propagated to all Clients, which immediately begin to evaluate the Fixlet messages from the new site.

For more information abot sites, as well as how to create custom sites, see the ***Tivoli Endpoint Manager Console Guide***.

Using Analyses

An Analysis is a collection of property expressions that allows an Operator to view and summarize various properties of Tivoli Endpoint Manager Client computers across a network. The collection is grouped together to be labeled, edited, and activated against groups of computers and have the results displayed together. For example, suppose you have a custom application deployed in your network, and you want to craft an analysis to give you important information about the state of your machines relative to that custom application.

There are several pre-made Analyses that examine important aspects of your networked computers, including their hardware, applications, and Server/Relay/Client relationships.

Studying these default Analyses can be instructive when you want to make your own analysis or customize existing ones. Custom Analyses can help you monitor aspects of your network that are vital to your company's operation.

The Retrieved Properties that underlie each Analysis are created using Relevance expressions. For example, to make sure you have fully deployed the most recent Tivoli Endpoint Manager Client software, you might use an expression such as **version of client**. This simple expression is evaluated on every computer where the analysis is targeted, allowing you to see explicitly which version of the Tivoli Endpoint Manager Client is running on each computer, or to view a summary of how many machines are running each version.

Analyses are targeted with yet another Relevance statement, which might be as simple as TRUE, which would include all connected Clients. Generally, you want to narrow the scope with a Relevance statement such as name of operating system as lowercase starts with "win", which would limit the Analysis to Windows computers only.

To display an Analysis,

1. Click the **Analyses** icon in the Domain Panel navigation tree (left panel of the interface).
2. Click an entry in the resulting **Analysis List Panel**.

The body of the Analysis is shown in the Work Area below the list. The Analysis display region has several tabs:

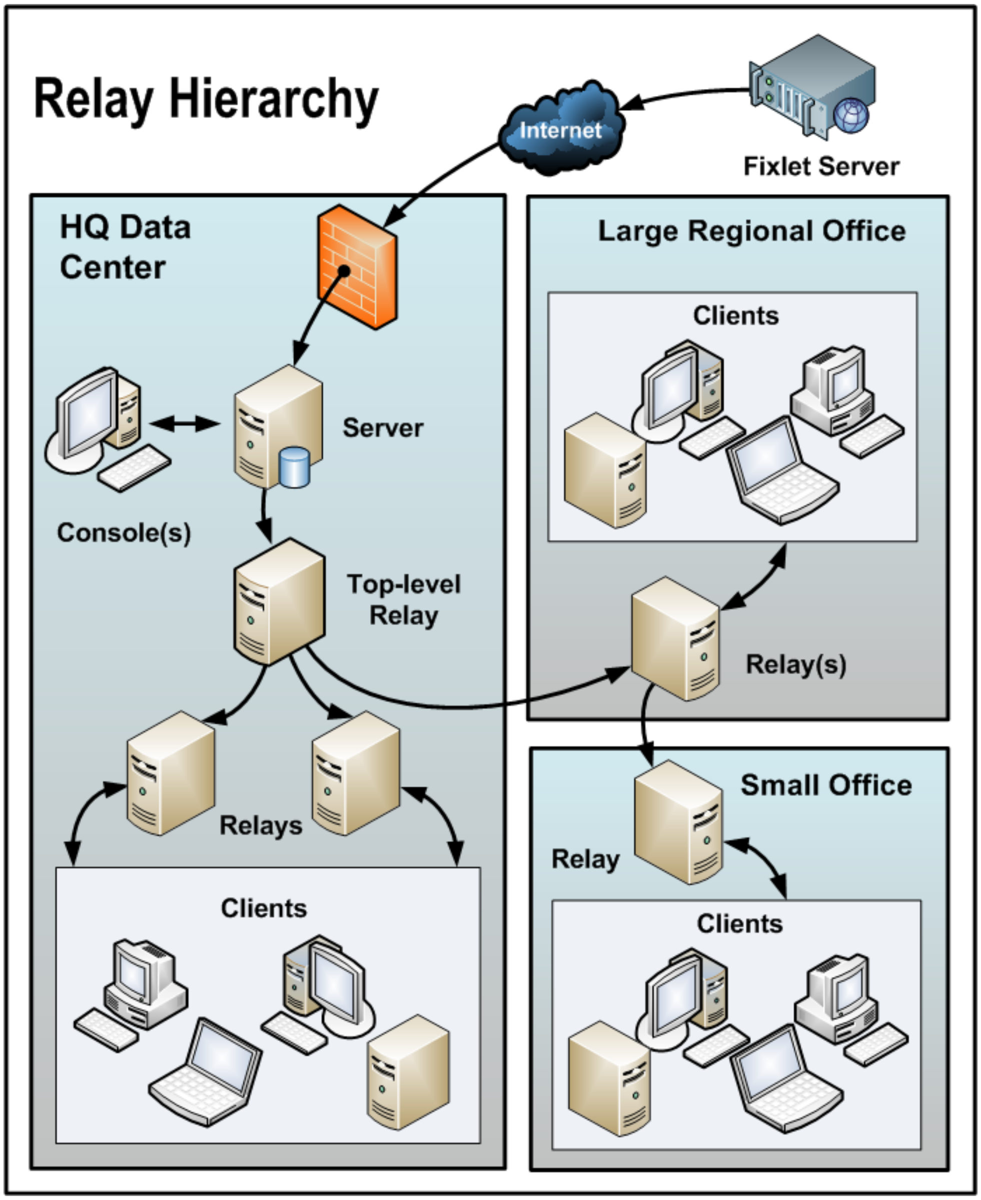
- **Description**: This is an HTML page providing a description of the analysis.
- **Details**: This panel provides a property-by-property listing of the chosen analysis, as well as the Relevance statement that is being used to target the chosen computers. At the bottom is a text box for entering a comment to be attached to this analysis.
- **Results**: This dialog lists the actual results of the analysis, which can be filtered and sorted by the pre-assigned properties (this tab is only available if the Analysis is activated).
- **Applicable Computers**: This is a list of all the computers where the selected analysis is applicable. You can filter the list by selecting items from the folders on the left, and sort the list by clicking the column headers.

Part Three

Configuring the Components

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

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



Using Relays

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

- **Relieving Downstream Traffic**. The Tivoli Endpoint Manager Server has many tasks, one of the most taxing of which is distributing files, such as patches or software packages, and Fixlet messages to the Clients. Relays can be set up to ease this burden, so that the Server does not need to distribute the same file to every Client. Instead, the file is sent once to the Relay, which in turn distributes it to the Clients. In this model, the Client connects directly to the Relay and does not need to connect to the Server.
- **Reducing Upstream Traffic**. In the upstream direction, Relays can compress and package data (including Fixlet relevance, action status, and retrieved properties) from the Clients for even greater efficiencies.
- **Reducing Congestion on Low-Bandwidth Connections**. If you have a Server communicating with computers in a remote office over a slow connection, designate one of those computers as a Relay. Then, instead of sending patches over the slow connection to every Client independently, the Server sends only a single copy to the Relay (if it needs it). That Relay, in turn, distributes the file to the other computers in the remote office over its own fast LAN. This effectively removes the slow connection bottleneck for remote groups in your network.
- **Reducing the Load on the Server**. The Tivoli Endpoint Manager Server has many tasks including handling connections from Clients and Relays. At any given instant, the Server is limited in how many connections it can effectively service. Relays, however, can buffer multiple Clients and upload the compressed results to the Server. Relays also distribute downloads to individual Clients, further reducing the workload of the Server and allowing the program to operate faster and more efficiently.

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

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

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

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

Generally, the Relay uses minimal resources and does not have a noticeable impact on the performance of the computer running it (see the next section on Relay requirements). The Tivoli

Endpoint Manager Clients can be set to automatically find their closest Relay. These features allow for significant savings in both hardware and administrative overhead.

Note: If the connection between a Relay and Server is unusually slow, it might be beneficial to connect the Relay directly to the Internet for downloads. More information about Relays can be found by visiting the Tivoli Endpoint Manager support site, or by talking to your IBM Software Support.

Relay requirements

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

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

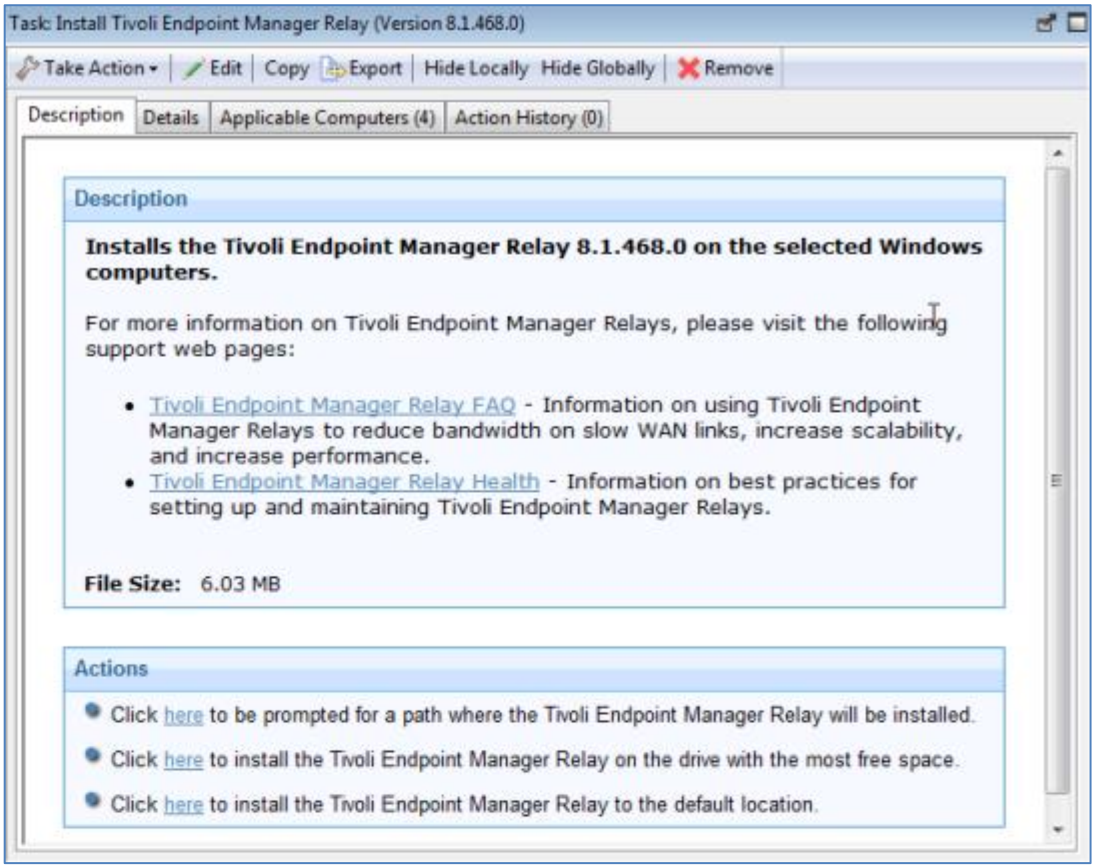
- The Tivoli Endpoint Manager Relay must have a two-way TCP connection to its parent (which can be a Server or another Relay).
- The Tivoli Endpoint Manager Relay can be installed on an ordinary workstation, but if many Clients simultaneously download files, it might slow the computer down. Also, for the Relay to work correctly, the computer must be powered on, which means workstations that are commonly powered off are poor choices for Relays.
- Workgroup file servers, print servers, SMS servers, AntiVirus servers, domain controllers, test servers, and other server-quality computers that are always turned on are good candidates for installing a Relay. Install relays on an existing shared server to reduce the total hardware cost of deploying Tivoli Endpoint Manager. Most companies already have partially-utilized servers in the appropriate places throughout their networks. If you need to purchase a new computer for the task, the Relay requirements are low. An inexpensive workstation-class computer or bottom-of-the-line server should suffice.
- Relays must be installed on Windows 2000, Windows XP, Windows Server 2003, Windows Vista®, Windows Server 2008, Windows 7, Windows Server 2008 R2, Red Hat Enterprise Linux 4/5/6, or Solaris 10 computers.
- Because older versions of Internet Explorer used outdated network libraries, the computers running the Relays must have at least Internet Explorer 4.0 or later to work correctly.
- More information about Relays can be found at the Tivoli Endpoint Manager support site.
- The Tivoli Endpoint Manager Relay cache size is configurable, but is set to 1GB by default. It is recommended that you have at least 2 GB available for the Relay cache to prevent hard drive bottlenecks.

Designating a Relay

To set up a Relay, you need to designate a Windows 2000, XP, Server 2003, Vista, Server 2008, 7, Server 2008 R2, Red Hat Enterprise Linux 4/5/6, or Solaris 10 computer that is running a Client to act as the Relay. The Tivoli Endpoint Manager Clients on your network detect the new Relays and automatically connect to them. To create a Relay, use the Console, and follow these steps:

1. In the Console, open the **Fixlets and Tasks** icon in the Domain Panel and then click **Tasks Only** to see a list of all Tasks.

2. Find the Task with the title **Install Tivoli Endpoint Manager Relay** (it might include a version number after it). This Task is relevant when there is at least one Client that meets the requirements for the Relay.



Task: Install Tivoli Endpoint Manager Relay (Version 8.1.468.0)

Description

Installs the Tivoli Endpoint Manager Relay 8.1.468.0 on the selected Windows computers.

For more information on Tivoli Endpoint Manager Relays, please visit the following support web pages:

- Tivoli Endpoint Manager Relay FAQ - Information on using Tivoli Endpoint Manager Relays to reduce bandwidth on slow WAN links, increase scalability, and increase performance.
- Tivoli Endpoint Manager Relay Health - Information on best practices for setting up and maintaining Tivoli Endpoint Manager Relays.

File Size: 6.03 MB

Actions

- Click here to be prompted for a path where the Tivoli Endpoint Manager Relay will be installed.
- Click here to install the Tivoli Endpoint Manager Relay on the drive with the most free space.
- Click here to install the Tivoli Endpoint Manager Relay to the default location.

3. Choose your deployment option by choosing one of the actions in the Task. You can target single or multiple computers with this action.

Automatically Discovering Relays

When you have set up your Relays, you are almost finished. If they are configured to perform automatic relay selection, the Clients automatically find the closest relay and point to that computer instead of the server. This is the recommended technique, because it dynamically balances your system with minimal administrative overhead. To make sure your Clients are set up to automatically discover relays:

1. Start up the Console and select the **BigFix Management** Domain. From the Computer Management folder, click the **Computers** node to see a list of Clients in the list panel.
2. Shift- and ctrl-click to select the set of computers you want to automatically detect Relays. Press **Ctrl-A** to select the entire set of Clients.
3. Right-click 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 select all the Clients in your network, so you will see the multiple-select dialog.
4. Check the box marked **Relay Selection Method**.
5. Click the button marked **Automatically Locate Best Relay**.
6. Click **OK**.

Defaulting to Automatic Relay Discovery

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

1. As described in the previous section, open the **Edit Computer Settings** dialog.
2. Select the **Target** tab.
3. Click the button labeled **All computers with the property**.
4. In the window below, select **All Computers**.
5. Select the **Constraints** tab.
6. Uncheck the **Expires On** box.
7. Click **OK**.

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

Notes about Automatic Relay Discovery

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

- ICMP must be open between the Client and the Relay. If the Client cannot send ICMP messages to the Relays, it is unable to find the optimal Relay (in this case it uses the failover relay if specified or picks a random relay).
- Sometimes fewer network hops are not a good indication of higher bandwidth. In these cases, Relay Auto-selection might not work correctly. For example, a datacenter might have a Relay on the same high-speed LAN as the Clients, but a Relay in a remote office with a slow WAN link is fewer hops away. In a case like this, manually assign the Clients to the appropriate optimal Relays.
- Relays use the DNS name that the operating system reports. This name must be resolvable by all Clients otherwise they will not find the Relay. This DNS name can be overridden with an IP address or different name using a Task in the Support site.
- Clients can report the distance to their corresponding relays. This information is valuable and should be monitored for changes. Computers that abruptly go from one hop to five, for iexample, might indicate a problem with their relays.
- More information about Relays, automatic relay selection, and troubleshooting Relays can be found at the Tivoli Endpoint Manager support site.

Using Relay Affiliation

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

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

Creating Client Affiliation Groups

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

`_BESClient_Register_Affiliation_SeekList`

This Client setting should be set to a semi-colon (;) delimited list of relay affiliation groups, for example:

```
AsiaPacific;Americas;DMZ
```

Creating Relay and Server Affiliation Groups

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

```
_BESRelay_Register_Affiliation_AdvertisementList
```

This Client setting should also be set to a semi-colon (;) delimited list of relay affiliation groups, for example:

AsiaPacific;DMZ;*

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

Relay Affiliation List Information

There are no predefined relay affiliation group names; you can choose any group names that are logical to your deployment of Tivoli Endpoint Manager. There are some naming rules you must observe:

- Do not use special characters (including “.”) when choosing names
- Group names are not case-sensitive
- Leading and trailing whitespaces are ignored in comparisons

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

For more information about Relay Affiliation, see the article at the Tivoli Endpoint Manager support site.

Manually Selecting Relays

You might want to manually specify exactly which Clients must connect to which Relay. You can do this by performing the following steps:

1. Start up the Console and select the **BigFix Management** Domain. From the Computer Management folder, click the **Computers** node to see a list of Clients in the list panel.

2. Shift- and ctrl-click to select the set of computers you want to attach to a particular Relay.

3. Right-click 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 selected one or multiple computers.

4. Check the box labeled **Primary Relay** and then select a computer name from the drop-down list of available Relay servers.

5. Similarly, you can assign a **Secondary Relay**, which will be the backup whenever the Primary Relay Server is unavailable for any reason.

6. Click the **OK** button**.**

Viewing Relay Selections

To see which Clients are selecting which Relays:

1. Start up the Console and select the **BigFix Management** Domain.

2. From the **Computer Management** folder, click the **Computers** node to see a list of Clients.

3. Look under the **Relay** column in the List Panel (this column might be hidden; in which case you might need to right-click the column headings and make sure **Relay** is checked). The Tivoli Endpoint Manager Relay columns show information including the Relay method, service, and computer.

By default, the Clients attempt to find the closest Relay (based on the fewest number of network hops) every six hours. More information about Relays can be found at the Tivoli Endpoint Manager support site.

Monitoring Relay Health

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

Here are some suggestions for monitoring your Relay deployment:

- Click the **BigFix Management** domain and the **Analyses** node and activate the Relay Status analysis. This Analysis contains a number of properties that give you a detailed view of the Relay health.

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

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

Optimizing the Servers

Tivoli Endpoint Manager operates efficiently, with minimal impact on network resources. However, there might be installations that stretch the recommended configurations, where there are too many Clients for the allotted server power. The best solution is to choose a server with the required characteristics for your environment; you might 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 IBM Software Support has more information about which modifications might be best for your particular deployment.

Here are some possible optimization techniques:

- Deploy **Relays** to reduce the load on the server. This is the most effective way to increase the performance and responsiveness of Tivoli Endpoint Manager. Generally, the more Relays, the better the performance (as a rule of thumb, one Relay for 500 to 1000 Clients is a good choice, although it can be much higher for a dedicated computer).
- Slow down the **Client heartbeat** from **File > Preferences**. This decreases the frequency of messages that are regularly dispatched by the Clients to update their retrieved properties. Reducing this frequency reduces the amount of network traffic generated, but also decreases the timeliness of the retrieved properties. However, regardless of the heartbeat settings, the Clients always send their latest information whenever they receive a refresh ping from the Server or when they notice that a Fixlet is relevant.
- Slow down the **Fixlet List Refresh** rate from **File > Preferences**. This decreases the update frequency for the information displayed in the Console. If there are many Clients or Consoles simultaneously connected or the database is very large, reducing this frequency can substantially reduce the load on the Server. If multiple Console operators are going to be simultaneously using the Console, set the refresh rate to be something higher than the default (15 seconds) to reduce the load on the Tivoli Endpoint Manager database. Consider changing it to 60-120 seconds or more if there are many Console operators. The Tivoli Endpoint Manager Administration Tool on the Server allows you to set a global minimum refresh rate.
- Your database administrator might be able to help you with the following optimizations:
    - Change the SQL Server Recovery Model for the BFEnterprise database to **Simple** rather than **Full,** which is the default.
    - Reduce the percentage of memory allocated to SQL Server from 100% to 85%, to ensure that the web server and operating system are not short of memory.

- More performance recommendations can be found at the Tivoli Endpoint Manager support site.

Optimizing the Consoles

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

- **Make sure you have sufficient memory**. The Tivoli Endpoint Manager Console benefits greatly from capacious memory to speed up the viewing, filtering, and sorting of content (Fixlet messages, Tasks, Actions, and so on). If your computer does not have enough physical memory, the Console will run noticeably slower. You can check memory usage from the Task Manager (Ctrl-Shift-ESC). Select the Performance tab and refer to the Physical Memory section. If the available memory is less than 10% of the total memory, you are running low on RAM and can benefit by adding more.
- **Use high-speed network connections** between your Consoles and Servers, preferably with LAN connections of at least 100 MBPS. The Tivoli Endpoint Manager Database can be sizeable for a large network, so running the Console from a computer with a slow connection often results in very long load times.
- **Use remote control software**. With so much data to load and display, operating the Console in a remote office over a slow link can be tedious. In situations like this, you might be able to benefit from solutions such as Citrix, Terminal Services, or other remote control software. Set up the remote control server on a computer with fast access to the Server. Allow that machine to present instances of the Console and let the branch office run these Consoles remotely. The database stays in the main office, and the remote office has optimal performance. For more information, see the section on **Remote Citrix / Terminal Services Configuration** (page 99).
- **Delete old actions**. The Tivoli Endpoint Manager database stores information about old actions, which the Console loads in at startup and saves out at shutdown. If you do not need to track these old actions, you can delete them, allowing the Console to load and close faster. Note that deleted actions continue to exist in the database, but are not loaded into the Console or Web Reports and can be undeleted if necessary.
- More information about enhancing performance is available at the Tivoli Endpoint Manager support site.

Managing Replication (DSA)

Replication servers are simple to set up and require minimal maintenance. You might want to change the interval or allocate your Servers differently. Most of these changes are done through the Tivoli Endpoint Manager Administration Tool. Here you can see the current settings for your Servers and make the appropriate changes.

Change the Replication Interval

1. Start up the **Tivoli Endpoint Manager Administration Tool**.
2. Select the **Replication** tab.
3. Select the server you want from the drop-down menu. Using longer replication intervals means that the servers replicate data less often, but have more data to transfer each time. Note that replication intervals can be different for “replicating from” and “replicating to” a server.
4. Select the replication interval from the menu on the right.
5. Click **OK**.

Switching the Master Server

By default, server 0 (zero) is the master server. The Administrator Tool only allows you to perform certain administrative tasks (such as creating and deleting users) when you are connected to the master server. If you want to switch the master to another server, you must set the deployment option **masterDatabaseServerID** to the other server ID. Here is how:

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

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

Uninstalling a Replication Server

To uninstall a replication server, call the database-stored procedure **delete_replication_server**, which removes the specified ID from the replication set. Be careful not to delete the wrong server, or you might lock yourself out. The details of this procedure are beyond the scope of this guide, but basically you must log in to the database with SQL Server Management Studio. You can call the procedure with something like:

```
dbo.delete_replication_server( 1 )
```

This deletes the Server with ID=1.

The steps involved in completely deleting the server are beyond the scope of this guide, but the full procedure is available in a KB article at the Tivoli Endpoint Manager support site.

Managing Bandwidth

File downloads consume the bulk of the bandwidth in a typical 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 Server or on the Client or on both (in which case the lower of the two values is used). This can be important whenever you have bandwidth issues, as in the following situations:

- A remote office with a thin channel
- Remote dial-in users or users on a slow connection
- A shared channel with higher-priority applications
- A WAN or LAN that is already saturated or has stringent load requirements

Bandwidth throttling settings (and other Relay, Server, and Client settings) can be set using the Tasks from the Support site. Select the **BigFix Management** domain and select the **BES Component Management** node in the navigation tree to see the entire task list.

For more information About Relays, visit the Tivoli Endpoint Manager support site.

Dynamic Throttling

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

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

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

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

- **DynamicThrottleEnabled:** This setting defaults to zero (disabled). Any other value enables dynamic throttling for the given link.
- **DynamicThrottleMax:** This setting usually defaults to the maximum unsigned integer value, which indicates full throttle. Depending on the link, this value sets the maximum data rate in bits or kilobits per second.
- **DynamicThrottleMin:** This setting defaults to zero. Depending on the link, this value sets the minimum data rate in bits or kilobits per second. This value places a lower limit on the percentage rate given below.
- **DynamicThrottlePercentage:** This setting defaults to 100%, which has the same effect as normal (non-dynamic) throttling. It represents the fraction of the maximum bandwidth you want to use when the network is busy. It typically has a value between five and ten percent, to prevent it from dominating existing network traffic. (A zero for this setting is the same as 100%.)

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

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

```
_BESRelay_HTTPServer_DynamicThrottleEnabled
_BESRelay_HTTPServer_DynamicThrottleMaxKBPS
_BESRelay_HTTPServer_DynamicThrottleMinKBPS
_BESRelay_HTTPServer_DynamicThrottlePercentage
```

The Tivoli Endpoint Manager **Client settings:**

```
_BESClient_Download_DynamicThrottleEnabled
```

```
 _BESClient_Download_DynamicThrottleMaxBytesPerSecond
 _BESClient_Download_DynamicThrottleMinBytesPerSecond
 _BESClient_Download_DynamicThrottlePercentage
```

The Tivoli Endpoint Manager **Gathering settings:**

```
 _BESGather_Download_DynamicThrottleEnabled
 _BESGather_Download_DynamicThrottleMaxBytesPerSecond
 _BESGather_Download_DynamicThrottleMinBytesPerSecond
 _BESGather_Download_DynamicThrottlePercentage
```

Note: For any of these settings to take effect, you must restart the affected services (Server, Relay, or Client).
If you set a Server and its connected Client to differing maximums or minimums, the connection chooses the smaller value of the two.

Creating Client Dashboards

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

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

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

Place the Dashboard file (named _dashboard.html) and any accompanying graphics files into this folder. The next time the Client starts up, it incorporates these files into its interface, adding to the **Dashboard** tab. When you clicks this tab, the Dashboard calculates the latest values of each Relevance clause and displays them.

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

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

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

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

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

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

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

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

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

For example, to print out the operating sysem and the computer name, add these two lines:

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

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

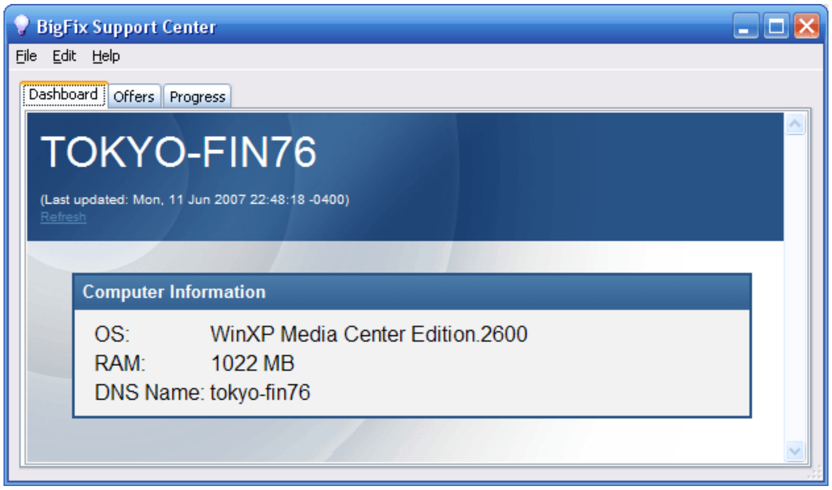
```
<html>
  <head>
    <link type="text/css" rel="stylesheet" href="offer.css"></link>
    <title>BigFix Dashboard Example</title>
  </head>
  <body>

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

    <div class="section">
      <div class="sectionHeader">Computer Information</div>
      <div class="subsection">
        <table>
          <tr> <td valign="top">OS: </td>
              <td><?relevance operating system ?></td></tr>
          <tr> <td valign="top">RAM: </td>
```

```
              <td><?relevance (size of ram)/1048576 ?> MB</td></tr>
          <tr> <td valign="top">DNS Name: </td>
              <td><?relevance dns name ?></td></tr>
        </table>
      </div>
    </div>
  </body>
</html>
```

For the offer.css to work correctly the following graphics files must be copied to the __UISupport directory from the Client directory:

```
bodyBg.jpg,
bodyHeaderBg.jpg
bullet.gif
sectionHeaderBG.gif
```

When run from the Client, this dashboard produces the following output:



TOKYO-FIN76

(Last updated: Mon, 11 Jun 2007 22:48:18 -0400)

Refresh

Computer Information

OS:	WinXP Media Center Edition.2600
RAM:	1022 MB
DNS Name:	tokyo-fin76

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

Geographically Locating Clients

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

1. In the Console, go to the **BigFix Management** domain, click the **Computer Management** folder node, and then click the **Location Property Wizard** node. A wizard document opens.

2. The wizard creates a named property allowing the Clients to identify themselves based on their subnet, IP range, or other information. Read the instructions in the wizard to create the property.

Locking Clients

You can change the locked status of any Tivoli Endpoint Manager Client in the network. This lets you exclude specific computers or groups of computers from the effects of Fixlet actions. This could be useful, for example, if you wanted to exclude certain development computers from any changes or updates. It also provides a powerful technique for testing new Fixlet actions on a limited set of unlocked computers, while keeping the rest of the network locked down. Client computers can be locked forever (until explicitly unlocked) or for a defined period of time.

Changes are made to the locked status of a Client by sending an action. As a consequence, the Console operator must supply proper authentication to lock or unlock any computer. Even though a Client is locked, there is still a subset of actions that can be accepted by the client. These include clock changes and unlock actions as well as actions from the Support site.

To lock or unlock a computer, follow these steps:

1. Click the **Computers** icon in the Domain Panel navigation tree to see the List Panel of networked Tivoli Endpoint Manager Client computers.
2. Select the computers that you want to lock.
3. Right-click and select **Edit Computer Settings** from the pop-up menu. (or select **Edit Computer Settings** from the **Edit** menu). The Edit Setting dialog opens.
4. Click the checkbox to either lock or unlock the computer.

Although the Console does not provide an explicit interface for setting an expiration date on the lock, you can create a custom Action to do this. For more information, see the ***Action Guide***.

Viewing Reports over the Web

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

Web Reports can be viewed at any time from **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Web Reports** or from the Console under **Tools > View Web Reports**.

Aggregating Multiple Servers into One Web Reports Server

Any Web Report server can be set up to include data from any other Server. To do this, the program must be able to connect to the other databases using ODBC communications over TCP/IP (that is, the computers must be on the same LAN or connected by VPN, and so on).

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

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

2. Log in to the Web Reports as an administrator.

3. Click **Administration > Database Settings > Add New Database** link.

4. Enter a Server Name that identifies 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 Server you want to include (for example, 192.168.100.123 or besserver1.acme.com).

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

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

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

Logging Web Reports

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

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

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

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

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

HTTPS Configuration

To provide more security to Web Reports, you can use HTTPS instead of HTTP to make your browser connection. To use HTTPS, you must have a proper SSL certificate. The SSL certificate must be in standard OpenSSL PKCS7 (.pem) file format. If the certificate meets all of the trust requirements of the connecting browser, then the browser connects without any interventions by the user. If the certificate does not meet the trust requirements of the browser, then the user is prompted with a dialog asking if it is OK to proceed with the connection, and provided with access to information about the certificate. Typically, a trusted certificate is one which is signed by a trusted authority (for example, Verisign), contains the correct host name, and is not expired. The .pem file is your SSL certificate, which you must obtain through your favorite CA. If you do no't require authentication back to a trusted root, you can also generate a self-signed certificate with the OpenSSL utilities (see the Tivoli Endpoint Manager support site for more information). When you have a certificate, place it on the computer running web reports (usually the Server) and follow these directions:

1. Run **regedit** and locate

   ```
   HKEY_LOCAL_MACHINE\Software\BigFix\EnterpriseClient\Settings\Client
   ```

   You need to add or modify three subkeys; one for the HTTPS flag, one for the location of the SSL certificate, and one for the HTTPS port number.

   For x64 systems, the key is here:

   ```
   HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\EnterpriseClient\Settings\Client
   ```

2. Create a new subkey of **Client** called _WebReports_HTTPServer_UseSSLFlag (it might already exist).

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

4. Create a new subkey of **Client** called _WebReports_HTTPServer_SSLCertificateFilePath (it might already exist).

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

6. Create a new subkey of **Client** called _WebReports_HTTPServer_PortNumber (it might already exist).

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

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

9. Restart the **BESWebReports** Service.

Part Four

Working with Tivoli Endpoint Manager

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

Adding New Operators and Master Operators

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

- **Ordinary Operators** manage a subset of the Clients based on their management rights and have restricted privileges to administer Tivoli Endpoint Manager functions.
- **Master Operators** have the ability to manage all the Clients and can also assign management rights to other operators.

The Site Administrator has the most important primary key (license.pvk), and can do anything a Master Operator can. However, it is bad practice to use your site key for ordinary operations. Instead, create a Master Operator account and use that key (publisher.pvk) exclusively for Console operations. To add new Operators and Master Operators to the Tivoli Endpoint Manager system, simply repeat the steps outlined in **Adding New Operators and Master Operators** (page 72).

Assigning Management Rights

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

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

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

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

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

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

2. Click on the **BigFix Management** domain and click the **Operators** node (if this choice is not available, you might not have the correct authorization to perform this command). You see a list of Console operators.

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

4. If user rights have already been set for this user, you 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 the **Delete** button.)

5. Use the filter panel on the left to narrow down the computers you want to assign to this operator. By shift- or ctrl-clicking on items in the **Retrieved Properties** or **Group** folders, you can specify a set of computers that share common properties or settings. As new computers are added to the network, they are automatically classified by their retrieved properties or group, and the correct Console operators are automatically 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 example, if you assign a user permissions on a certain subnet and a laptop moves to a different location with a different subnet, the user canno longer 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 Console:

1. Select **Manage Signing Keys** from the **Tools** menu.

2. Click the **Change Password** button at the bottom of the dialog.

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

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

Changing the Database Password

You can change your database password from the Console.

1. Select **Change Database Password** from the **File** menu (you must have the correct permissions to select this item).

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

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

Removing a Console Operator

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

1. Launch the program by selecting **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool**.

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

3. When you have deleted the operator, click **OK.** This removes the operator's privileges from the database, stops all of the user’s pending actions, and notifies the Clients that the private keys from that user are no longer valid.

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

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

Using NT Authentication

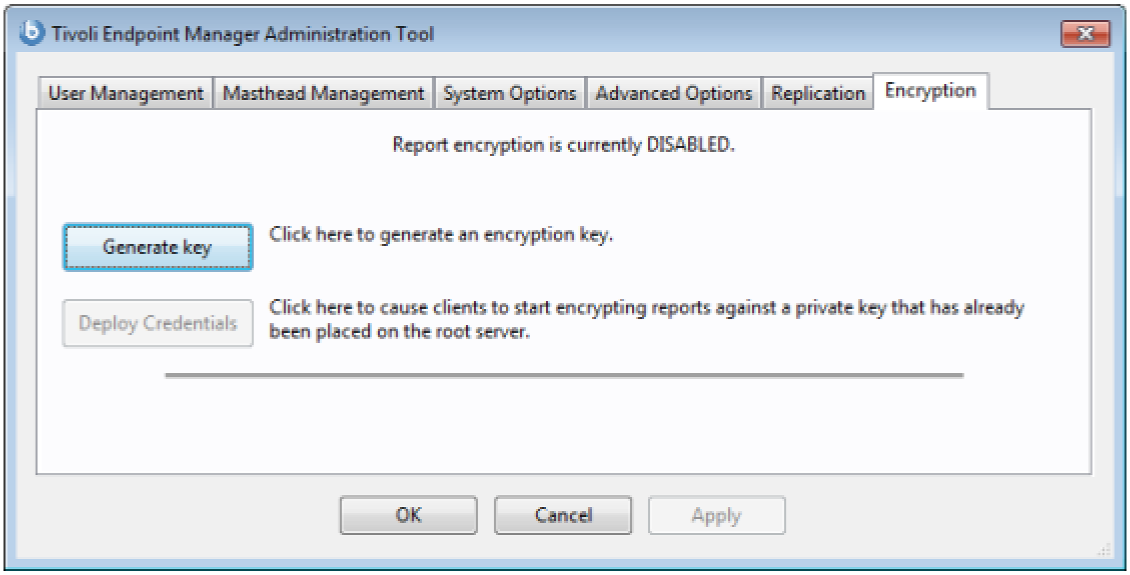
By default, Consoles create an ODBC connection to the SQL database, and the DSN is set to use SQL authentication. You can change this DSN to use NT authentication through the Windows ODBC Data Source Administrator. Doing so causes the Console to ask the current Windows user to authenticate with the SQL Server. For more information, see the article on NT authentication at the Tivoli Endpoint Manager support site.

Managing Client Encryption

Server and Relay-bound communications from Clients can be encrypted to prevent unauthorized access to sensitive information. To enable it, you must generate a key and provide a setting value. The setting is accomplished in the Console and is described in the section labeled **Enabling Encryption on Clients** (see page 40). The key is generated from the **Encryption** tab of the Tivoli Endpoint Manager Administration Tool:

1. Launch the Tivoli Endpoint Manager Administration Tool by selecting **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool**.

2. Select the **Encryption** tab.



Report encryption is currently DISABLED.

Click here to generate an encryption key.

Click here to cause clients to start encrypting reports against a private key that has already been placed on the root server.

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

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

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

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

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

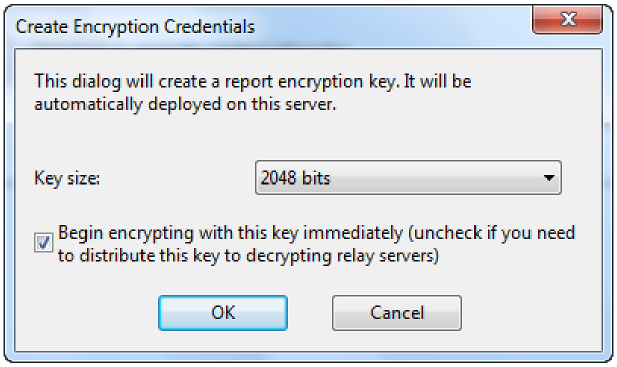
Generating a New Encryption Key

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

1. Launch the Tivoli Endpoint Manager Administration Tool by selecting **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool**.

2. Select the **Encryption** tab.

3. Click the **Generate key** button. The Create Encryption Credentials dialog opens.



Create Encryption Credentials

This dialog will create a report encryption key. It will be automatically deployed on this server.

Key size: 2048 bits

☑ Begin encrypting with this key immediately (uncheck if you need to distribute this key to decrypting relay servers)

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

5. Click **OK** to distribute this new key to your Clients. You must provide your Site Administration Private Key to propagate the Action. A final dialog asks for confirmation. For more information on encryption key sizes and server requirements, see the knowledge-base article on server requirements at the Tivoli Endpoint Manager support site.

Creating Top-level Decrypting Relays

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

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

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

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

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

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

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

There are a few considerations:

- You must manually transfer the key file from the server to the relay every time you create a new encryption key.
- During the transfer process, it is important not to expose your private key file. This means you must not move the key over the internet because anyone listening might be able make a copy of your private key file. Therefore it is best to physically transfer the key from one computer to another, for example, with a USB key.
- During the encryption key creation process, you have the option to create the private key file, but not propagate it out in the masthead. This step allows you time to transfer the new key file to the Relays before clients start posting encryption messages with that key.

Managing Downloads

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

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

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

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

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

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

For information about troubleshooting Relays, including bandwidth and downloading, see the KB article on relay health at the Tivoli Endpoint Manager support site.

Dynamic Download White-lists

Dynamic downloading extends the flexibility of Action scripts, adding the ability to use relevance clauses to specify URLs.

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

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

```
http://.*\.site-a\.com/.*

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

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

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

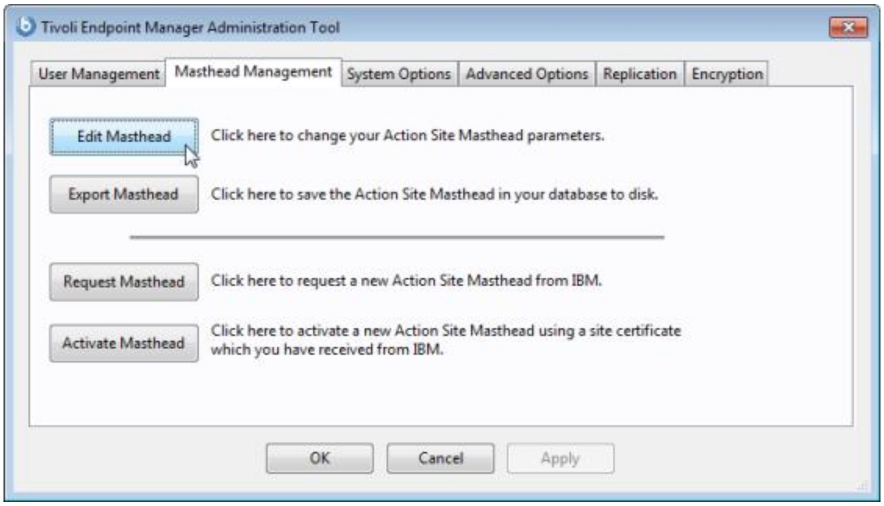
Editing the Masthead

You can change certain default parameters stored in the masthead by using the **Tivoli Endpoint Manager Administration Tool**. Here is how:

1. Launch the program from **Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool**.

2. Browse to the location of your site license and click **OK**.

3. Select the **Masthead Management** tab and Click the **Edit Masthead** button.



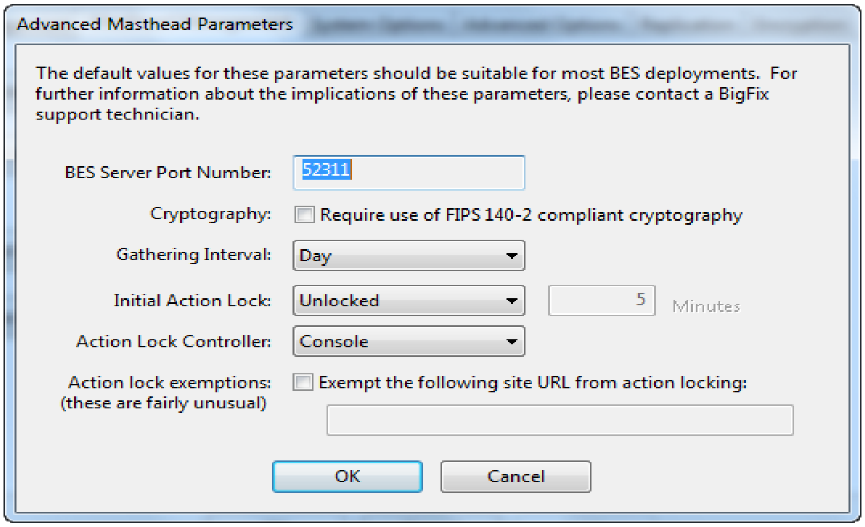
Click here to change your Action Site Masthead parameters.

Click here to save the Action Site Masthead in your database to disk.

Click here to request a new Action Site Masthead from IBM.

Click here to activate a new Action Site Masthead using a site certificate which you have received from IBM.

4. The Edit dialog opens.



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

Cryptography: □ Require use of FIPS 140-2 compliant cryptography

Gathering Interval: Day

Initial Action Lock: Unlocked 5 Minutes

Action Lock Controller: Console

Action lock exemptions: (these are fairly unusual) □ Exempt the following site URL from action locking:

Note: It is recommended that you keep the default settings on this page unless you have a specific reason to change them. Improper settings can cause Tivoli Endpoint Manager to work in non-optimal ways. Consult with the IBM software support for more details.

5. The parameters you can edit include:

- **Server Port Number:** In general, you will not want to change this number. In addition, if you decide to change this number *after* deploying the Clients, Tivoli Endpoint Manager will not work correctly. See **Modifying Port Numbers** in the next section.
- **Cryptography:** Check this box to implement the Federal Information Processing Standard on your network. This changes the masthead so that every TIVOLI ENDPOINT MANAGER component attempts to go into FIPS mode. By default, the client continues in non-FIPS mode if it fails to correctly enter FIPS, which might be a problem with certain legacy operating systems. Be aware that checking this box can add 3-4 seconds to the Client startup time.
- **Gathering Interval:** This option determines how long the Clients wait without hearing from the Server before they check whether new content is available. In general, whenever the Server gathers new content, it attempts to notify the 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 Client from the Server's perspective, a smaller interval becomes necessary to get timely response from the Clients. Higher gathering rates l only slightly affect the performance of the Server, because only the differences are gathered; a Client does not gather information it already has.
- **Initial Lock state:** You can specify the initial lock state of all Clients. Locked Clients report which Fixlet messages are relevant for them, but do not apply any actions. The default is to leave them unlocked and to lock specific Clients later on. However, you might wish to start with the Clients locked and then unlock them on an individual basis to give you more control over newly-installed Clients. Alternatively, you can set them to be locked for a certain period of time (in minutes).
- **Action Lock Controller:** This parameter determines who can change the action lock state. The default is **Console**, which allows any Console operator with management rights to change the lock state of any Client in the network. If you want to delegate control over locking to the end user, you can select **Client**, but this is not recommended.
- **Action Lock Exemptions:** In rare cases, you might need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL.

6. Click **OK** to enter the changes.

7. Enter your site password at the prompt.

Note: The masthead changes do NOT affect Clients that are already deployed, but you can export the masthead using the Administration Tool and replace the masthead in the Server so that Clients deployed with the new masthead use these changes.

Modifying Port Numbers

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

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

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

Modifying Global System Options

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

1. Launch the Administration Tool from Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool.

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

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

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

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

Scheduling Replication

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

1. Launch the Administration Tool from Start > Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool.

2. Select the **Replication** tab.

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

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

Extending the Tivoli Endpoint Manager License

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

1. Notify your IBM representative (if you have not paid for the extended license, you must talk to your sales person or reseller to buy an extended license).

2. Your server checks daily for a new version of your license. If you want to force your server to check immediately, in the Console, go to the **BigFix Management** domain, click the **License Overview** node, and click the **Check for license update** button.

Re-creating Site Credentials

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

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

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

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

Note: The Tivoli Endpoint Manager Site Administrator can change the password of the site-level key, if he or she knows the current password.

Updating the Tivoli Endpoint Manager

Like the other software installations in your enterprise, the Tivoli Endpoint Manager program itself must sometimes be maintained and updated. This capacity is built into the system. To guarantee that you are running the latest version of Tivoli Endpoint Manager, be sure to install the Client on all Server and 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 want to use the Fixlet messages to automatically update the Tivoli Endpoint Manager components, you can choose to manually update each component instead. Instructions on how to do this are included in the upgrade Fixlet message or are available from your support technician.

IBM Announcements

IBM maintains a mailing list to announce new products, updates, informational notices, and other information useful to Tivoli Endpoint Manager Administrators. IBM highly recommends that all customers subscribe to the announcements mailing list at: http://bigmail.bigfix.com/mailman/listinfo/besadmin-announcements.

Changing the Client Icon

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

1. Run the Tivoli Endpoint Manager Administration Tool (**Start > Program Files > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool**).

2. Click the **System Options** tab.

3. Click the **Change Icon** button and use the **Open** dialog to browse for your icon (.ico) file.

4. The Administration Tool immediately propagates this graphic to the Clients, but it is not incorporated into the interface until the Client restarts. After that, when a Client interface opens (in response to an action, a dashboard or an offer), it includes the graphic icon you specified.

Maintenance and Troubleshooting

If you are subscribed to the Patches for Windows site, you can ensure that you have the latest upgrades and patches to your SQL Server database servers. This means that you must install the Client on all your computers, including the Server and Console computers. In addition, you might 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 Tivoli Endpoint Manager 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. Tivoli Endpoint Manager writes out many temporary files, which might create a lot of disk fragmentation, so defragment your drive when necessary.Regular maintenance also involves running the occasional error-check on your disk drives.
- The Tivoli Endpoint Manager **Diagnostics Tool** performs a complete test on the server components and can be run any time you experience problems. See the section on **Running the TIVOLI ENDPOINT MANAGER Diagnostics Tool** (page 31).
- Check the **BigFix Management** domain often. There are a number of Fixlets available that can detect problems with any of your Tivoli Endpoint Manager components. This can often prevent problems before they ever affect your network.
- Check the Tivoli Endpoint Manager Knowledge Base at http://support.bigfix.com/. This site is continually updated, and if you cannot find an existing knowledge-base article about your question, you can find information about how to submit a question to the IBM software support.
- Add Relays to improve the overall system performance and pay close attention to them. Healthy Relays are important for a healthy deployment.
- Review the **Deployment Health Checks** dashboard in the **BigFix Management** domain for optimizations and failures.
- Set up monitoring activities on the Servers to notify you in the event of a software or hardware failure, including:
  - Server powered off or unavailable
  - Disk failure
  - Event log errors about Server applications
  - Server services states
  - FillDB buffer directory data back-up situations

Part Five

Resources

Deployment Scenarios

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

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

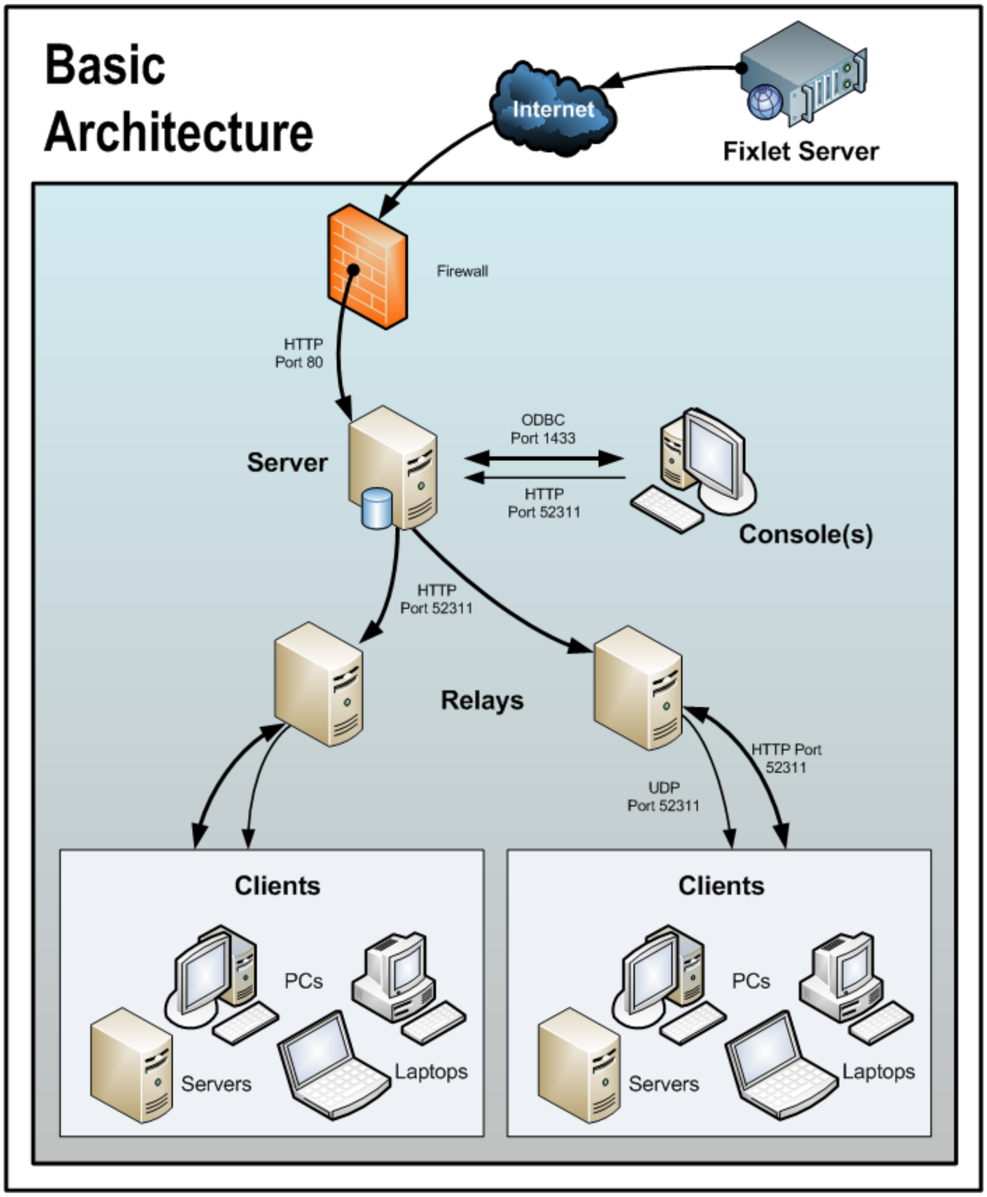
Relays are generally most efficient in fairly flat hierarchies. A top-level Relay directly eases the pressure on the Server, and a layer under that helps to distribute the load. However, hierarchies greater than two tiers deep might be counterproductive and must be carefully deployed. Multiple tiers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

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

With the correct deployment of Servers and Relays, networks of any size can be accommodated. Beyond the examples shown here, your IBM support technician can help you with other configurations.

Basic Deployment

This is a vastly simplified deployment designed to point out the basic hierarchy and the ports used to connect the components.



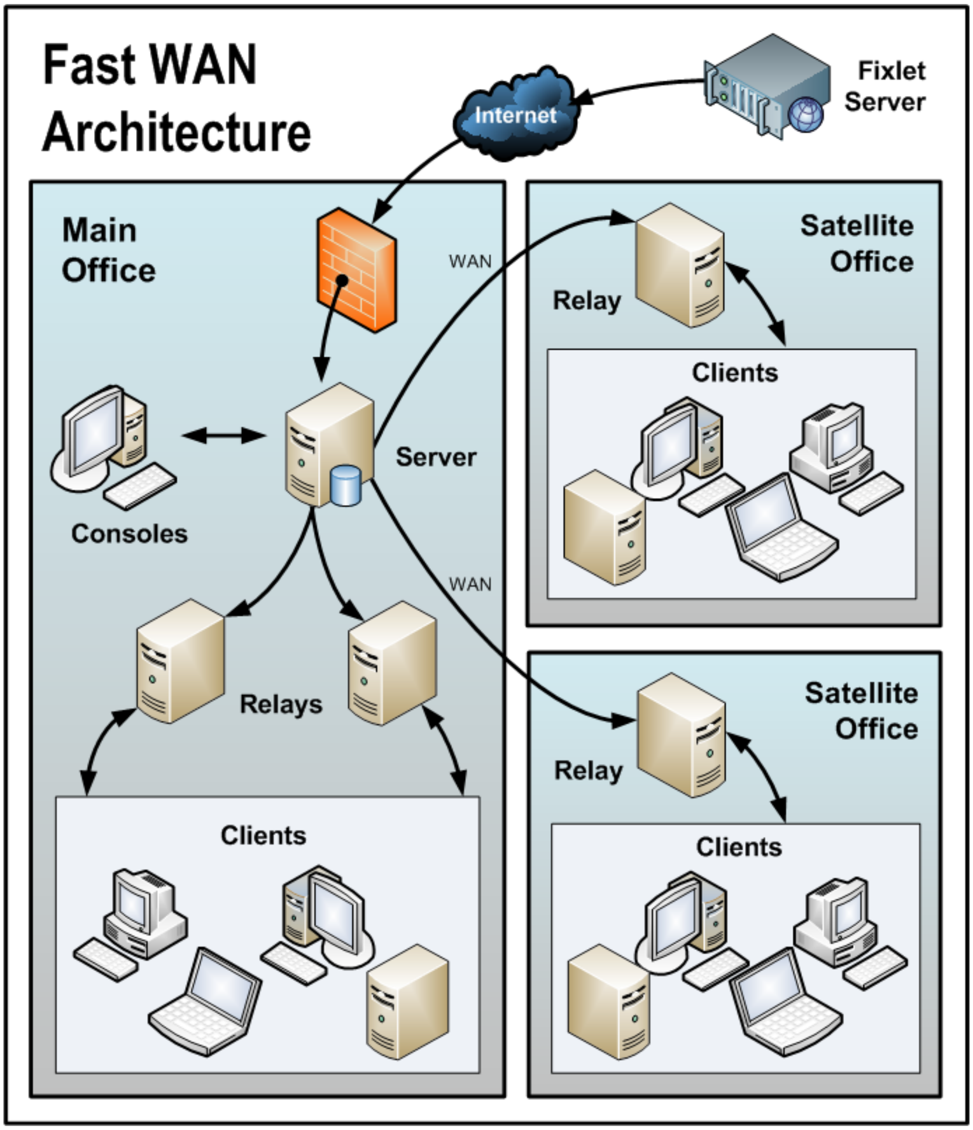
Note the following about the diagram:

- Port 80 is used to collect Fixlet messages over the Internet from Fixlet providers such as IBM.
- A dedicated port (defaulting to 52311) is used for HTTP communications between Servers, Consoles, Relays, and Clients.
- You need both an ODBC and an HTTP connection to run the Console.
- Relays are used to share the server load. This diagram only shows two Relays, but you can use dozens or even hundreds of Relays in a similar flat hierarchy. Typically a Relay is deployed for every 500-1,000 computers.
- The Tivoli Endpoint Manager Relays require an HTTP port (defaulting to 52311) to communicate with the Clients.
- The Tivoli Endpoint Manager Relays can also take advantage of a UDP port to alert the Clients about updates, but this is not strictly necessary.
- The Tivoli Endpoint Manager Clients are typically PCs or Workstations, but can include other servers, dockable laptops and more. Any device that can benefit from patches and updates is a candidate to include in the deployment.

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

Main Office with Fast-WAN Satellites

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

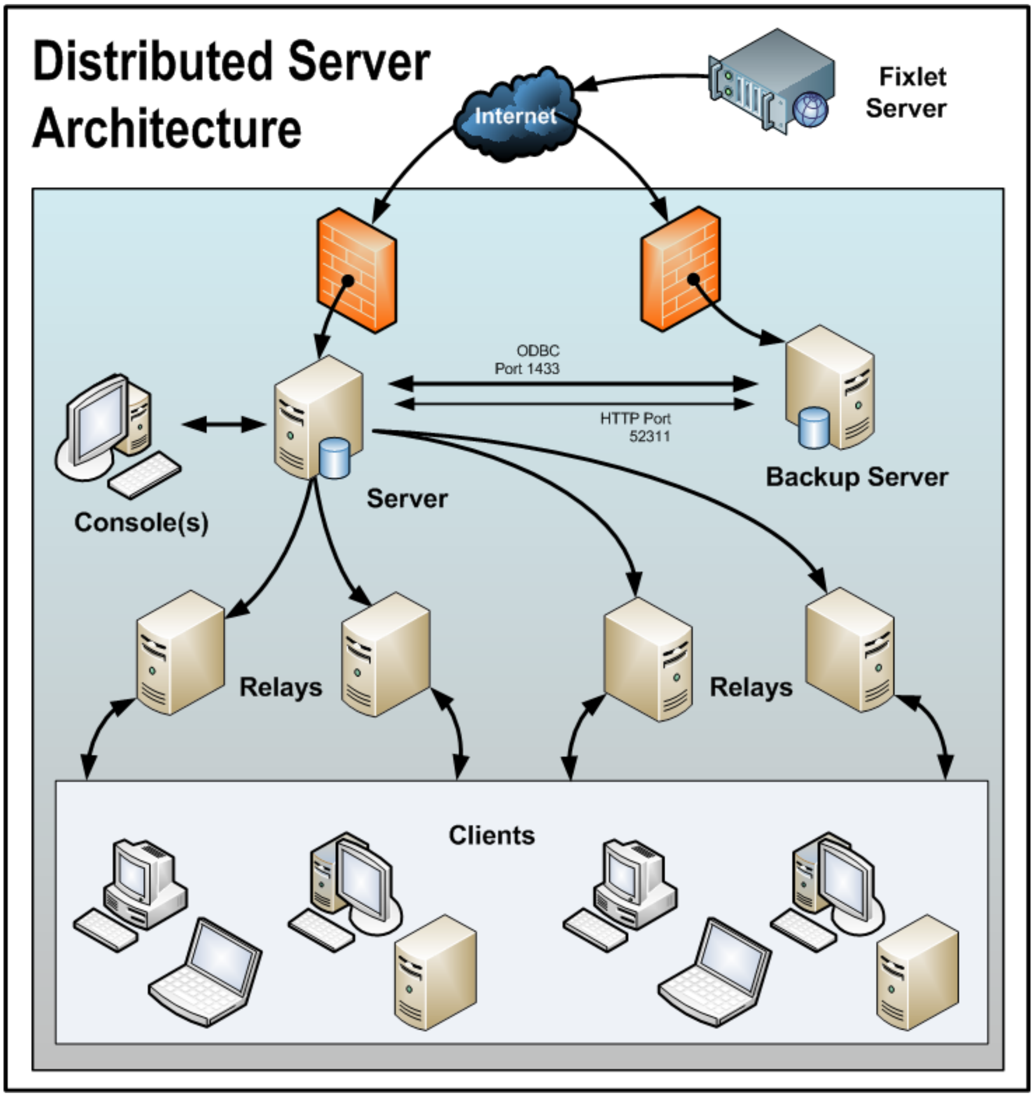


Note the following about the diagram:

- In this configuration, the Relays are used both to relieve the Server and to distribute the communications, optimizing the bandwidth.
- This scenario has large WAN pipes, so office relays can communicate directly to the main Server. A thin WAN could force a change in the layout of the Relays (see the scenarios above and below).
- The more Relays in the environment, the faster the downloads and response rates.
- Because of the nature of this network, when the Clients are set to **Automatically Locate Best Relays**, many of the Relays are the same distance away. In this scenario, the Clients automatically load-balance themselves amongst all the Relays that are nearby.
- For this high-speed LAN, a relatively flat hierarchy is recommended, with all Relays reporting directly to the main Server. Any extra levels in the hierarchy would only introduce unnecessary latency. However, if there were over 50-100 Relays in this environment, another level of Relays should be considered.

Distributed Server Architecture Setup

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



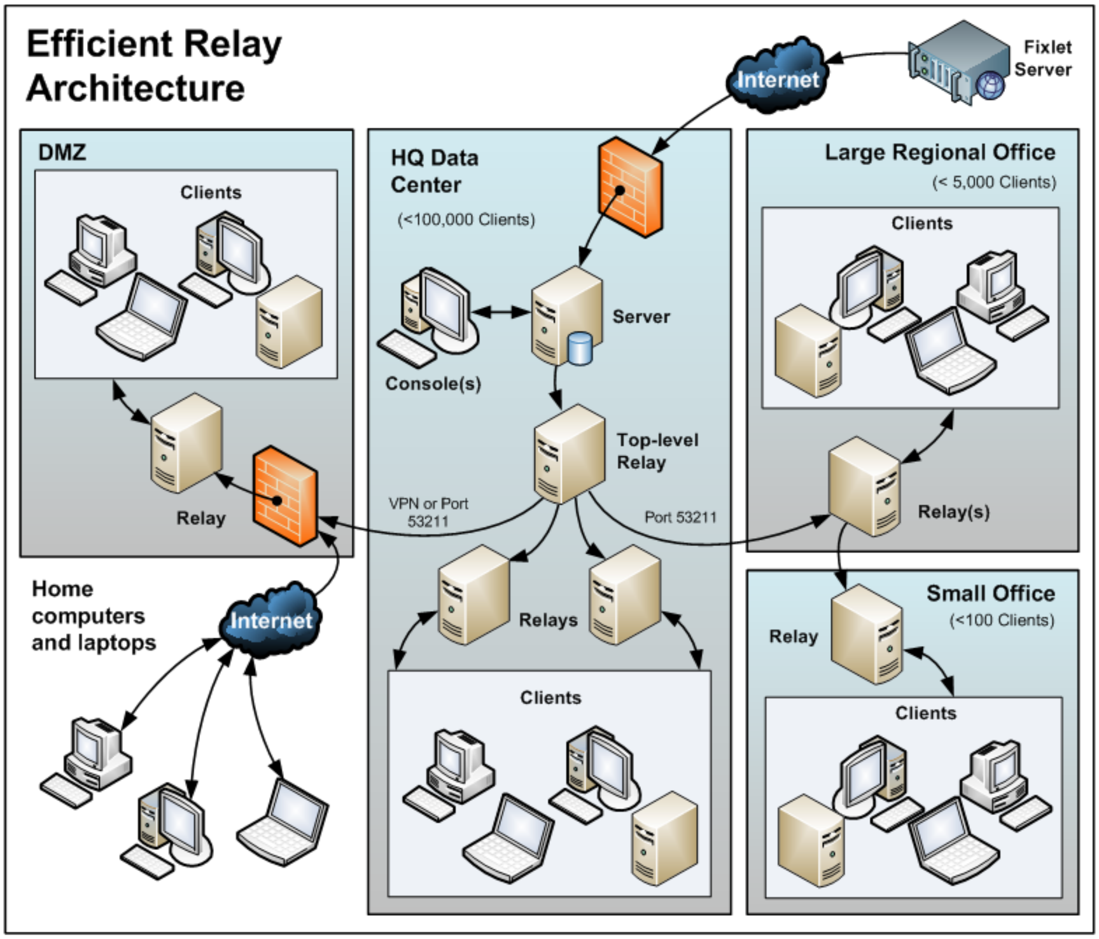
In the case of a failover, the Relays will automatically find the backup server and reconnect the network.

Note the following about the diagram:

- The Tivoli Endpoint Manager Servers are connected by a fast WAN, allowing them to synchronize several times per hour.
- The servers need both an ODBC and an HTTP link to operate and replicate properly.
- There is a primary Server with an ID of 0 (zero). It is the first Server that you install, and it is the default server for running the Tivoli Endpoint Manager Administration Tool.
- For the sake of clarity, this is a minimal configuration. A more realistic deployment would have a top-level Relay and other WAN connections to regional offices.
- The Tivoli Endpoint Manager Servers and Relays are configured so that control can be automatically routed around a server outage (planned or otherwise), and upon failover reconnection, the databases will be automatically merged.
- The Tivoli Endpoint Manager Servers communicate on a regular schedule to replicate their data. You can review the current status and adjust the replication interval through Tivoli Endpoint Manager Administration > Replication. For the best possible performance, these pipes should be fat.
- This diagram only shows two Servers, but the same basic architecture would apply to each additional server. With multiple servers, a shortest-path algorithm is used to guide the replication.
- When an outage or other problem causes a network split, it is possible to for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected on failover, precedence will go to the version on the server with the lowest Server ID.

Efficient Relay Setup

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

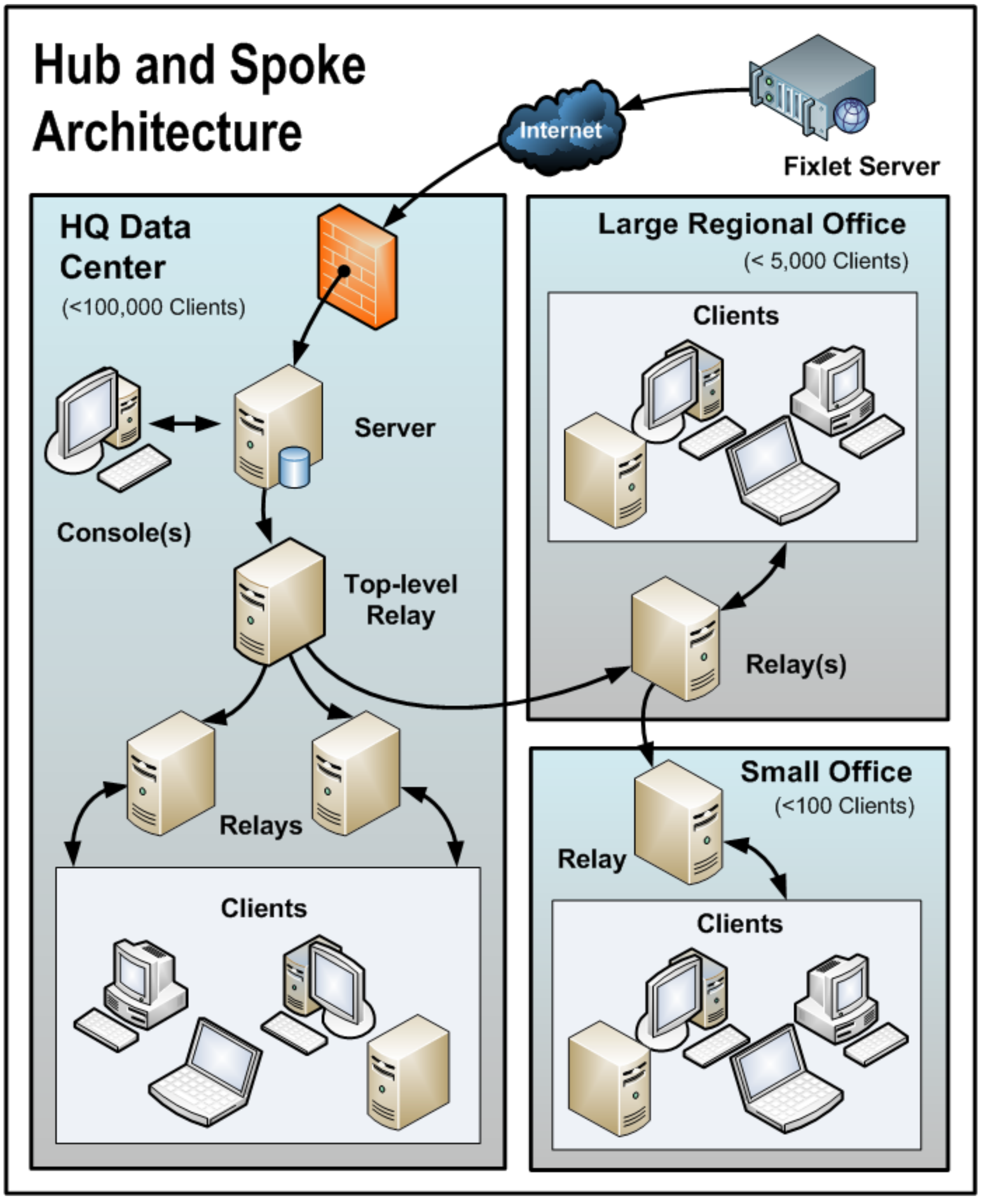


Note the following about the diagram:

- There is a dedicated server computer known as the Top-Level Relay that is used to take the load off of the Server computer.
- All Relays are manually configured to point to either the top level Relay or to another Relay that is closer. The general rule for configuring Relays is that you want as few levels as possible to the Relays unless there is a bandwidth bottleneck. Communications over thin pipes should be relay to relay. The top-level Relay will relieve the Server, and the secondary Relay can allow a single download to be distributed over hundreds of Clients.
- There is a Relay in the DMZ set up with a special trust relationship with the Server. This Relay will allow Clients in the DMZ or on the public Internet to be managed by Tivoli Endpoint Manager. The DMZ places a security firewall between the Relay and the set of home computers and laptops reporting in from the Internet.
- This diagram shows a single Relay in the large regional office. However, for offices with more than a few hundred clients, there will typically be multiple Relays to effectively distribute the load.
- As a general rule, you should deploy at least one Relay per 500-1000 Clients to maximize the efficiency of the Relay. See the article on relays at the Tivoli Endpoint Manager support site for more information.

Hub and Spoke

This scenario involves a main data center, a small number of large regional offices and many small regional offices. This configuration is common in large international organizations. The Tivoli Endpoint Manager Clients are installed on computers in offices all around the world. Many of these locations have slow WAN connections (8 kbps-512 kbps), but there will be many offices with faster WAN connections (1mbps-45mbps).



Often these locations are configured in a hub-and-spoke arrangement. This scenario builds on the previous one, but the hub-and-spoke configuration permits more levels in the Relay hierarchy.

Note the following about the diagram:

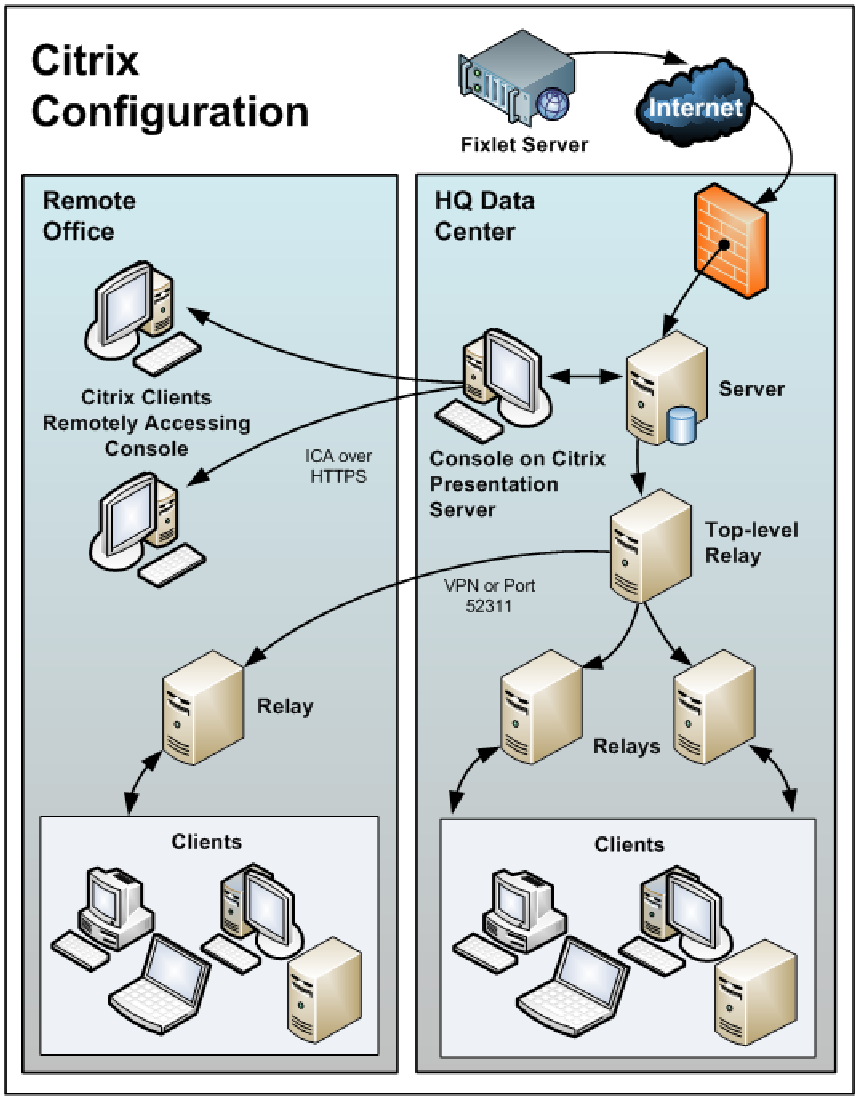
- In this scenario, the Relays are carefully deployed at the proper junctions within the WAN to optimize bandwidth. Poor placement of Relays can adversely impact your network performance.
- It is vital that at least one Relay is installed in every location with a slow WAN connection. Often a company will already have a server in just such a spot, acting as a file server, print server, AV distribution server, SMS distribution server or domain controller, or any other computer. The Tivoli Endpoint Manager Relay is usually installed on these existing computers.
- To provide redundancy in a typical office, more than one Relay should be installed. In case a Relay fails for any reason (powered down, disconnected from the network, etc.), its attached Clients can then automatically switch-over to a different Relay. A redundant relay is less important in very small offices because fewer computers are affected by the failure of a Relay.
- When the Clients are set to **Automatically Locate Best Relays**, they will choose the closest one. If any Relay should fail, the Clients will automatically seek out another Relay. You should monitor the Relay configuration after the initial automated setup (and periodically after that) to ensure that the Clients are pointing to appropriate locations. Talk to your support technician for more details on how to protect against overloading WAN pipes with Tivoli Endpoint Manager data.
- Bandwidth throttling at the Relay level is very helpful in this configuration. The Tivoli Endpoint Manager Relays are set up to download slowly across the WAN pipes so as not to saturate the slow links. See the article on throttling at the Tivoli Endpoint Manager support site for more information.
- Instead of pointing to the main Server, the Relays are configured to point to the top level Relay. This frees up the Server to couple more tightly to the Console and improves reporting efficiency.

The Tivoli Endpoint Manager Relays are configured to manually create the optimal hierarchy. The hierarchy has three levels (from the top down):

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

Remote Citrix / Terminal Services Configuration

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



Note the following about the diagram:

- In the main office, the Console is set up on a computer that is close to the Server for fast data collection. This is your Presentation Server.
- You must create user accounts for each remote user. These users will then be able to access the Console quickly because the time-critical data loading is done at the main office over a fast link.
- Your remote connection can be over HTTPS to improve security.
- Note that running a Console from a Presentation Server containing the private key is inherently less secure than if the key is stored on a removable drive.
- You might be able to benefit from load-balancing software to spread the remote accesses across multiple servers.
- The main bottleneck for a Console running on Citrix is memory size. If the Console runs out of memory, its performance will drop sharply. A good technique to determine the memory requirement is to open up the Console as a Master Operator. Check the memory used: this will indicate the maximum memory requirement per user. Then log in as a typical operator and use this as your average memory requirement. If your Citrix server can support all concurrent users with the maximum memory then a single box will suffice. If not, then use the average memory requirement per user to determine how many extra Citrix servers you may need.
- The second constraint is CPU power. During refreshes, the Console works best with a full CPU core. This means the Presentation server will be optimized with one CPU core running the Console for each concurrent user.
- The final concern is disk space for the Console cache. You can get a feel for the size of the cache by looking at an example on your local box: C:\Documents and Settings\<USERNAME>\Local Settings\Application Data\BigFix\Enterprise Console\BES_bfenterprise. There should be enough disk space to provide one cache file for each Console operator.

Glossary

Action Password—See signing password.

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

BigFix Enterprise Suite (BES)—The previous name for Tivoli Endpoint Manager.

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

Console—A management program that provides an overview of the status of all the computers with the Client installed in the network, identifying which might be vulnerable and offering corrective actions. Previously known as the BES Console, it is now known as the Tivoli Endpoint Manager Console, or simply Console.

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

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

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

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

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

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

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

Installation Generator—An application that creates installers for the core Tivoli Endpoint Manager system components.

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

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

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

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

Operator—A person who operates the Tivoli Endpoint Manager 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.

Relay—This is a Client 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 Clients, which dynamically choose the best Relay to connect to. Previously known as the BES Relay, it is now known as the Tivoli Endpoint Manager Relay, or simply Relay.

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

Root Server—Refers to the HTTP or HTTPS services offered by the main Server as an alternative to IIS. The Tivoli Endpoint Manager Root Server is specially tuned to Fixlet traffic and is more efficient than IIS for this application. Previously known as the BES Root Server, it is now known as the Tivoli Endpoint Manager Root Server, or simply Root Server.

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 Tivoli Endpoint Manager system. The server processes may be hosted by a single server computer or segmented to run on separate server computers or replicated on redundant servers. Previously known as the BES Server, it is now known as the Tivoli Endpoint Manager Server, or simply Server.

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

Site Administrator —The only Tivoli Endpoint Manager Console Operator with the right to create new Operators.

Site Administrator—The person in charge of installing Tivoli Endpoint Manager and authorizing Console operators.

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

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

System install folder—The directory on the Tivoli Endpoint Manager Server where the Server software and related files (including Console and Client installers) will be installed.

Tivoli Endpoint Manager database—A component of the system that stores data about individual computers and Fixlet messages. The Tivoli Endpoint Manager Server’s interactions primarily affect this database, which runs on SQL Server.

Tivoli Endpoint Manager—A preventive maintenance tool for enterprise environments that monitors computers across networks to find and correct vulnerabilities with a few simple mouse-clicks.

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

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

Part Six

Support

Technical Support

BigFix technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- BigFix Support Site
- Documentation
- Knowledge Base
- Forums and Communities

Part Seven

Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this

document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such

provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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

IBM Corporation

2Z4A/101

11400 Burnet Road

Austin, TX 78758 U.S.A.

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

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

Information concerning non-IBM products was obtained from the suppliers of those products, their

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

COPYRIGHT LICENSE:

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

TRADEMARKS:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

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

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

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

Other company, product, and service names may be trademarks or service marks of others.

Part Eight

Index