

IBM Endpoint Manager  
9.0 (Revised September 2013)

*Administrator's Guide*





IBM Endpoint Manager  
9.0 (Revised September 2013)

*Administrator's Guide*



**Note**

Before using this information and the product it supports, read the information in “Notices” on page 189.

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

© **Copyright IBM Corporation 2010, 2013.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.



---

# Contents

## Chapter 1. Introduction . . . . . 1

Service Management Connect. . . . .	2
Architectural components overview. . . . .	2

## Chapter 2. Sample deployment scenarios . . . . . 5

Basic deployment. . . . .	6
Main Office with Fast-WAN Satellites . . . . .	7
Distributed Server Architecture setup . . . . .	9
Efficient relay setup . . . . .	10
Hub and spoke . . . . .	11
Remote Citrix / Terminal Services Configuration . . . . .	13

## Chapter 3. Assumptions and requirements . . . . . 17

Assumptions . . . . .	17
Server requirements . . . . .	18
Console requirements . . . . .	19
Client requirements. . . . .	19
Database requirements. . . . .	19
Security requirements . . . . .	20
Network configuration requirements . . . . .	21

## Chapter 4. Types of installation . . . . . 23

Evaluation installation. . . . .	23
Production installation. . . . .	24
A basic installation . . . . .	25
A typical installation . . . . .	27
A multiple server installation . . . . .	27

## Chapter 5. Before installing . . . . . 31

Managing licenses . . . . .	31
Creating the License Authorization File . . . . .	32
Licensing Assistance . . . . .	34
Upgrading the masthead on the clients . . . . .	34
Modifying port numbers . . . . .	37

## Chapter 6. Installing on Windows systems . . . . . 39

Installation Steps . . . . .	39
Step 1 - Downloading IBM Endpoint Manager. . . . .	39
Step 2 - Requesting a license certificate and creating the masthead . . . . .	40
Step 3 - Installing the components. . . . .	46

## Chapter 7. Installing on Linux systems 71

Installing and configuring DB2 . . . . .	71
Installation Steps . . . . .	72
Step 1 - Downloading IBM Endpoint Manager. . . . .	72
Step 2 - Installing the Server. . . . .	73
Step 3 - Verifying Server Installation . . . . .	77
Installation Command Options . . . . .	78
Silent installation . . . . .	78

Installation Folder Structure . . . . .	79
Configuration, Masthead, and Log Files . . . . .	80
Managing the Endpoint Manager Services . . . . .	80
Changing the DB2 password . . . . .	81
Changing the DB2 port . . . . .	81
Removing the Primary Server on Linux systems . . . . .	82
Authenticating Additional Servers (DSA) . . . . .	82
Using DB2 Authentication . . . . .	82
Installing Additional Linux Servers (DSA) . . . . .	83
Understanding the server components . . . . .	84
Installing the Console . . . . .	85
Installing the Client Deploy Tool . . . . .	85
Installing the clients . . . . .	85
Using the Client Deploy Tool . . . . .	86
Installing the Client Manually . . . . .	88
Installing the client with MSI . . . . .	88
Running the IBM Endpoint Manager Administration Tool . . . . .	89

## Chapter 8. Post-installation configuration steps . . . . . 93

Post-installation steps . . . . .	93
Subscribing to Fixlet Sites . . . . .	96
Using relays . . . . .	97
Relay requirements. . . . .	98
Designating relays . . . . .	99
Automatically discovering relays . . . . .	99
Defaulting to Automatic Relay Discovery . . . . .	100
Notes about Automatic Relay Discovery . . . . .	100
Assigning a relay when the server is unreachable . . . . .	101
Using relay affiliation . . . . .	105
Manually selecting relays . . . . .	106
Viewing relay selections . . . . .	107
Monitoring relay health . . . . .	107
Setting up a proxy connection. . . . .	107
Setting a proxy connection on the server . . . . .	110
Setting up a proxy connection on a relay . . . . .	112
Setting up a proxy connection on a client or a child relay using the console . . . . .	112
Best practices to consider when defining a proxy connection in version 9.0 . . . . .	113
Managing operators and permissions . . . . .	115
Site administrator responsibilities. . . . .	115
Operators permissions . . . . .	116
Operators and analyses . . . . .	118
Adding console operators . . . . .	118
Integrating Linux Server with Active Directory . . . . .	118
Managing Replication (DSA) on Windows systems . . . . .	122
Changing the replication interval on Windows systems . . . . .	122
Switching the master server on Windows systems . . . . .	122
Uninstalling a Windows replication server. . . . .	123
Managing Replication (DSA) on Linux systems . . . . .	123

Changing the replication interval on Linux systems . . . . .	123
Switching the master server on Linux systems . . . . .	124
Uninstalling a Linux replication server . . . . .	124
HTTPS Configuration . . . . .	125
Configuring HTTPS manually on Windows systems . . . . .	127
Configuring HTTPS manually on Linux systems . . . . .	127
Downloading files in air-gapped environments . . . . .	128
On Windows systems . . . . .	128
On Linux . . . . .	129
Transferring Downloaded Files . . . . .	130
Managing Client Encryption . . . . .	132
Generating a new encryption key. . . . .	133
Creating top-level decrypting relays. . . . .	134
Message Level Encryption (MLE) Overview . . . . .	135
Changing the Client Icon . . . . .	136

## **Chapter 9. Running backup and restore . . . . . 137**

Backing up on Windows systems. . . . .	137
Backup Procedure . . . . .	137
Recovery procedure . . . . .	138
Verifying restore results . . . . .	138
Backing up on Linux systems . . . . .	139
Backup procedure . . . . .	139
Recovery procedure . . . . .	140
Verifying restore results . . . . .	141

## **Chapter 10. Upgrading on Windows systems. . . . . 143**

Upgrade Paths to V9.0 . . . . .	143
Before upgrading . . . . .	144
Upgrading the Installation Generator . . . . .	144
Upgrading the Server . . . . .	144
Upgrading the Console . . . . .	145
Upgrading the Relays . . . . .	145
Upgrading the Clients . . . . .	145
Upgrading the Web Reports . . . . .	145

## **Chapter 11. Upgrading on Linux systems. . . . . 147**

Upgrade types and paths . . . . .	147
Before upgrading . . . . .	148
Upgrading the server. . . . .	148
Upgrading the console . . . . .	149
Upgrading the relays. . . . .	149
Upgrading the Clients . . . . .	149
Upgrading the Web Reports . . . . .	149

## **Chapter 12. Additional configuration steps . . . . . 151**

Optimizing the servers . . . . .	151
Optimizing the consoles. . . . .	152
Managing Bandwidth . . . . .	152
Dynamic Throttling . . . . .	153

Managing Downloads . . . . .	154
Dynamic download White-lists . . . . .	155
Creating client dashboards . . . . .	156
Geographically locating clients . . . . .	158
Locking clients . . . . .	158
Editing the Masthead on Windows systems . . . . .	159
Editing the Masthead on Linux systems . . . . .	161
Modifying Global System Options . . . . .	162
Scheduling replication . . . . .	163
Extending the IBM Endpoint Manager License . . . . .	164
Re-creating Site Credentials. . . . .	164

## **Chapter 13. Maintenance and Troubleshooting . . . . . 165**

### **Appendix A. Upload and archive manager settings. . . . . 167**

Editing the archive manager settings . . . . .	167
Creating a Custom Action . . . . .	168
Archive Manager . . . . .	168
Archive Manager Settings . . . . .	168
Archive Manager internal variables . . . . .	169
Archive Manager Index File Format . . . . .	169
Upload Manager . . . . .	170
Upload Manager Settings . . . . .	170
PostFile . . . . .	172
PostFile Settings . . . . .	173
Resource Examples . . . . .	173

### **Appendix B. Command-Line Interface 175**

Location . . . . .	175
Conventions and usage . . . . .	175
User Authentication and Session Management . . . . .	175
Local Data Directory . . . . .	176
FIPS Deployments. . . . .	176
Making Requests . . . . .	176
Query Parameters . . . . .	177
POST and PUT Input. . . . .	177
Portability . . . . .	177
IEM CLI Examples . . . . .	178
Login . . . . .	178
Operators . . . . .	178
Advanced Options . . . . .	178
System Options. . . . .	179
Export masthead . . . . .	179
Actions . . . . .	180
Fixlet . . . . .	180
LDAP . . . . .	181
Role . . . . .	182

### **Appendix C. Glossary. . . . . 183**

### **Appendix D. Support . . . . . 187**

### **Notices . . . . . 189**

---

## Chapter 1. Introduction

IBM® 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. Using 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.

IBM Endpoint Manager is easy to install and has built-in public and 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. IBM 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 IBM Endpoint Manager. It provides you with:

1. System requirements for each component.
2. Licensing and installation instructions.
3. Information about configuring and maintaining IBM Endpoint Manager.

For further information about product components functionality and operating instructions, see the IBM Endpoint Manager *Console Operator's Guide*.

---

## Versions

The guide includes the functions introduced in IBM Endpoint Manager, Version 9.0.

---

## Service Management Connect

Connect, learn, and share with Service Management professionals: product support technical experts who provide their perspectives and expertise.

Access Service Management Connect at <https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=it#/wiki/Tivoli%20Endpoint%20Manager>.

Use Service Management Connect to:

- Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
- Connect one-on-one with the experts to collaborate and network about Tivoli and the (enter your community name here) community.
- Read blogs to benefit from the expertise and experience of others.
- Use wikis and forums to collaborate with the broader user community.

---

## Terms used in this guide

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

**Console**

always means IBM Endpoint Manager Console

**Client** always means IBM Endpoint Manager Client

**Server** always means IBM Endpoint Manager Server

**Relay** always means IBM Endpoint Manager Relay

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

---

## Architectural components overview

The IBM Endpoint Manager system has the following main components:

**IBM Endpoint Manager clients:**

Also called agents, are installed on every computer that you want to manage using IBM Endpoint Manager. They access a collection of Fixlet messages that detects security exposures, incorrect configurations, and other vulnerabilities. The client can implement corrective actions received from the console through the server. The IBM Endpoint Manager Client runs undetected by users and uses a minimum of system resources.

The IBM Endpoint Manager also allows the administrator to respond to screen prompts for those actions that require user input. IBM Endpoint Manager clients can encrypt their upstream communications, protecting

sensitive information. IBM Endpoint Manager Client software can run in Windows, Linux, Solaris, HP-UX, AIX, and Macintosh operating systems.

#### **IBM Endpoint Manager Servers :**

Offer a collection of interacting services, including application services, a web server, and a database server, forming the heart of the IBM Endpoint Manager system. They coordinate the flow of information to and from individual computers and store the results in the IBM Endpoint Manager database. The IBM Endpoint Manager Server components operate quietly in the background, without any direct intervention from the administrator. IBM 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 IBM Endpoint Manager supports multiple servers, adding a robust redundancy to the system.

#### **IBM Endpoint Manager Relays:**

Increase the efficiency of the system. Instead of forcing each networked computer to directly access the IBM Endpoint Manager Server, relays spread the load. Hundreds to thousands of IBM Endpoint Manager clients can point to a single IBM Endpoint Manager Relay for downloads, which in turn makes only a single request to the server. IBM Endpoint Manager relays can connect also to other relays, further increasing efficiency. An IBM Endpoint Manager relay need not be a dedicated computer; the software can be installed on any Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Red Hat Enterprise Linux 4,5,6, or Solaris 10, computer with the IBM Endpoint Manager client installed. As soon as you install an IBM Endpoint Manager relay, the clients in your network can automatically discover and connect to them.

#### **IBM 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 IBM Endpoint Manager Console allows an authorized user to quickly and simply distribute fixes to each computer that needs them without impacting any other computers in the network. You can run the IBM Endpoint Manager console 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 IBM Endpoint Manager Server. Consoles for large deployments are often hosted from Terminal Servers or Citrix Servers.



---

## Chapter 2. Sample deployment scenarios

The following deployment scenarios 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 low-speed communications.

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 that would service from 50-200 second-tier relays. The following examples help you deploy the most efficient network layout.

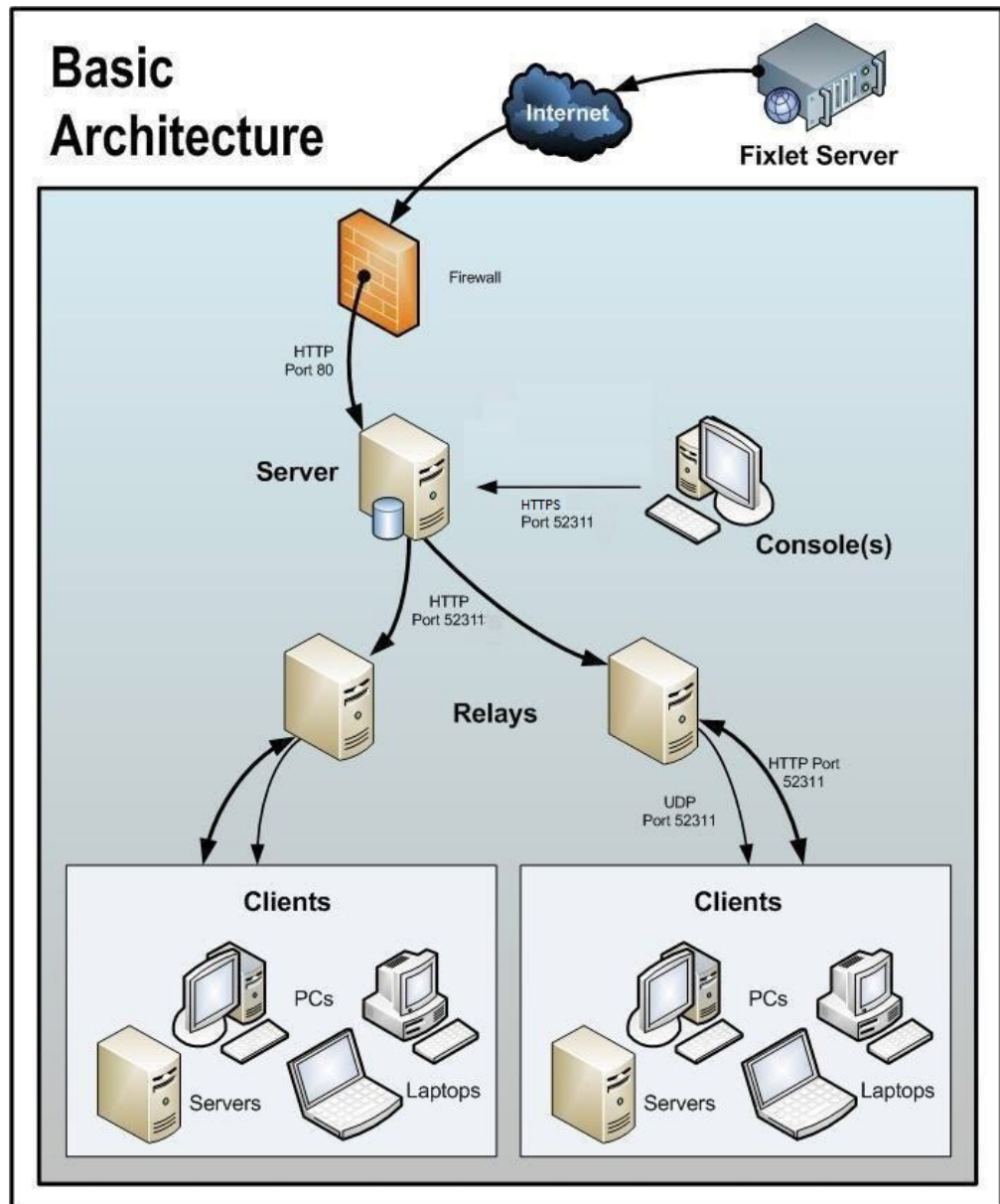
Note that additional servers can also add robustness to a network, by spreading the load and supplying redundancy. Using redundant servers allows failbacks and failovers to be automated, providing minimal data loss, even in serious circumstances.

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 very simplified deployment that points 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, relays, and Clients.
- A dedicated port (defaulting to 52311) is used for HTTPS communications between servers and Consoles.



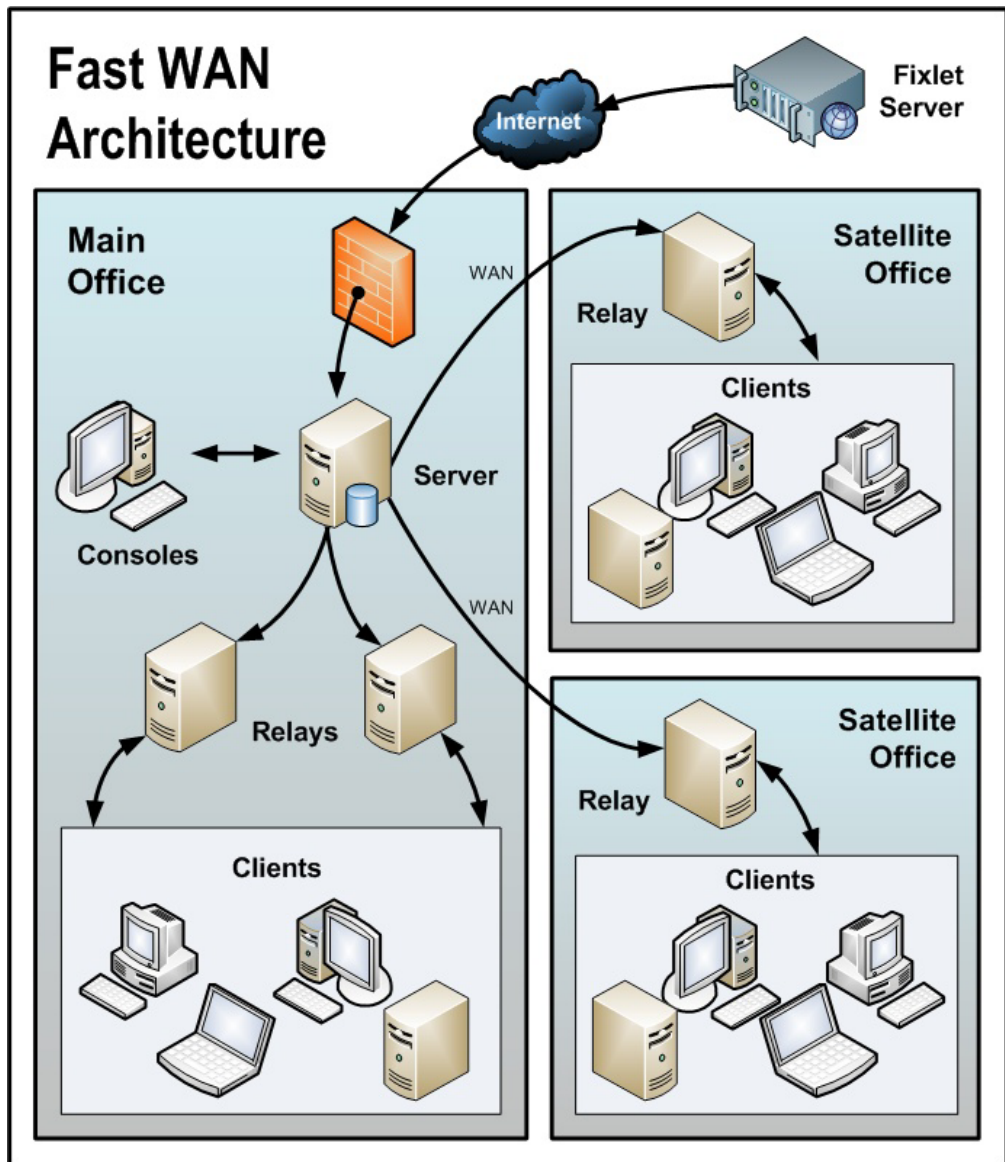
- Relays are used to share the server load. This diagram only shows two relays, but you can use dozens or even hundreds of relays in a similar flat hierarchy. Typically a Relay is deployed for every 500-1,000 computers.
- The IBM Endpoint Manager relays can also take advantage of a UDP port to alert the Clients about updates, but this is not strictly necessary.
- The IBM 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.

IBM 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 consider.

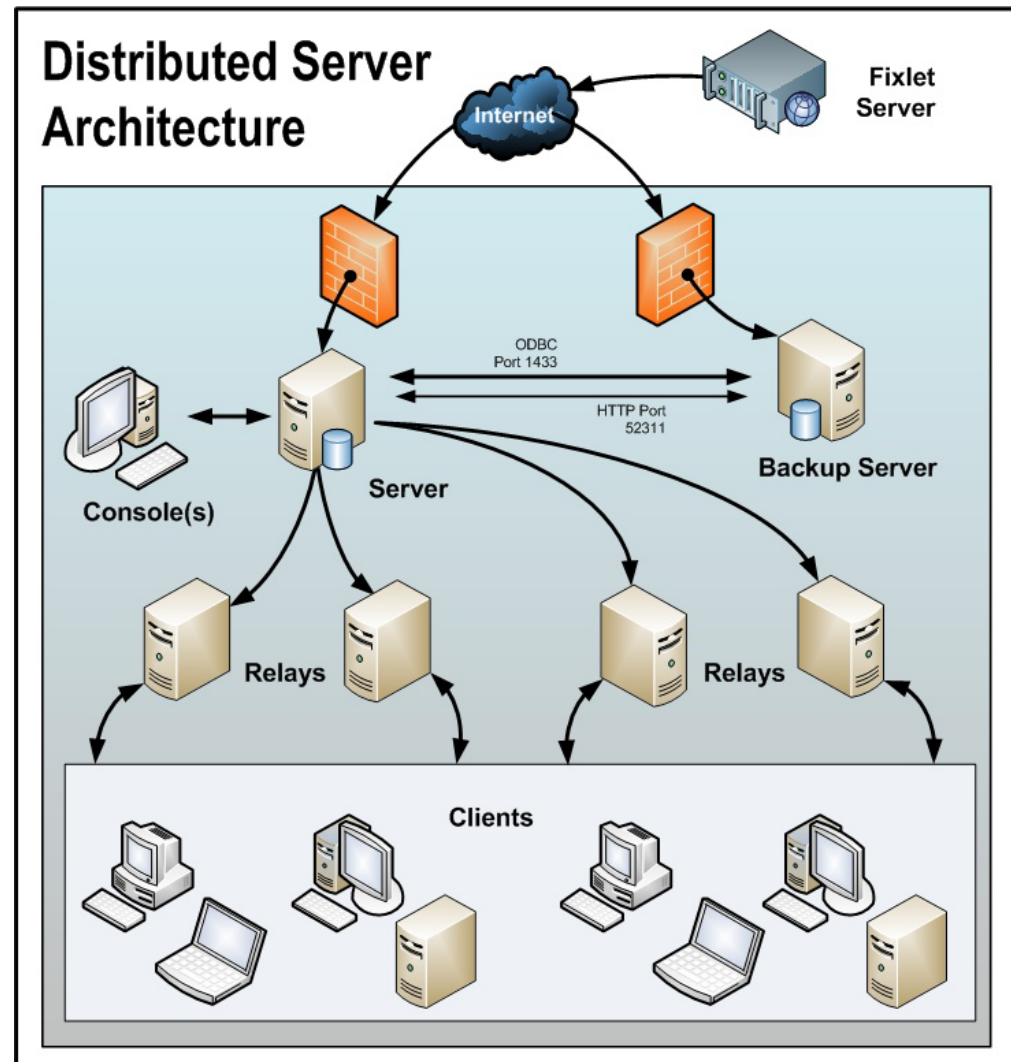


Note the following about the diagram:

- 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 with 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 relay**, 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 might want to deploy multiple, fully-redundant servers to maintain continuous operation even in the event of serious disruptions. Multiple servers also help to distribute the load and create a more efficient deployment. Here is a simple diagram of how multiple servers might be set up to provide redundancy:



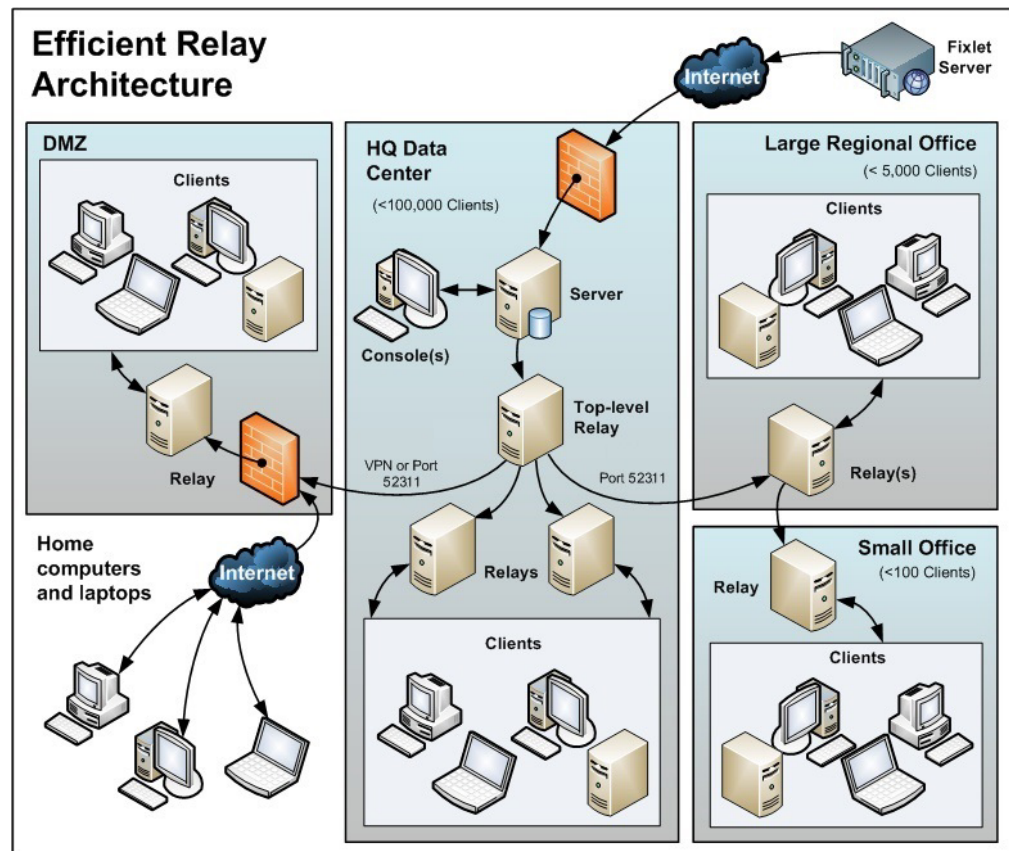
In the case of a failover, the relays automatically find the backup server and reconnect the network. Note the following about the diagram:

- The IBM 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 IBM 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 IBM 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 are automatically merged.
- The IBM Endpoint Manager servers communicate on a regular schedule to replicate their data. You can review the current status and adjust the replication interval through IBM 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 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 goes 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.



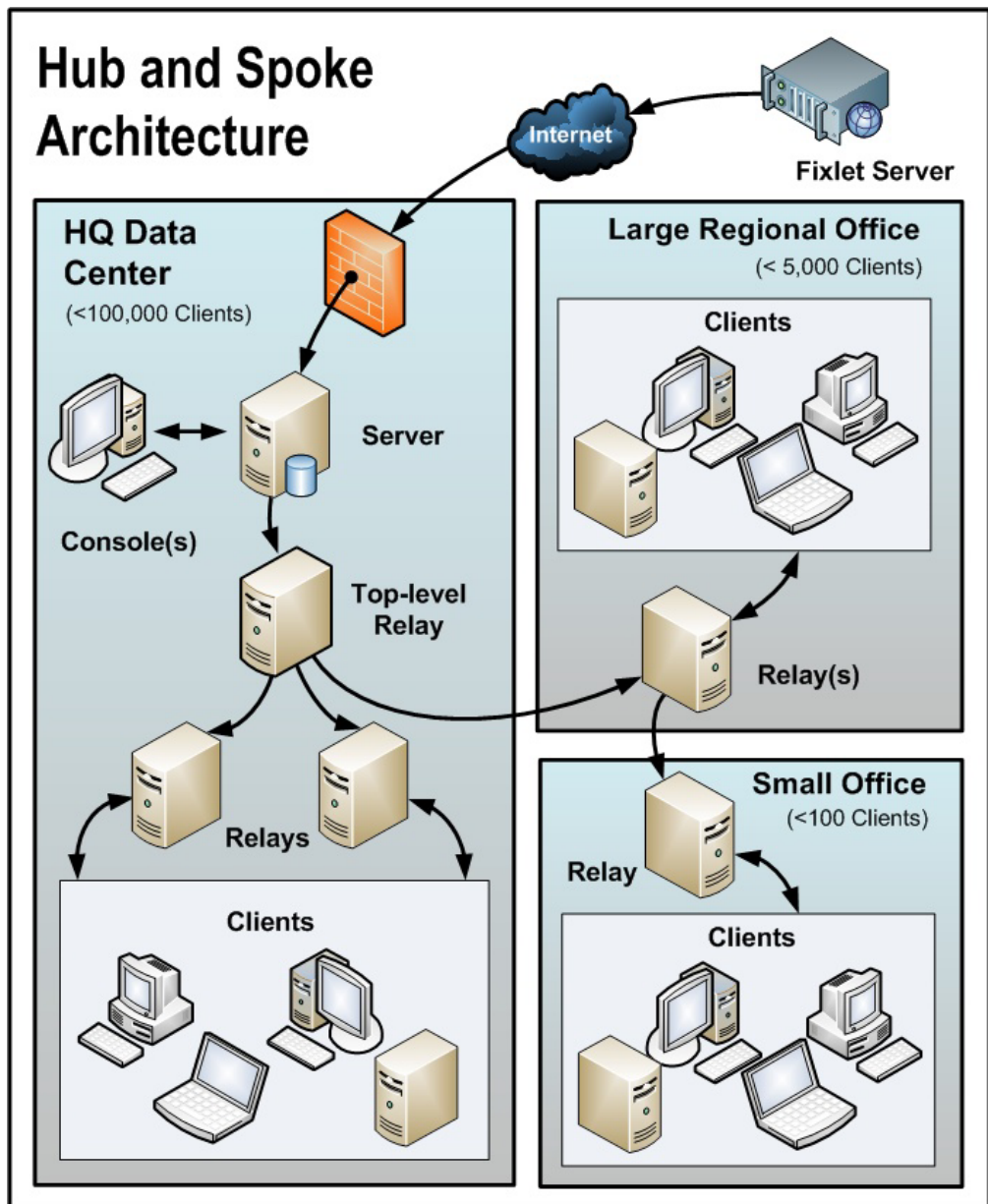
Note the following about the diagram:

- There is a dedicated server computer known as the Top-Level relay that is used to take the load off 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 relieves the server, and the secondary relay allows 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 allows clients in the DMZ or on the public Internet to be managed by IBM 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. For more information see the article on relays at the IBM Endpoint Manager support site.

---

## 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 IBM 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 are 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 already has a server in just such a location, acting as a file server, print server, AV distribution server, SMS distribution server or domain controller, or any other computer. The IBM Endpoint Manager relay is usually installed on these existing computers.
- To provide redundancy in a typical office, more than one relay should be installed. If a relay fails for any reason (powered down, disconnected from the



network, and so on.), 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 Relay**, they will choose the closest one. If any relay fails, the clients 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 about how to protect against overloading WAN pipes with IBM Endpoint Manager data.
- Bandwidth throttling at the relay level is very helpful in this configuration. The IBM Endpoint Manager relays are set up to download slowly across the WAN pipes so as not to saturate the slow links. For more information see the article on throttling at the IBM Endpoint Manager support site.
- 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.

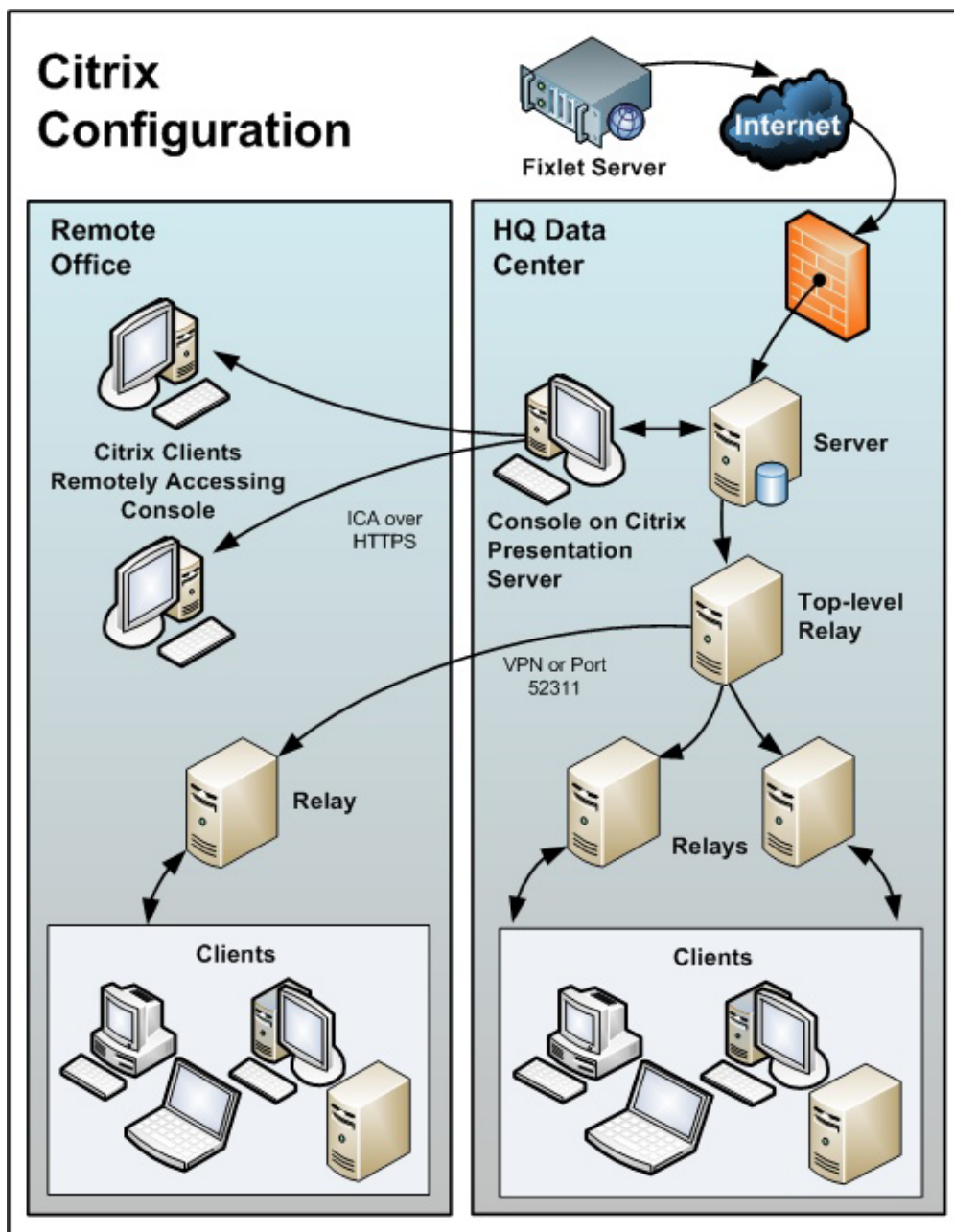
The IBM Endpoint Manager relays are configured to manually create the optimal hierarchy. The hierarchy has three levels (from the top down):

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 IBM 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 can then 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 decreases sharply. A good technique to determine the memory requirement is to open the console as a Master Operator. Check the memory used: this indicates 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 suffices. If not, then use the average memory requirement per user to determine how many extra Citrix servers you might 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 understand the size of the cache by looking at an example on your local computer:  
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.



---

## Chapter 3. Assumptions and requirements

IBM Endpoint Manager runs efficiently using minimal server, network, and client resources. 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 IBM Endpoint Manager allows a single server to support hundreds of thousands of computers.

---

### Assumptions

The process of getting the IBM 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:

- IBM Endpoint Manager servers can make connections to the Internet on port 80. The IBM 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 IBM Endpoint Manager Server from the Internet Fixlet Server. For more information, see the article about air-gaps at the IBM Endpoint Manager support site.
- Each IBM 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 HTTP connection to the IBM Endpoint Manager server.
- Each IBM Endpoint Manager client computer in the network must be able to make an HTTP connection to a server or relay on the specified port (the default port is 52311, but any available port can be used).
- Each console in the network must be able to make an HTTPS connection to a server on the same port as the clients (default value is 52311).

Some enterprises might not meet one or more of these conditions, but can still deploy IBM Endpoint Manager in their environments. For more information see **Deployment Scenarios** (page Chapter 2, “Sample deployment scenarios,” on page 5) If your network configuration does not match any of the scenarios in this chapter, contact a support technician for more options.

The initial deployment of a minimal IBM Endpoint Manager system (server, console, and a few clients) takes about one hour to complete.

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 IBM 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.

---

## Server requirements

To find the latest information about server requirements, see IBM Endpoint Manager Server Requirements.

### Supported operating systems:

- Windows:
  - Windows 2008 R2 (x86, x64) Enterprise
  - Windows 2008 (x86, x64) Enterprise
  - Windows 2003 (x86, x64) Enterprise
  - Windows Server 2012

**Note:** The Windows firewall must be turned off. User Account Control on Windows 2008 and Windows 2008 R2 must be disabled or lowered so that services that do not run as LOCAL SYSTEM are not interfered with by the User Account Control pop-up messages.

**Note:** Ensure that .NET Framework 3.5 is installed before starting to install Endpoint Manager on a new Windows Server 2012.

- Linux:  
Red Hat Enterprise Linux (RHEL) Server x86-64 version 6 Fixpack 3 or higher (64-bit Architecture)

### Dependencies:

- IBM DB2 10.1. For information about how to install DB2 server on Red Hat Enterprise Linux Server 64-bit see IBM DB2 Version 10.1 Information Center.
- Korn Shell (KSH), required by IBM Endpoint Manager Linux Installer script
- 32 bit-compatibility libraries, required by IBM Endpoint Manager Linux Server and WebReports components:

- pam-x.x.x-x.el6.i686
  - cyrus-sasl-lib-x.x.x-x-el6-i686
  - libstdc++-x.x.x-x.el6.i686 and all their prerequisites
  - fontconfig.i686
  - libXext.i686
  - libXrender.i686
  - zlib.i686

**Note:** Windows Endpoint Manager servers cannot be migrated to Linux Endpoint Manager servers. The Linux Endpoint Manager server is for new installations only.

### Minimum disk space requirements to install Endpoint Manager server and WebReports on Linux:

Endpoint Manager Server: 300MB; DB2: 1GB (6GB recommended)

Endpoint Manager Web Reports: 250MB; DB2: 700MB

For additional hardware requirement information, see Detailed hardware requirements by operating system family.

---

## Console requirements

To find the latest information about console requirements, see IBM Endpoint Manager Console Requirements.

The IBM 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 increases, you might need a more powerful computer.

The IBM 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 IBM 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

To find the latest information about client requirements, see IBM Endpoint Manager for Lifecycle Management V9.0. .

---

## Database requirements

The database stores all the data retrieved from the Clients. Before installing the IBM Endpoint Manager server, ensure that the database requirements are met.

- IBM Endpoint Manager server on Windows systems supports the following configurations:
  - Local or remote SQL Server 2005, 2008, 2008 R2, or SQL Server 2012.

**Important:** Ensure that the user that logs in to install the IBM Endpoint Manager server has the sa rights for the MSSQL Server to create the database and its tables.

- IBM Endpoint Manager server on Red Hat Enterprise Linux systems supports the following configurations:
  - If the DB2 server is installed locally: DB2 10.1 Enterprise server Edition 64-bit or Workgroup Server Edition 64-bit.
  - If the DB2 server is installed remotely: IBM Data Server client 10.1.

**Note:** To check if you have a server or a client installed and to verify the DB2 edition, you can run the `db2licm -l` command. On the computer where the DB2 server is installed, you receive a detailed report, if only the client is installed you receive an empty report. To check which DB2 version is installed, run the `db2level` command.

---

## 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 IBM Endpoint Manager, you must use the Installer on Windows and the script `install.sh` on Linux 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.

During the installation process a server signing key is created and stored as a file on the server machine. Whenever operators issue an action, it is digitally signed by the server signing key, and the Client will only trust actions that are signed by that key. Since Clients will trust any action signed by the server signing key, it is important to protect the server signing key file. To protect the server signing key file, administrator access to the server machine must be restricted.

Fixlet messages are also digitally-signed. The Fixlet site author signs each message with a key that can be traced back to the IBM 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 IBM 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.
- Make sure that TCP/IP and UDP on the specified port (default value is 52311 for all the components, included the Console) is completely unblocked at all internal routers and internal firewalls.
- Verify that your external router forbids inbound and outbound traffic on the specified port (default value is 52311 for all the components) so that IBM Endpoint Manager-related traffic will be unable to flow into or out of your network.

You can administer roaming laptops by putting an authenticating relay in your DMZ. For additional details see Internal Relays..

- Verify with your network administrator that you can allow the Server to access the Internet via port 80. The BES Root Server service on Windows and the

beserver service on Linux access the Internet and by default they run as the SYSTEM account on Windows and as root on Linux.

**Note:** On Windows, if the SYSTEM account cannot reach the Internet because of proxy or firewall restrictions, then you must set the proxy by performing the following command:

```
BESAdmin /setproxy /user:username /pass:password
```

Detailed instructions about how to configure the server are available from the knowledge base at the IBM 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 IBM Endpoint Manager support site.

- Secure the Server computers and the SQL 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 incorrectly. Contact your IBM software support if you have any specific questions about lockdown procedures.

---

## Network configuration requirements

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

- All internal network communication is on one specified port (52311 is the default port for all the components, including the console) 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 IBM Endpoint Manager Server should connect to the network at 100 mbps or higher.
- Consoles should have high speed connections to the IBM Endpoint Manager Server (100 mbps or higher)
- The Windows Firewall must be turned off on the IBM Endpoint Manager Server machine.
- The IBM Endpoint Manager Client must be installed on the IBM 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 IBM Endpoint Manager Components** (page Chapter 12, “Additional configuration steps,” on page 151). For information about larger installations, see **Deployment Scenarios** (page Chapter 2, “Sample deployment scenarios,” on page 5).

The IBM Endpoint Manager Server requirements and performance can also be affected by other factors in addition to the number of Clients. These factors 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 to have more than 30 operators, you might want to have a more powerful Server to support the additional load.

### **Relays**

Use 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.

**Note:** To improve performance, you can connect from 500 to 1000 Clients to each Relay and use a parent child relay configuration.

### **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 IBM Endpoint Manager support site.



---

## Chapter 4. Types of installation

Before you install the product, decide if you want to do an evaluation or production installation.

If you choose evaluation installation, you install a trial Endpoint Manager Server for a period of 30 days and you do not need to buy a license.

If you choose production installation you must purchase a license. When you receive your IBM Endpoint Manager license authorization file, you are ready to create a personalized **action site masthead** that, in turn, allows you to install and use IBM 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 and is linked to the hostname or IP address of the server machine.

---

### Evaluation installation

If you choose evaluation installation, you install a trial Endpoint Manager Server for a period of 30 days and you do not need to buy any license files from IBM.

During this type of installation, a request is automatically submitted for an Evaluation License and the installation completes using it. The evaluation installation requires that the Linux system where you are running the installation has internet connection (either direct or through a proxy).

This installation uses predefined values for all the configuration parameters. The only parameters that you can configure are:

- Server Identification Port Number (default: is 52311)
- Web Reports Server Port (default is: 80)

After an Evaluation installation, a user named EvaluationUser is created to log on both the IBM Endpoint Manager console and IBM Endpoint Manager WebReports.

During this type of installation, a request is automatically submitted for an Evaluation License and the installation completes using it. Ensure that the system where you are running the installation has internet connection, either direct or through a proxy.

This installation uses predefined values for all the configuration parameters. The only parameters that you can configure are:

- Server Identification Port Number. The default value: is 52311
- Web Reports Server Port. The default value is 80.

After an Evaluation installation, a user named EvaluationUser is created to log on both the IBM Endpoint Manager console and IBM Endpoint Manager Web Reports.

---

## Production installation

To install a production copy of IBM Endpoint Manager, you must first purchase a license from IBM or from an authorized reseller.

During the installation you can choose different types of setup depending on the license input file you have:

I want to install with a **BES license authorization file**  
I want to install with a **Production license** that I already have  
I want to install with an existing **masthead**

### BES license authorization file

After you purchase a license from IBM you receive an IBM Endpoint Manager license authorization file. You must use this file the first time you run a production installation. If you have not yet purchased a license, contact [sales@bigfix.com](mailto:sales@bigfix.com) or visit the IBM Endpoint Manager website at <http://www-01.ibm.com/software/tivoli/solutions/endpoint>.

The sales agent will want to know how many clients you intend to install. Based on this, the agent creates, signs, and emails you a **License Authorization** file, which will have a name like `CompanyName.BESLicenseAuthorization`.

If you run this installation and do not have access to the Internet, a temporary request (`beslicense.request`) is generated to request a production license (`license.crt`) from the IBM Endpoint Manager License Server and a `license.pvk` private key file. You can leave the installation in pending status until you receive the production license.

Copy the request named `request.BESLicenseRequest` on to a machine with access to Internet, visit the IBM Endpoint Manager website, post your request, and download your certificate. After you downloaded the certificate, copy it to the machine on which you are installing the server and continue the installation. If you exited the installation, to install the server you must run the installation using the option that requires an existing **Production license** file.

**Note:** The DNS/IP address that you choose becomes a permanent part of your deployment and must never change. For flexibility, it is strongly recommended that you use a DNS name instead of a static IP address. The installation program collects further information about your deployment and then creates the digital signature key `license.pvk` and a file called the action site masthead. This file combines configuration information (IP addresses, ports, and so on.) and license information (how many Clients are authorized and for how long) together with a public key that is used to verify the digital signatures.

### Production license

Use this option if you have already the production license `license.crt` and the private key file on the machine on which you are installing the server, but did not complete the server installation.

### An existing masthead

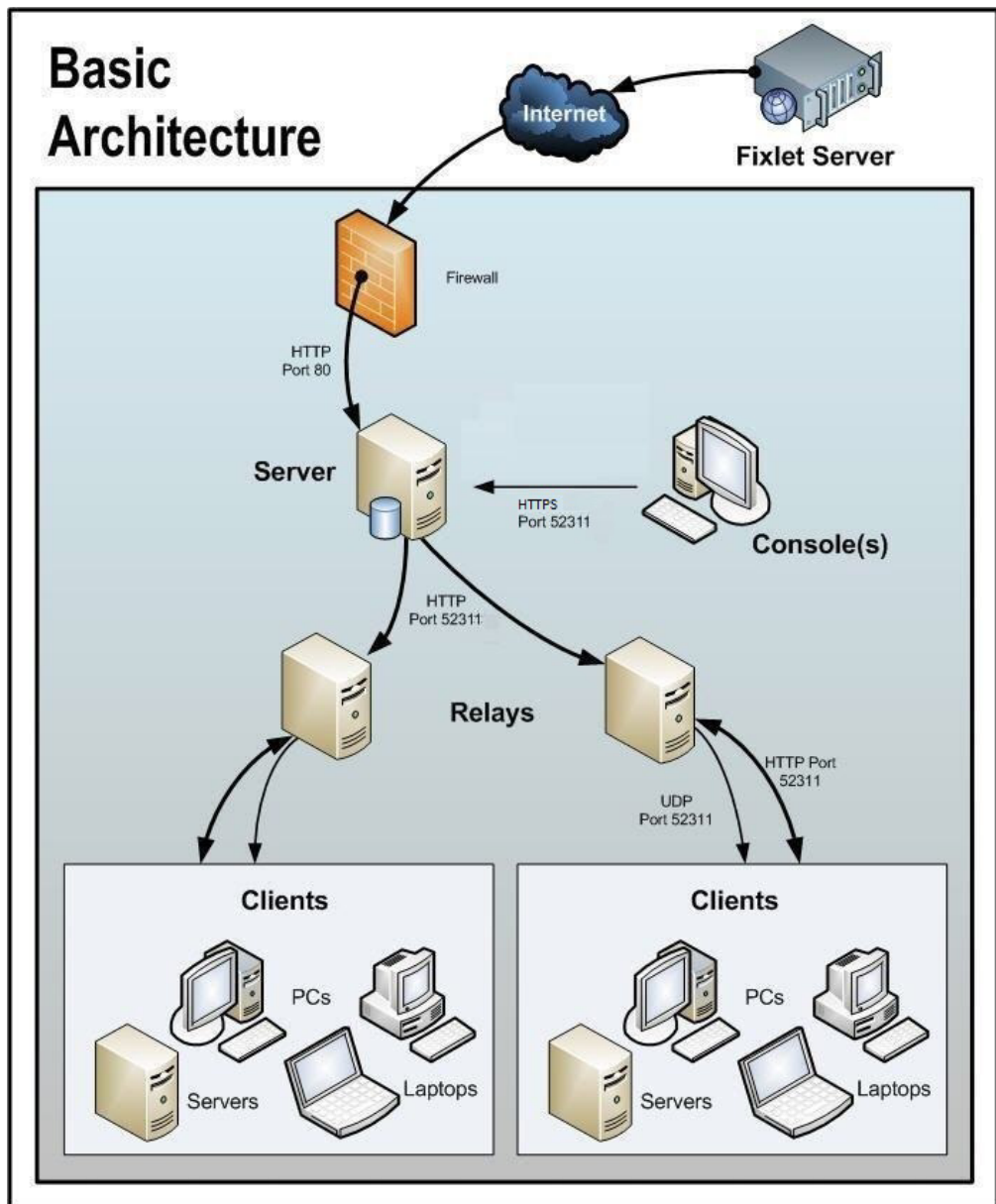
Use this type of installation to reinstall the Endpoint Manager server or a DSA server. The input file needed to run this installation is the action site masthead file that was generated during the first installation. The action site masthead has the extension `.afxm` and acts as a configuration file with parameters such as Endpoint Manager server IP address or server name,

port number, and locking behavior. It contains information necessary for the digital signature security scheme that Endpoint Manager uses (the masthead contains the public key information), and the licensing information that allows Endpoint Manager users to run Endpoint Manager with a specified number of users for a specified length of time. The Endpoint Manager Server installer requires the masthead file be in the server installation folder.

After the production installation a user (default name is IEMAdmin) is created to logon to the IBM Endpoint Manager Console and IBM Endpoint Manager WebReports

## **A basic installation**

A simplified IBM Endpoint Manager deployment is shown in the following diagram. 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 IBM 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 IBM Endpoint Manager console operator can then target actions to the appropriate computers to fix vulnerabilities, apply configuration policies, deploy software, and so on. 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 IBM Endpoint Manager, so that 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 IBM Endpoint Manager to work correctly. View the article about network traffic at the IBM Endpoint Manager support site, or ask your support technician for more details.

## A typical installation

Although the basic installation described above shows many of the specific ports needed to establish the IBM 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

IBM 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 IBM 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 IBM 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 fallback 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 IBM 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:

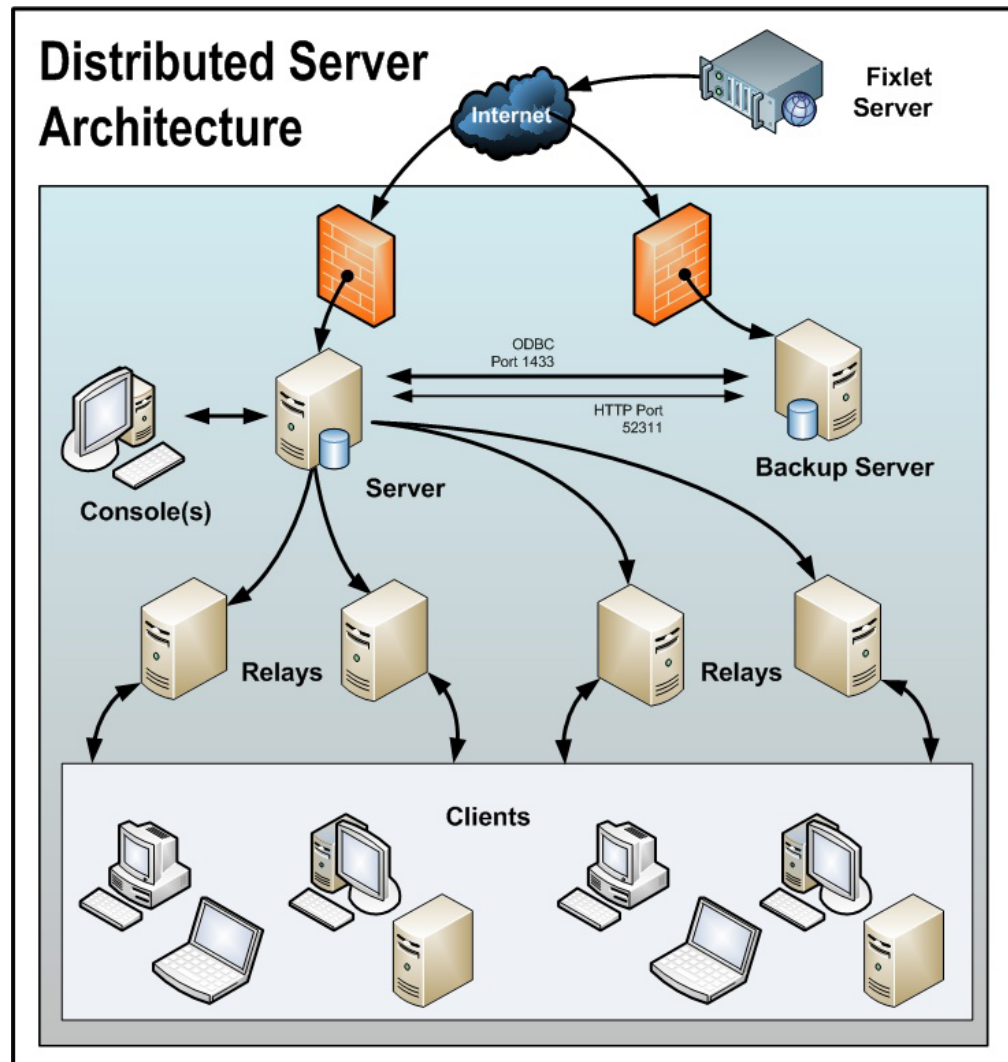
- Servers communicate on a regular schedule to replicate their data. You review the current status and adjust the replication interval through **IBM Endpoint Manager Administration Tool > Replication**.
- When each server is ready to replicate from the other servers in the deployment, it calculates the 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 that 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 **IBM 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 “Managing Replication (DSA) on Windows systems” on page 122).

#### **Distributed Server Architecture (DSA):**

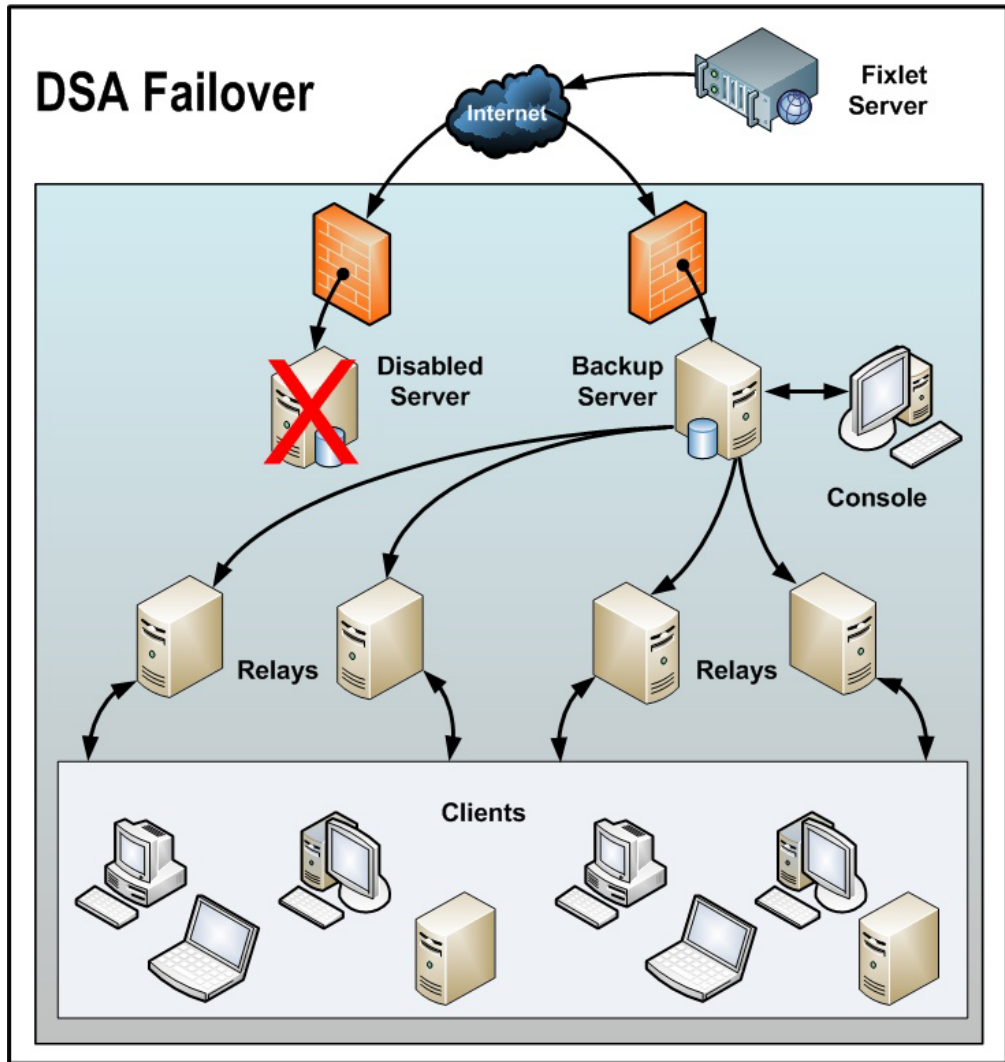
The following diagram shows a typical DSA setup with two servers. Each Server is behind a firewall, possibly in a separate office, although it is easy to set up multiple servers in a single office as well. The servers must have high-speed connections to replicate the IBM Endpoint Manager data (generally LAN speeds from 10 to 100Mbps are required). The IBM 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 (automatic 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.







---

## Chapter 5. Before installing

Before running the installation make sure that you read the following topics and run the requested activities if needed.

---

### Managing licenses

You must obtain a license key before you can install and use IBM Endpoint Manager. Your license is composed of two files:

- Your public key file: `license.crt`
- Your private key file: `license.pvk` protected by a password

The following table lists the tasks that are required to purchase, generate, and manage your license keys.

Task	Description
Check the product license requirements	It is important to understand the license requirements of the system you want to protect. A license lets you install the Endpoint Manager client on a specified number of computers.
Purchase a license	<p>You must purchase a license in the following situations:</p> <ul style="list-style-type: none"><li>• You want to purchase Endpoint Manager.</li><li>• Your trialware license expired.</li><li>• Your paid license expired.</li><li>• Your license is over-deployed and an updated <code>license.crt</code> is required for the increased license count purchase.</li><li>• Your upgrade license expired.</li></ul> <p>Within a few hours of your purchase you receive two emails. One email is sent from IBM as confirmation of your purchase. Another email contains instructions about how to access the IBM Endpoint Manager License Key Center. These emails are sent to the technical contact associated with the IBM Customer Number for the account.</p>
Get the license authorization file	To get your product license you must have an authorization file from the IBM Endpoint Manager License Key Center site. See “Creating the License Authorization File” on page 32.

<p>Generate your license files during installation:</p> <ul style="list-style-type: none"> <li>• Create the private key file</li> <li>• Request and get the license certificate</li> <li>• Generate the masthead file</li> </ul>	<p>During the installation of the Server, after you specify the license authorization file, you generate the <code>license.pvk</code> file, which is your private key file. You also request and get the <code>license.crt</code> file, which is your public key file. These two files together complete your license.</p> <p>See "Requesting the license files on Windows and Step 2 - Installing the Server".</p>
<p>Back up your license files</p>	<p>Store your <code>license.crt</code> (public key) file with your existing <code>license.pvk</code> (private key) file. Keep these two keys together and create a backup copy in a secure location. Only in this way are you in complete control of your license keys. Backing up your license files preserves the license files in case the database or the computer hard disk is damaged.</p> <p>In particular the <code>license.pvk</code> file is the part of your key files that needs to stay private. The <code>license.crt</code> file is your public key file and must be combined with your private key file to complete your license. You can open the license files in a text editor to review their contents.</p>
<p>Check license status and distribute the new license/masthead file</p>	<p>You can see the notifications about expired license and other license issues for the license that you imported into the console.</p> <p>See "Upgrading the masthead on the clients" on page 34.</p>

This is a summary of the steps to perform to get your license key files:

1. Purchase a license.
2. Get an authorization file from the IBM Endpoint Manager License Key Center site.
3. Start the Endpoint Manager installation and enter the authorization file when requested to get the `license.crt` file. At the end of the process both the public key and private key license files are generated together with the masthead file. This file contains configuration, license, and security information, including URLs that point to where trusted Fixlet content is available. It is used for installing DSA servers and is distributed to all the clients using that server.

## Creating the License Authorization File

To create your license authorization file (`.BESLicenseAuthorization`), containing deployment and licensing information and used during the installation to create your license files, access the IBM Endpoint Manager License Key Center. This site is an online license key delivery and management service that allows you to obtain and manage the license keys you need to use the product.

To create the authorization file perform the following steps:

1. Access the following link: <http://tem.subscribenet.com/>

2. Enter your email address and the password you received together with the instructions about how to access the Tivoli Endpoint Manager License Key Center.

IBM Endpoint Manager License Key Center
IBM

Welcome to the IBM Endpoint Manager License Key Center.

Please use the fields below to login and manage your Endpoint Manager licenses.

If this is your first visit, you should have received your initial login and password on your IBM Endpoint License Key Center welcome email. If you are a prior visitor, but cannot remember your password, please use the "Forgot your password link" below to reset your account.

If you are registering to a new account, please use the "Don't have a password link" below. Your site primary or site technical contact will need to approve your request prior to you gaining access.

**Email address**

**License Key Center Password**

☐ Keep me logged in

[Forgot your password?](#)  
[Don't have a password?](#)  
[Need other assistance?](#)

**Login**

3. For each product specify the allocated client quantity. If you leave 0 you cannot install the related product.

Product	Allocated Quantity	Available Quantity
<b>Core Protection Module (Trend) (*) (Client Device)</b> Order Date: <a href="#">Jul 22, 2011</a> License Expiration: December 30, 2021 Maintenance Expiration: Dec 30, 2021	0	817040
<b>Core Protection Module (Trend) (*) (Client Device)</b> Order Date: <a href="#">Aug 24, 2011</a> License Expiration: December 31, 2037 Maintenance Expiration: Dec 31, 2037	50000	6124989
<b>Lifecycle Management (Client Device)</b> Order Date: <a href="#">Jul 22, 2011</a> License Expiration: December 30, 2023 Maintenance Expiration: Dec 30, 2023	0	776570
<b>Lifecycle Management (Client Device)</b> Order Date: <a href="#">Aug 24, 2011</a> License Expiration: December 31, 2037 Maintenance Expiration: Dec 31, 2037	50000	5520016
<b>Lifecycle Management (Client Device)</b> Order Date: <a href="#">Jan 25, 2012</a> License Expiration: Does not expire. Maintenance Expiration: Jan 25, 2099	0	659385
<b>Lifecycle Management (Client Device)</b> Order Date: <a href="#">Aug 31, 2012</a> License Expiration: Does not expire. Maintenance Expiration: Aug 31, 2013	0	2475
<b>Mobile Device Management (Client Device)</b> Order Date: <a href="#">Mar 29, 2012</a> License Expiration: Does not expire. Maintenance Expiration: Mar 29, 2013	0	8848
<b>Mobile Device Management Beta (Client Device)</b> Order Date: <a href="#">Jan 25, 2012</a> License Expiration: Does not expire. Maintenance Expiration: Jan 25, 2099	0	684057
<b>Other Sites Allowed (Client Device)</b> Order Date: <a href="#">Aug 24, 2011</a>	50000	5373793

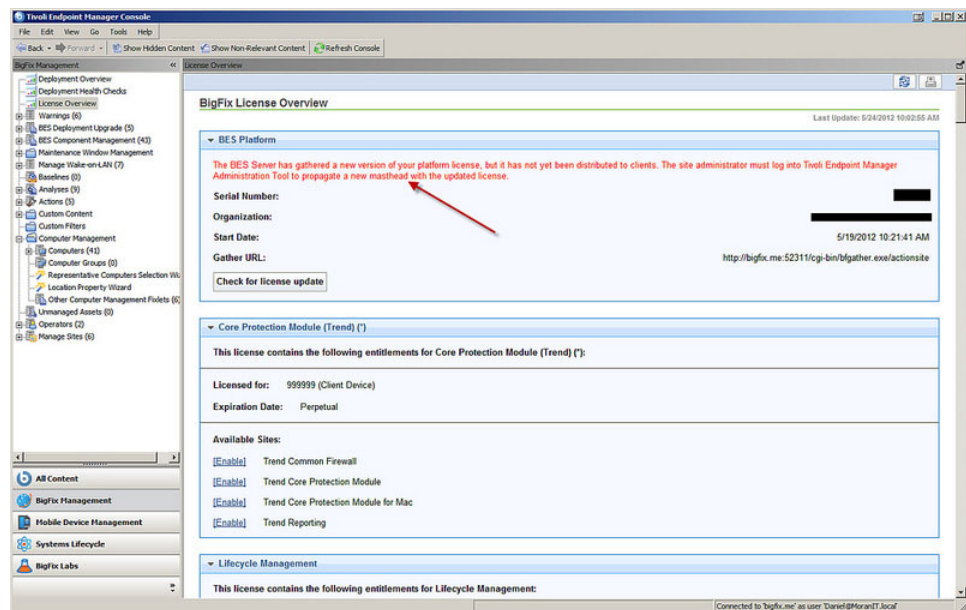
## Licensing Assistance

For specific problems with your license such as license expiration date, entitlement counts, or lost authorization files, contact the IBM Endpoint Manager licensing team at TEM@dk.ibm.com. Support questions not related to licensing, such as general installation problems, setup configuration, deployment questions, should be directed through the normal support and sales resource channels and not sent to this address.

## Upgrading the masthead on the clients

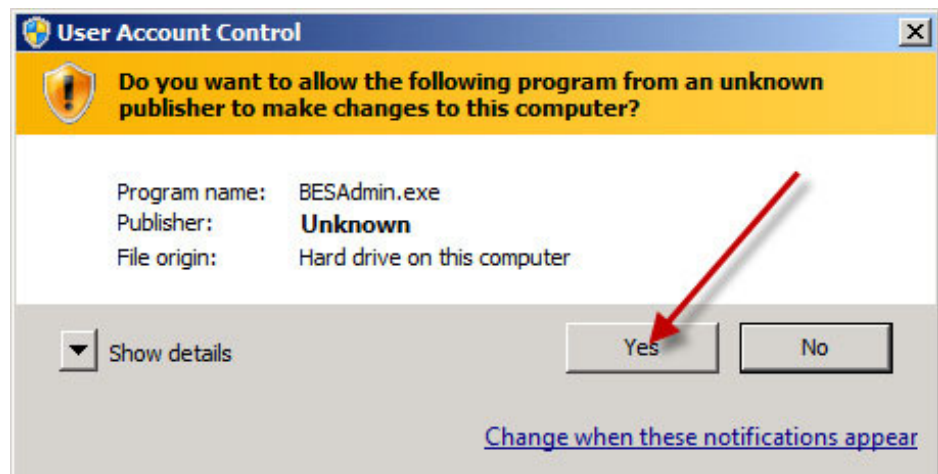
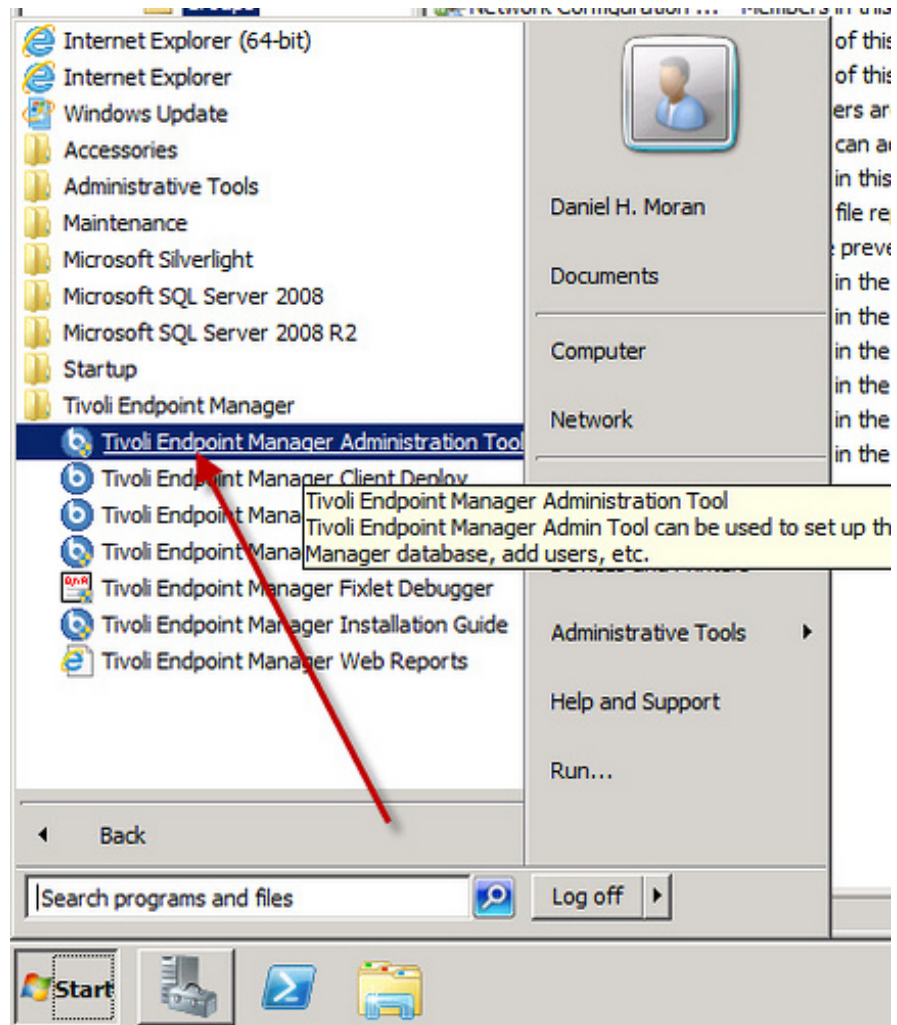
The masthead file is upgraded automatically on IBM Endpoint Manager V8.2 or later. For previous versions, to distribute a new masthead file with an updated license certificate, that extends your license, seat count, or entitlements, perform the following steps:

1. 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 then **Check for license update**. You might receive a notification that Endpoint Manager deployment has gathered an update to your license (a new `license.crt` file):



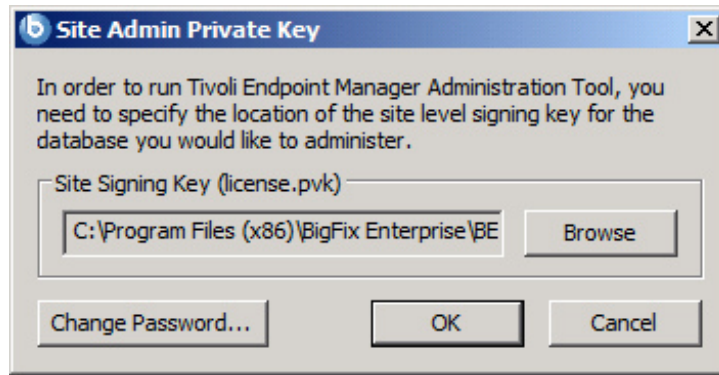
**Note:** To receive an updated license, contact IBM Endpoint Manager Licensing at TEM@dk.ibm.com, your authorized IBM reseller, your IBM sales representative or account manager.

2. After you receive your new `license.crt` file, save it on your server computer and open the Administration Tool by selecting **Start > All Programs > IBM Endpoint Manager > IBM Endpoint Manager Administration Tool**. After you log in, the installation Admin account distributes the masthead to the clients.



3. Choose your license.pvk file.

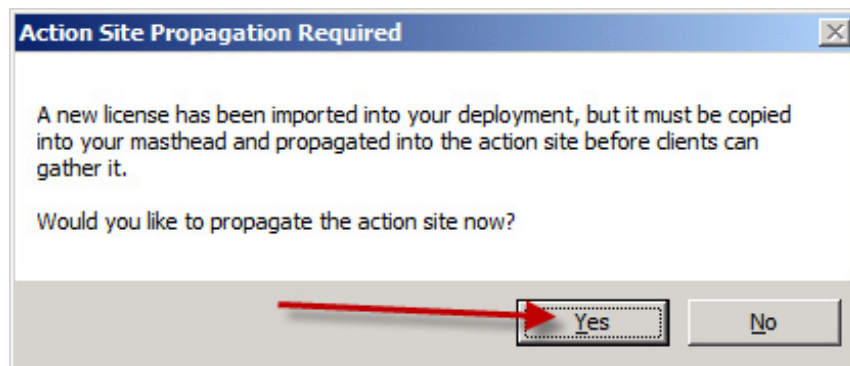




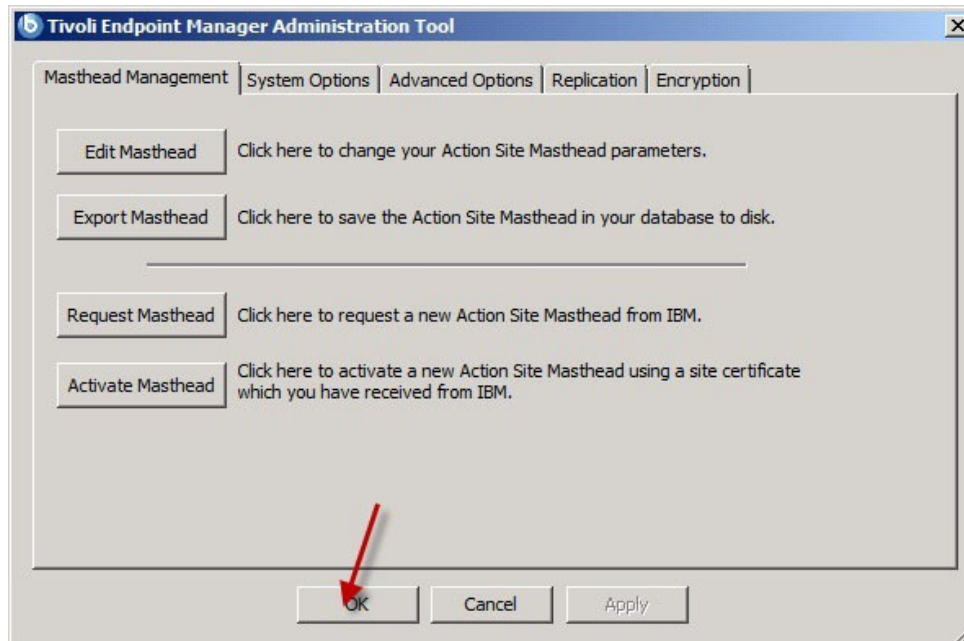
4. Enter your master (site level) password



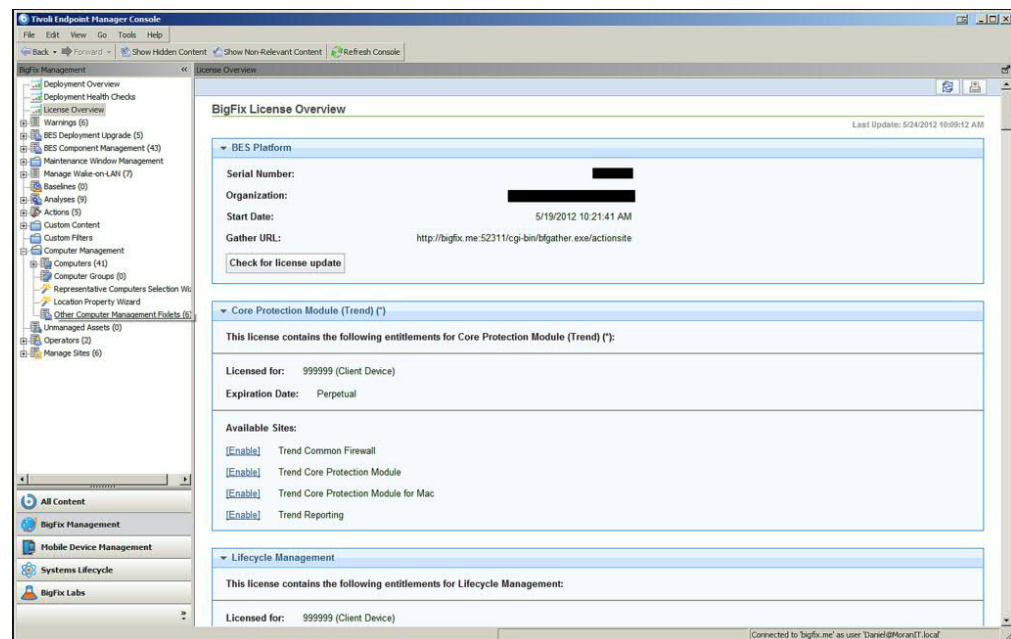
5. After the tool opens, it notifies you that a copy of this file on the clients is required. Click **Yes**.



6. In **Masthead Management**, click **OK**.



As soon as the clients receive the new masthead, they receive the updated license information.



## Modifying port numbers

By default, the server uses port **52311** to communicate with the clients, but you can choose any port number (although you should avoid the reserved ports between 1 to 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*.

Consoles use port **52311** to connect to the server.



---

## Chapter 6. Installing on Windows systems

Now that you understand the terms and the administrative roles, you are ready to get authorized and install the programs.

Because IBM Endpoint Manager is powerful, you might want to limit access to trusted, authorized personnel only. The product 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 by getting a **License Authorization** file, which will have a name like `CompanyName.BESLicenseAuthorization`.

The Installer program collect further information about your deployment and then creates a file called the **action site masthead**. This file establishes a chain of authority from the IBM 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) together with a public key that is used to verify the digital signatures. To create and maintain the digital signature keys and masthead, you use the **IBM Endpoint Manager Installer**, which you can download from IBM.

---

### Installation Steps

To install the product, perform the following steps:

1. Download IBM Endpoint Manager.
2. Request a license and create the masthead using the installer program. When it prompts you for the authorization file, use the License Authorization file (\*.BESLicenseAuthorization) that you created using your License Key Center account or, in the case of a Proof-of-Concept evaluation, that was provided to you by your IBM Technical Sales Representative.
3. Run the IBM Endpoint Manager installation.

#### Step 1 - Downloading IBM Endpoint Manager

Download IBM Endpoint Manager from the IBM Passport Advantage portal.

You can download IBM Endpoint Manager also from the support site at <http://support.bigfix.com/bes/install/downloadbes.html> or from the DeveloperWorks trial site at <http://www.ibm.com/developerworks/downloads/tiv/endpoint/>. The demonstration trial installer is the same installer program as that used for a normal production installation.

To install the server component download the following e-images from Passport Advantage:

Table 1. Parts required for installing Endpoint Manager Server

Software Name	Part Number	Content
IBM Endpoint Manager Platform Install V9.0.0 Multiplatform Multilingual (CIGP2ML)	CIGP2ML	<ul style="list-style-type: none"> <li>DB2_10_limited_CD_Linux_x86-64.tar.gz</li> <li>IBMIM_win32.exe</li> <li>IEM_Pltfm_Install_V90.zip</li> <li>IEM_V90_QS.zip</li> </ul>

To extract the Endpoint Manager Windows server installation files, perform the following steps:

1. Copy the Endpoint Manager Server zip file IEM\_Pltfm\_Install\_V90.zip to your Windows Server.
2. Expand the zip file using the following command:  

```
unzip IEM_Pltfm_Install_V90.zip
```

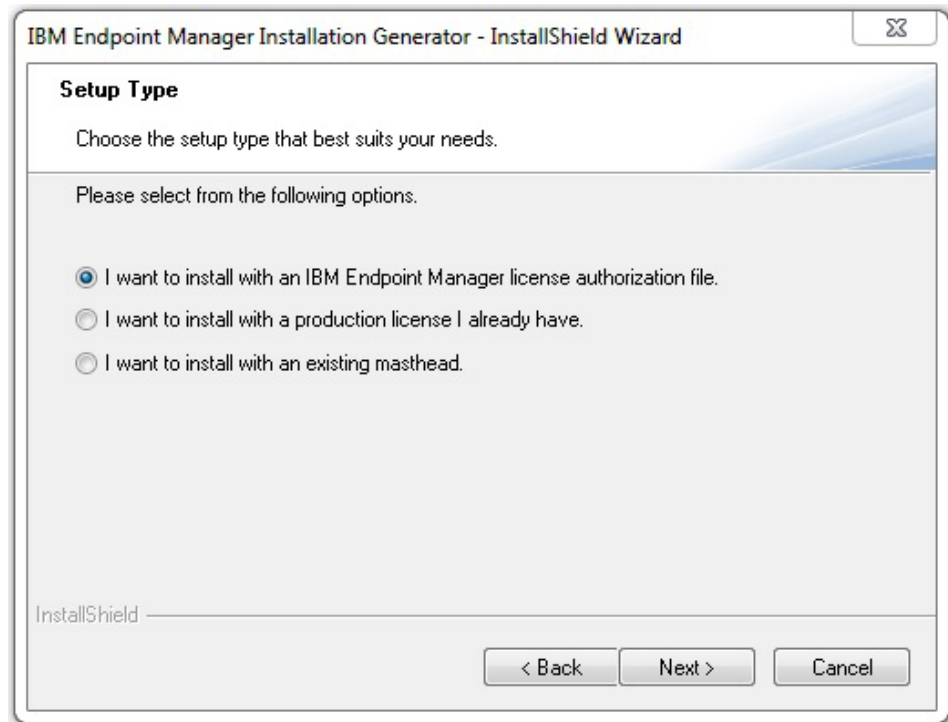
You can find the setup.exe file to install the Windows Server in the IEM\_Pltfm\_Install\_V90 folder.

## Step 2 - Requesting a license certificate and creating the masthead

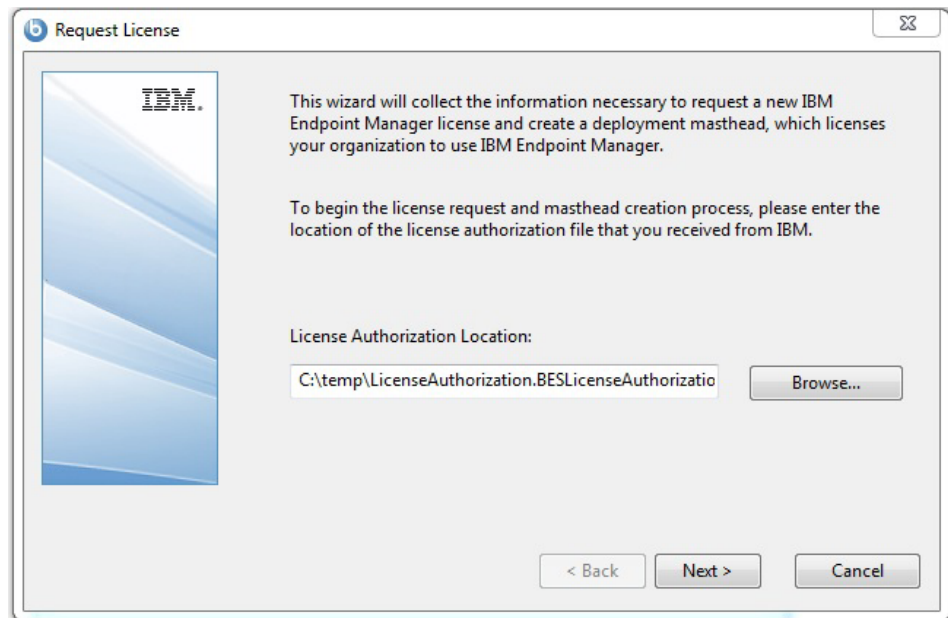
Before you perform the steps below, you must have purchased a license and obtained an IBM Endpoint Manager license authorization file (\*.BESLicenseAuthorization) using your License Key Center account or, in the case of a Proof-of-Concept evaluation, that was provided to you by your IBM Technical Sales Representative.

When you have your license authorization file, you are ready to request a license certificate and then create a personalized **site masthead** that, in turn, allows you to install and use IBM 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:

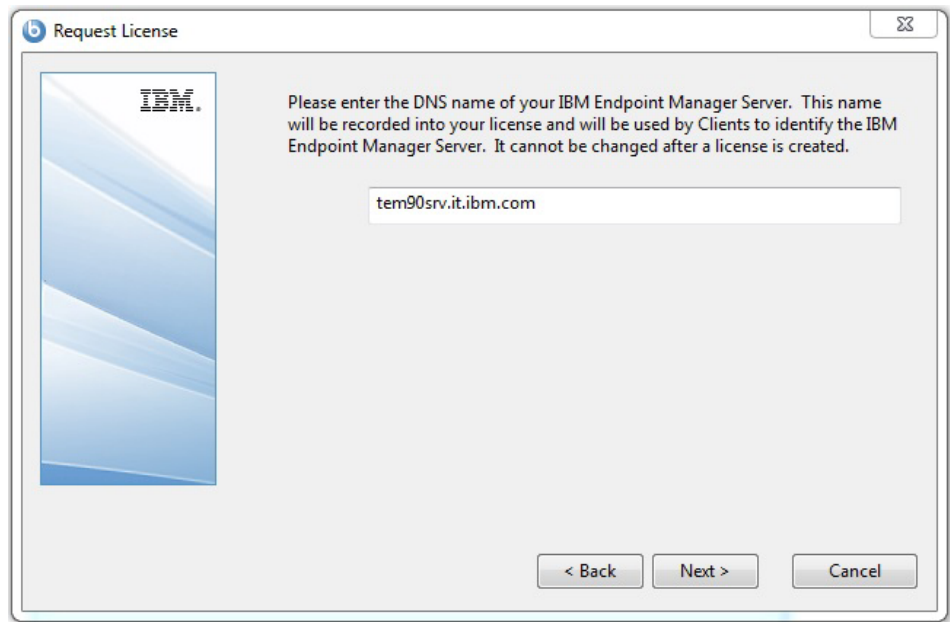
1. Run the IBM Endpoint Manager installer BigFix-BES-n.n.nnnn.n.exe, where *n.n.nnnn.n* is the version of the installer). When prompted, choose **Production** installation and accept the Software License Agreement. On the welcome screen, click **Next**.
2. After reading and accepting the License Agreement, select **I want to install with an IBM Endpoint Manager license authorization file**, to create your Private Key and Masthead.



3. Enter the location of your license authorization file, which has a name like `CompanyName.BESLicenseAuthorization`

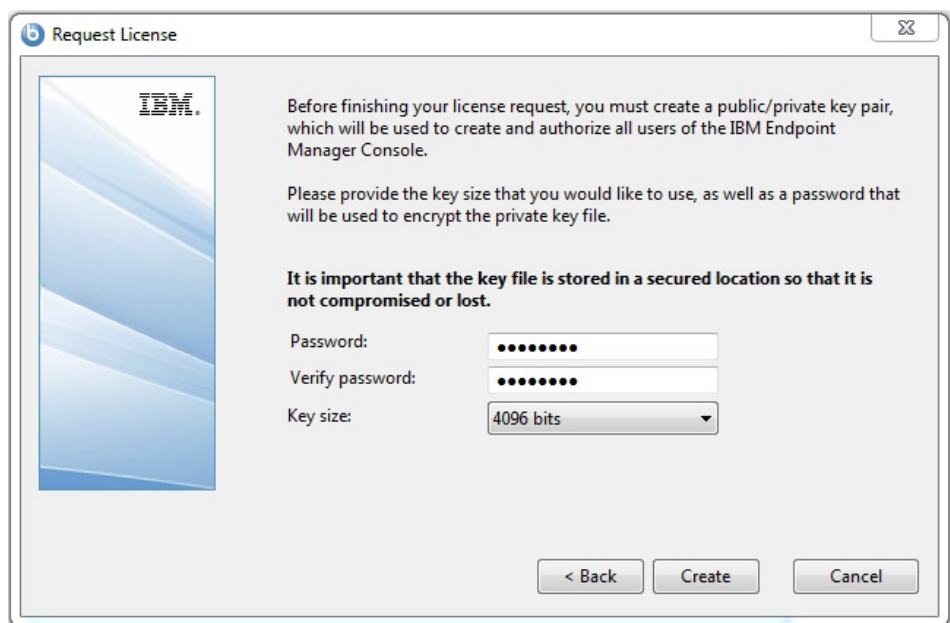


4. Specify a **DNS name** or **IP address** for your Endpoint Manager server and click **Next**.



**Note:** Enter a DNS name, such as `bes.companyname.com`, because of its flexibility when changing server computers and doing advanced network configurations. This name is recorded into your license certificate and is used by clients to identify the Endpoint Manager server. After your license certificate is created, the DNS name cannot be changed. To change the DNS name, you must request a new license certificate, which requires a completely new installation.

5. Type a site credential **password** to allow you to create a site admin key for your deployment. Type your password twice (for verification), and specify a key size (from 2K to 4K bits) for encrypting the private key file. Click **Create**.

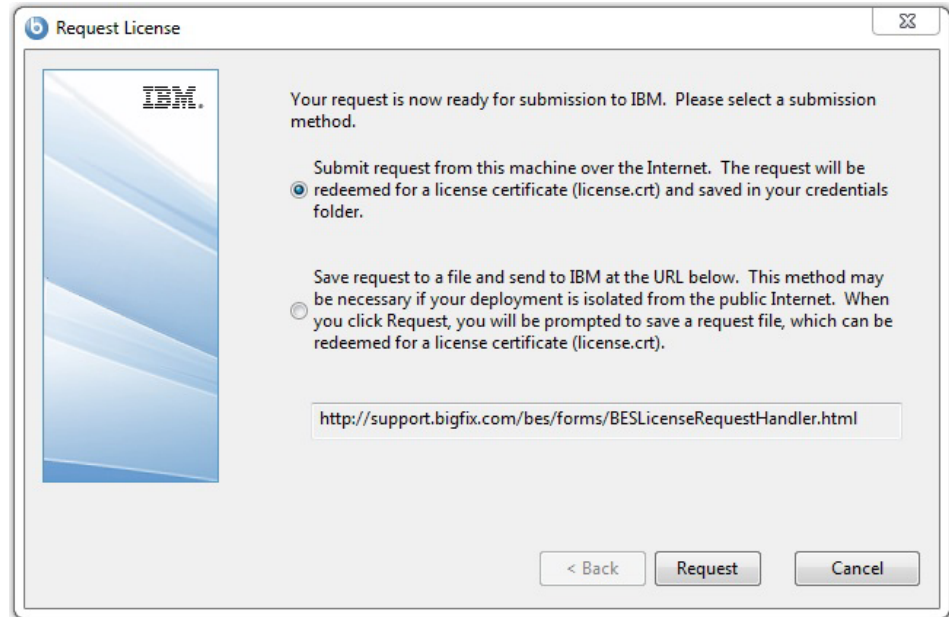


In this way you generate a private/public key pair used to create and authorize all Endpoint Manager users.

6. Save your private key (license.pvk) file from the **Browse for Folder** dialog in a folder with secure permissions or on a removable drive, such as a PGPDisk or a USB drive. Click **OK**.

**Important:** If you lose the private key file, a new license certificate needs to be created, which requires a completely new installation. In addition, anyone with the private key file and password have full control over all computers with IBM Endpoint Manager clients installed so ensure that you keep the private key file and password secured.

7. If you have internet connectivity, choose the option to submit your request over the internet to IBM.

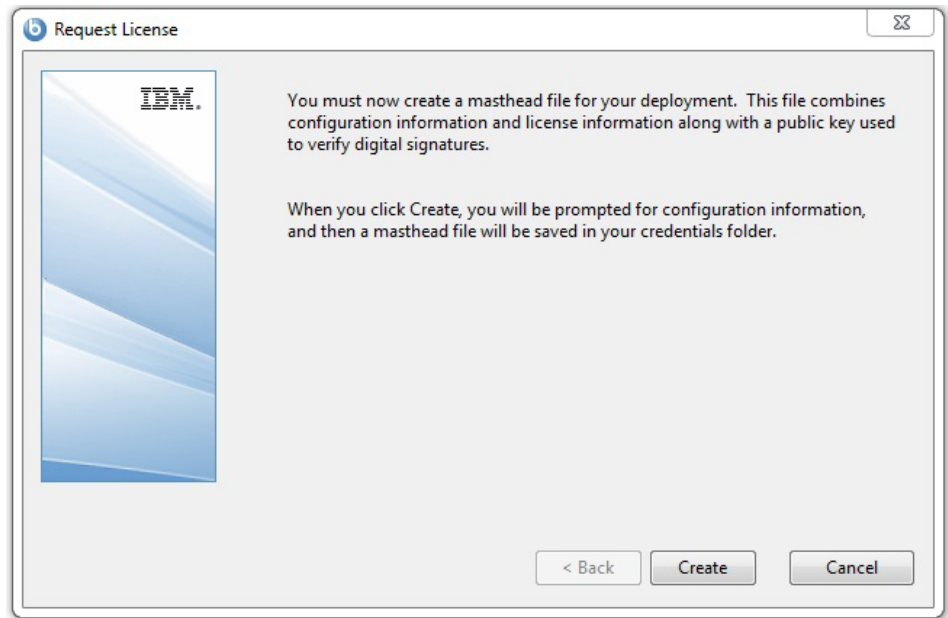


You are prompted for a location to save the resulting license certificate file (license.crt), and a request file is sent to IBM Endpoint Manager for license verification. Typically, you select the first choice, **submit request**, to post the request via the internet. This request consists of your original authorization file, your server DSN name and your public key, all packaged into a single file.

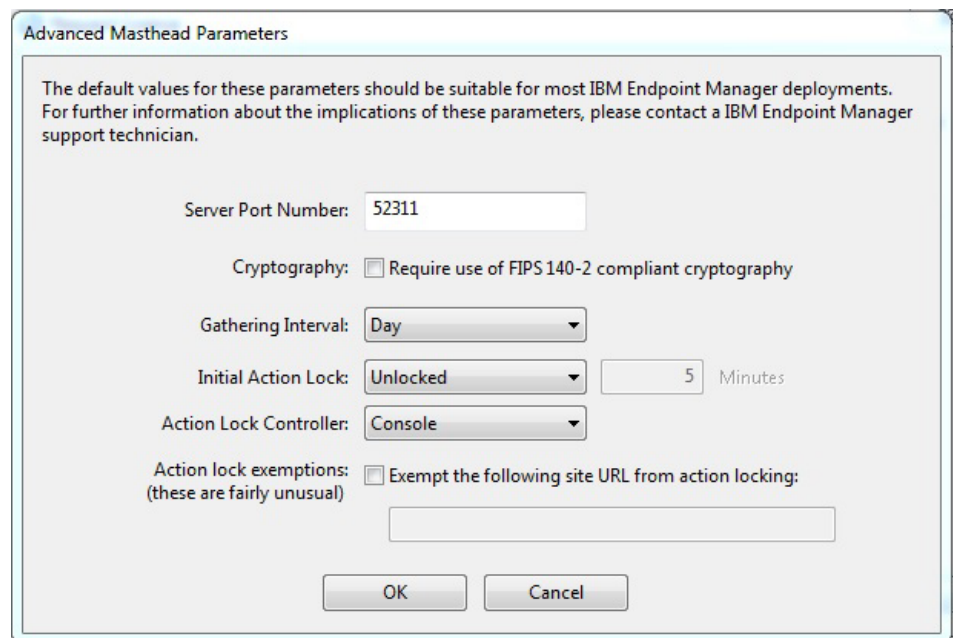
8. Click **Request**. The Wizard retrieves your license certificate (license.crt) from the IBM Endpoint Manager License server.

Alternatively, if you are on an airgap without internet connectivity, choose the option to save the request as a file named request.BESLicenseRequest. Copy the file to a machine with internet connectivity and submit your request to the URL of the Endpoint Manager website shown in the installer. The page provides you with a license.crt file. Copy the file back to the installation computer and import it into the installer.

9. From the **Request License** dialog, click **Create** to create the masthead file



10. Enter the parameters of the masthead file that contains configuration and license information together with a public key that is used to verify digital signatures. This file is saved in your credential folder.



You can set the following options:

#### Server Port Number:

In general, you do not need to change this number. 52311 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 can use a reserved port number (ports 1-1024), but this might reduce the ability to monitor or restrict traffic correctly and it prevents you from using port numbers for specific applications. If you do decide to change this number



after deploying the clients, IBM Endpoint Manager will not work correctly. For additional information, see *Modifying port numbers* in the next section.

**Note:** Do not use port number 52314 for the network communication between the Endpoint Manager components because it is reserved for proxy agents.

**Cryptography:**

Check this box to implement the Federal Information Processing Standard 140-2 in your network. This changes the masthead so that every IBM 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 a few 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 servers perspective, a smaller interval becomes necessary to get a timely response from the clients. Higher gathering rates only slightly affect the performance of the server, because only the differences are gathered; a client does not gather information that it already has.

**Initial Action Lock:**

You can specify the initial lock state of all clients, if you want to lock a client automatically after installation. 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 want 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 clients 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.

**Exempt the following site URL from action locking:**

In rare cases, you might need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL.

**Note:** You can specify only one site URL and it must begin with `http://`.

Click **OK** when you are finished.

11. Choose the folder in which to install the IBM Endpoint Manager component installers. The IBM Endpoint Manager Installation Guide wizard is launched to lead you through the installation of the IBM Endpoint Manager components.

**Note:** This step creates the installers for the IBM Endpoint Manager client, IBM Endpoint Manager console, and IBM Endpoint Manager server, but does not install the components.

**Note:** The private key (license.pvk) authorizes the creation and rotation of server signing keys, which are trusted by all agents. This key is *not* sent to IBM during the license certificate creation process, and must be carefully protected. To reinstall the server on your workstation, you must reuse the stored IBM Endpoint Manager credentials. If you did not save them, when you reinstall the server you must regenerate them.

## Step 3 - Installing the components

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 **IBM Endpoint Manager Installation Guide**.

When the components have been saved, the **IBM 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 IBM Endpoint Manager (server, console, and client), follow these steps:

1. If it is not already running, launch the Installation Guide (**Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Installation Guide**).
2. A dialog box opens, prompting you to select a component to install. Click the links on the left, in order from top to bottom, to install the IBM Endpoint Manager components. You can also Browse Install Folders. The component installers includes:
  - Install Server
  - Install Console
  - Install Clients
  -
3. The IBM Endpoint Manager server, console, and clients all have their own installers. Follow the instructions for each, as described in the following sections.

### Installing the Windows primary server

The IBM 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 “Server requirements” on page 18). Also, you can consult the knowledge-base article about server requirements at the IBM Endpoint Manager

**Important:** Ensure that the user that logs in to install the IBM Endpoint Manager server has the sa rights for the MSSQL Server to create the database and its tables.

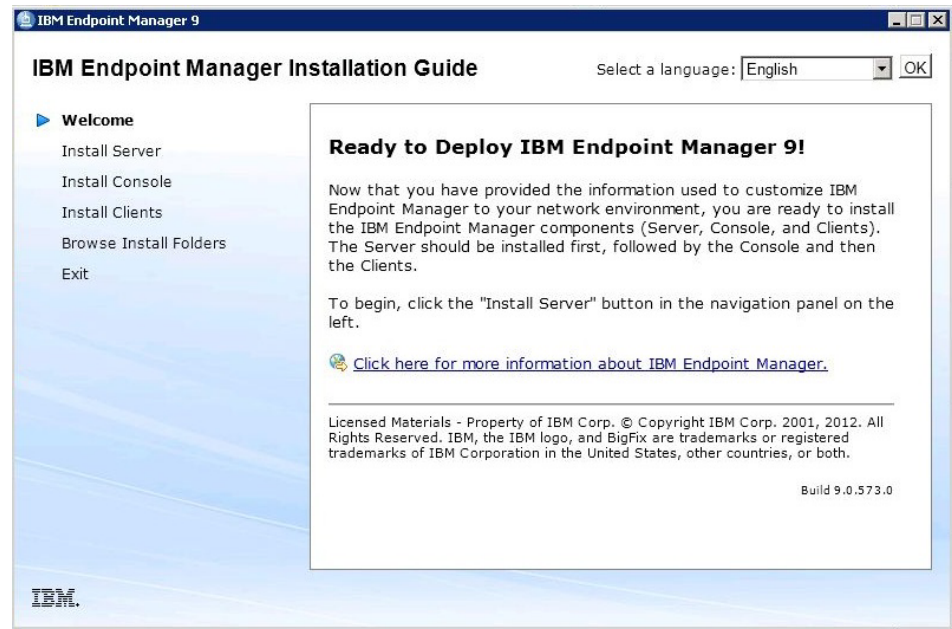
The default installation paths for the IBM Endpoint Manager components are:

- C:\Program Files\BigFix Enterprise\BES Server on 32-bit Windows systems
- C:\Program Files (x86)\BigFix Enterprise\BES Server on 64-bit Windows systems

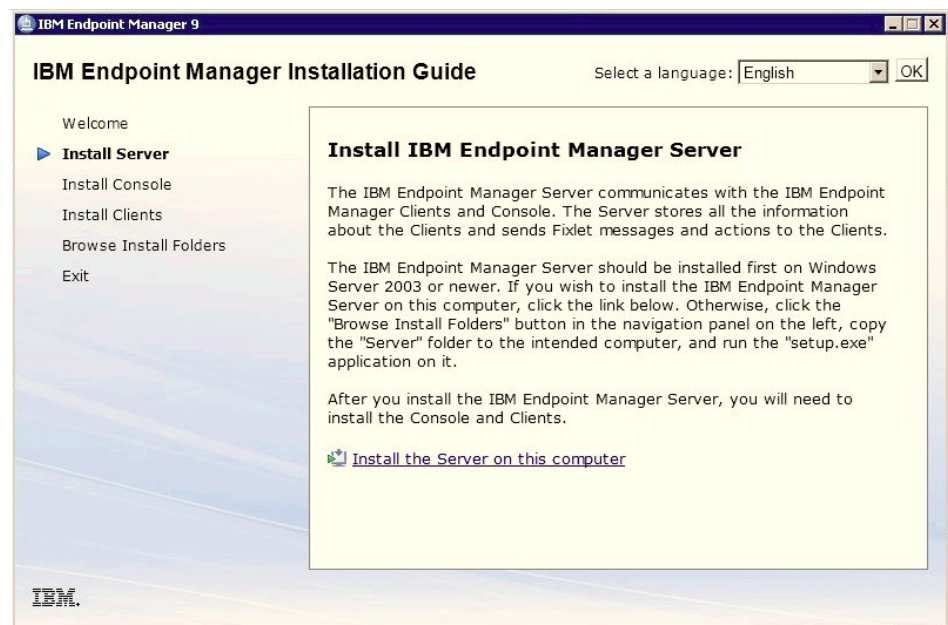


To install the server, follow these steps:

1. If you have not already done so, run the Installation Guide (**Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Installation Guide**). A new panel opens.



2. Click **Install Server**:



The IBM Endpoint Manager Server Install Wizard presents a welcome panel. Click **Install the Server on this computer** to install the server locally. To install the server on a different computer, click **Browse Install Folders** to open the IBM Endpoint Manager Installers folder and displays the Server folder. After you have copied the Server folder to the target computer, double-click setup.exe from that folder to launch the installer.

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

4. The installer prompts you for a destination for 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 chosen the destination, click **Next**.
5. A dialog displays a list of the Server components about to be installed. In general, accept the default components and click **Next**.
6. 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.
7. A dialog prompts you to select a **Local** or **Remote** database. If you want to use another computer to host the IBM Endpoint Manager Database, it must have a SQL Server already installed. The most common choice is to use the local database. If you are installing IBM Endpoint Manager with a remote database, see “Server installation with remote database” on page 49.
8. If you select **Local**, you are prompted for a destination for the database server component. The default location is **C:\Program Files\Microsoft SQL Server**.
9. 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 IBM Endpoint Manager port or errors will occur. Do not use port number 52314 for the network communication between the Endpoint Manager components because it is reserved for proxy agents.

10. 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.
11. The Server installer opens 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.
12. The program prompts you to locate your **license.pvk** file. Accept the default path (if specified) or click the **Browse** button to find a different location. Enter your password to initialize the database and click **OK** to continue.
13. 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).
14. Enter your password to initialize the database.
15. Enter your initial username and password for the console. This is the account used to log in to the console the first time. It is a fully privileged master operator account.
16. The IBM 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 IBM 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 tool, see **Running the IBM Endpoint Manager Diagnostics Tool**.

## Server installation with remote database:

Before installing an IBM Endpoint Manager server with a remote database, ensure that:

- You install the IBM Endpoint Manager Server as a user with SA privileges.
- The SQL Server Browser is running.
- The SQL Server Authentication is enabled.

*Creating a new database user:*

After creating a database instance on the machine where the Microsoft SQL Server is installed, if you do not want to use the SA user for the database connection, you must create a new user with SA Privileges.

To create a new user for a specific database instance, for example TEM81, perform the following steps:

1. Start the Microsoft SQL Server Management Studio.
2. In the Connect to Server panel, specify the following parameters:

### Server Type

Database Engine

### Server Name

<DB\_HOSTNAME>\<INSTANCE\_NAME> If the server hostname is NC118103 and the instance name is TEM81 the server name is: NC118103\TEM81.

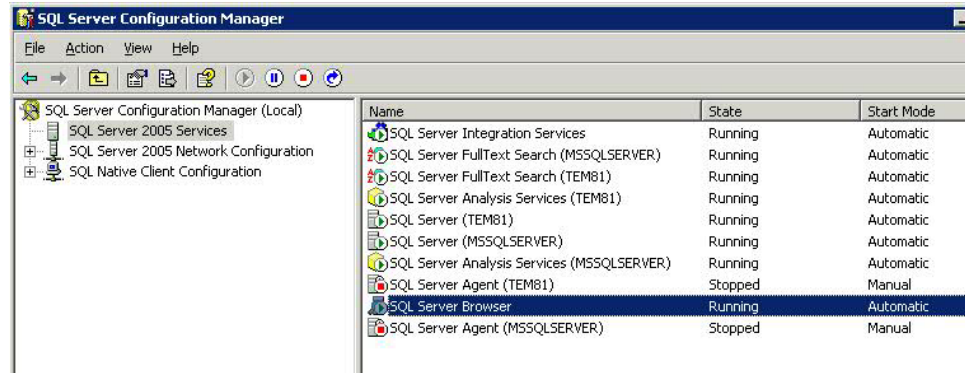


3. From the portfolio, select **Security -> Login -> New Login**.
4. In the **General** tab, specify the User Name and the credential for SQL Server Authentication.
5. In the **Server Roles** tab, select **sysadmin** and click **OK**.

### *Starting the SQL Server Browser:*

On the computer where the Microsoft SQL Server is installed, ensure that the SQL Server Browser is running by performing the following steps:

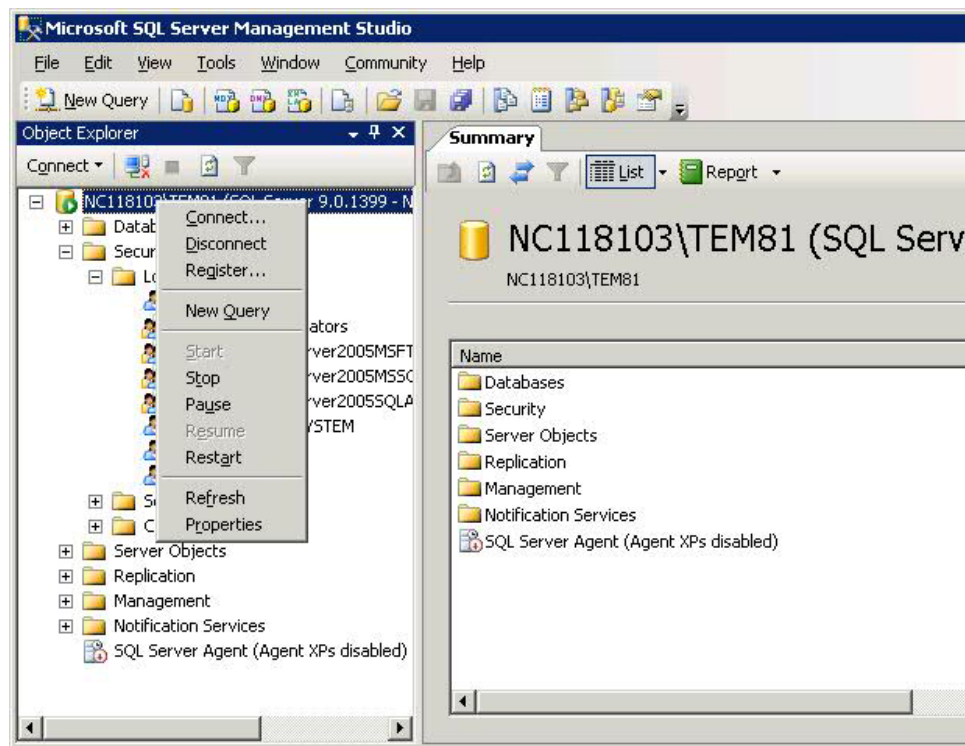
1. Start the **SQL Server Configuration Manager**.
2. Select **SQL Server 2005 Services** and start the SQL Server Browser if it is not running:



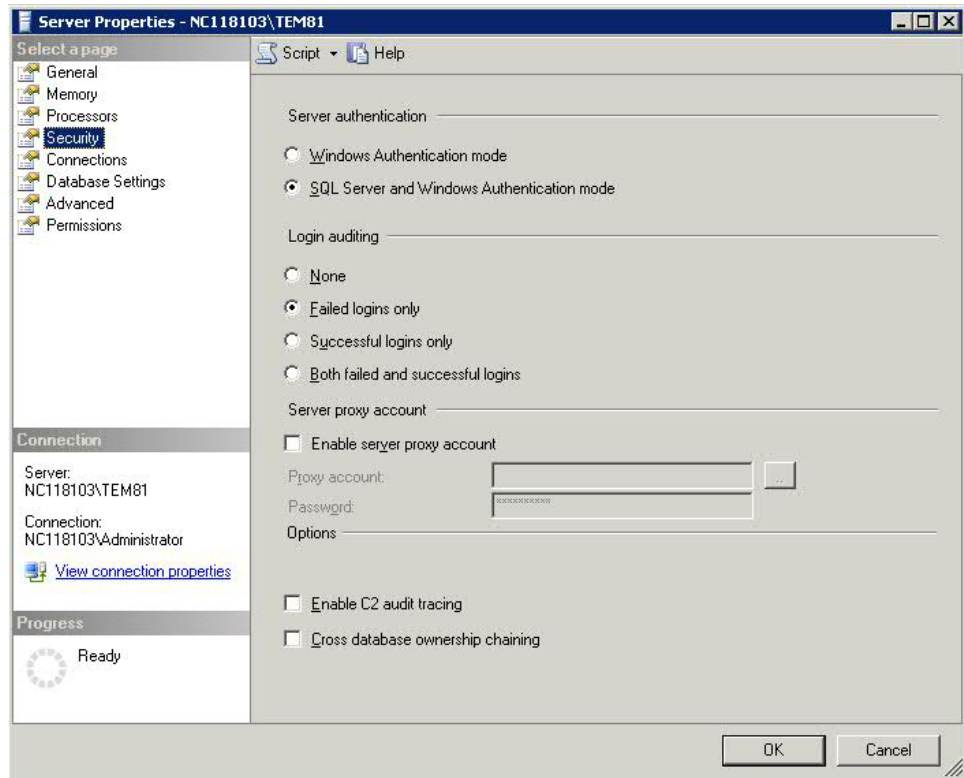
### *Enabling the SQL Server Authentication Mode:*

On the computer where the Microsoft SQL Server is installed, ensure that the SQL Server Authentication Mode is enabled by performing the following steps:

1. Start the Microsoft SQL Server Management Studio.
2. Select the database instance
3. Select **Properties > Security**.



4. Verify that **SQL Server and Windows Authentication mode** is selected.

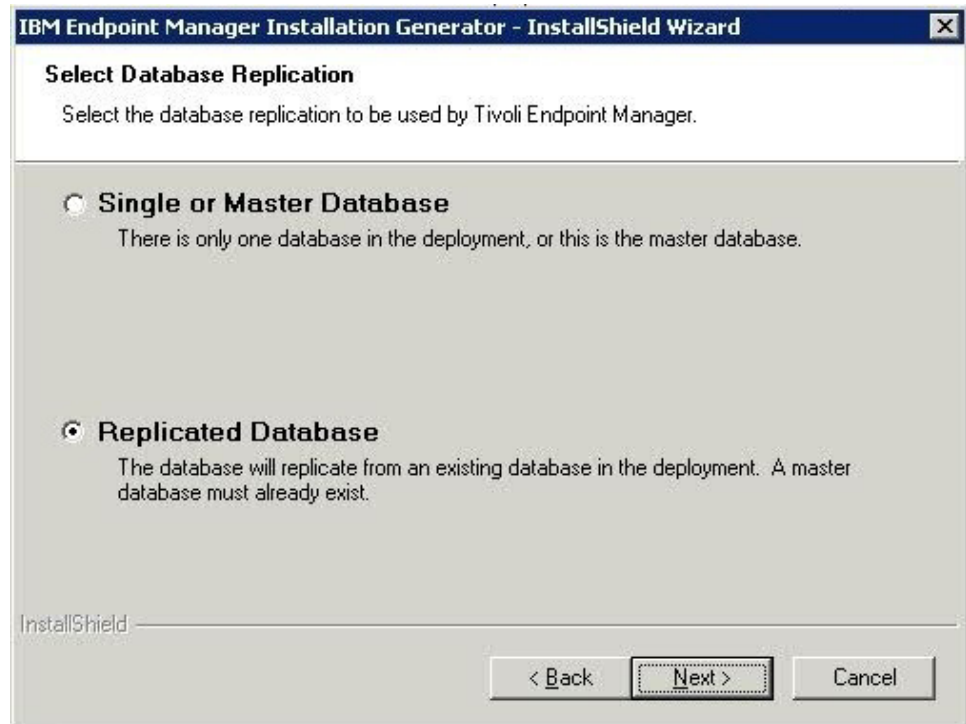


*Installing a server with remote database SQL authentication:*

To install an IBM Endpoint Manager server with a remote database, perform the following steps:

1. On the computer where you want to install the IBM Endpoint Manager server, run the installation.
2. During the server installation, select **Single or Master Database** as database replication.

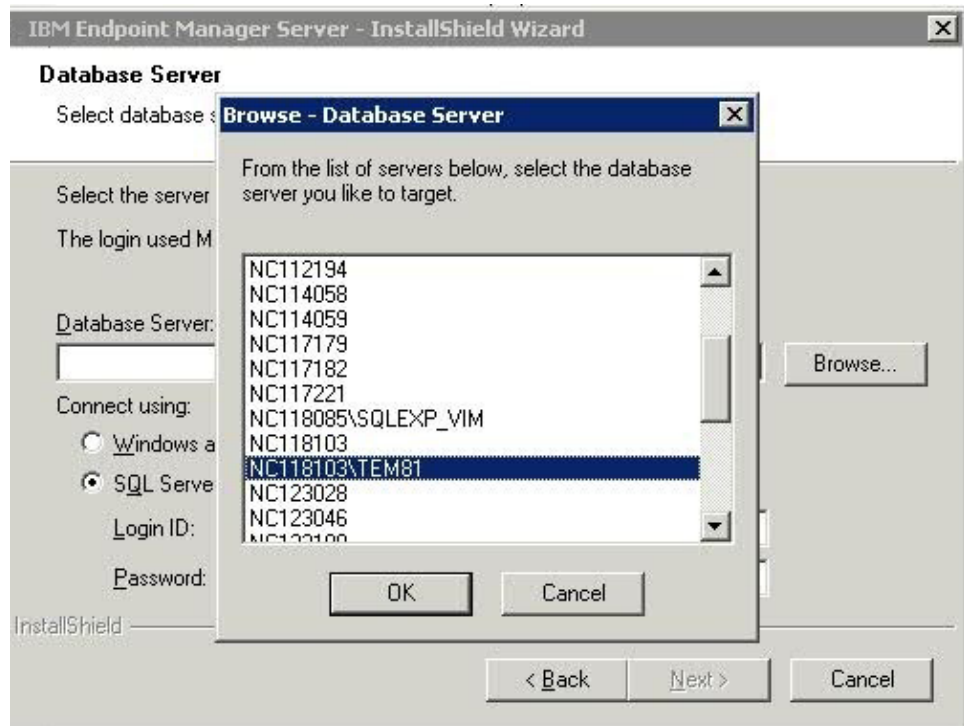




3. Select **Use Remote Database** as the type of database.



4. In the next window, click **Browse** and select the database server instance you want to use:



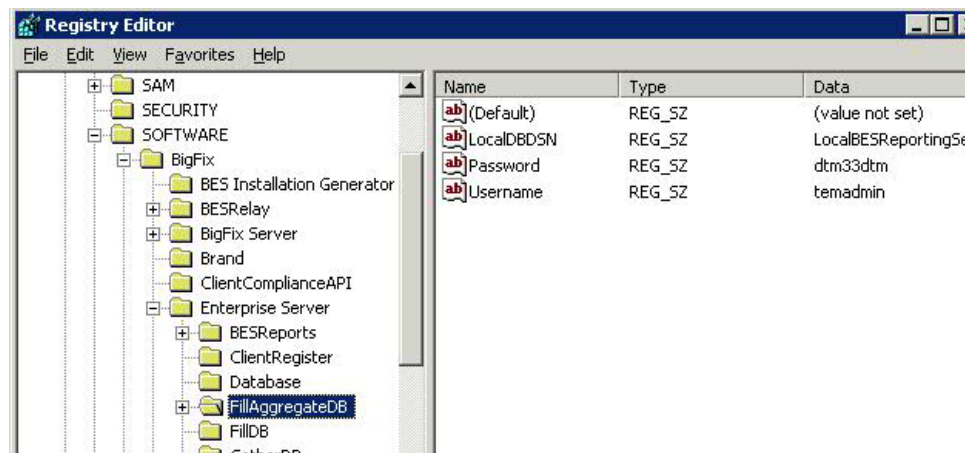
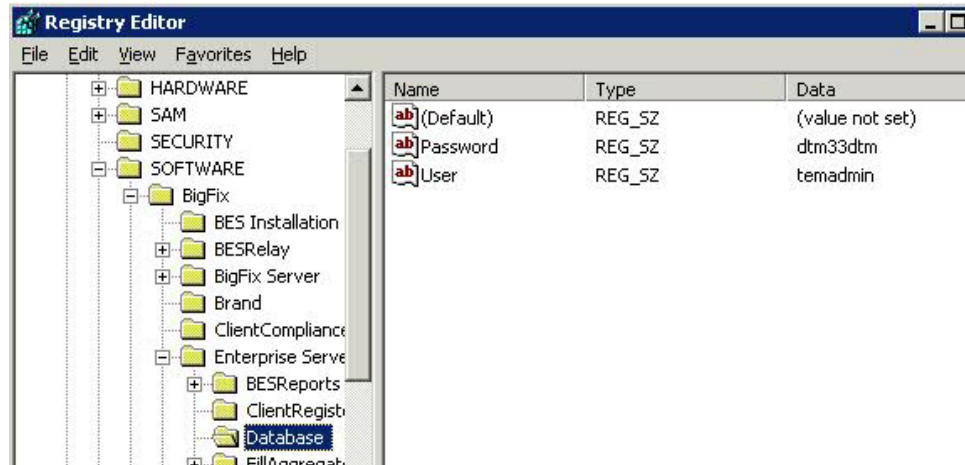
5. Click **SQL Server Authentication using the login ID and password below** and provide the credentials of the user with SA privileges.

**Note:** These credentials are stored in clear text in the Windows registry.



The database is created on the remote machine where the Microsoft SQL Server is installed. On the machine where the IBM Endpoint Manager Server is installed, the registry is updated with the database authentication credentials:





## Authenticating Additional Servers

Multiple servers can provide a higher level of service for your IBM 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.

You must first 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 method, each server uses the specified domain user or a member of the specified user group to access all the 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 in step 2, and restart the service.

#### Using NT Authentication with domain computer groups:

With this method, 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 your chosen servers. 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 method, 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. Choose 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: (on 64-bit systems, the key is HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB:  
 ReplicationUser = <login name>  
 ReplicationPassword = <password>
4. Restart the FillDB service.

**Note:** choose your authentication method on a deployment-wide basis; you cannot mix domain-authenticated servers with SQL-authenticated servers. Also, all IBM Endpoint Manager Servers in your deployment must be running the same version of SQL Server.

## Installing Additional Windows Servers

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

For each additional server that you want to add to your deployment, make sure it can communicate with the other servers, 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 installation to ensure 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 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. The Replication servers window shows you the server configuration for your current deployment. By default, your newly-installed server is configured to replicate directly from the master server every 5 minutes. You can adjust this as necessary. 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.
7. 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.
8. 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.
9. For SQL Authentication, add the following string values to the FillDB registry keys, and restart the FillDB Service.HKLM\Software\BigFix\Enterprise Server\FillDB (on 64-bit systems the key is: HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB:  
ReplicationUser = <login name>  
ReplicationPassword = <password>
10. On the newly-installed server, run the **IBM 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.

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

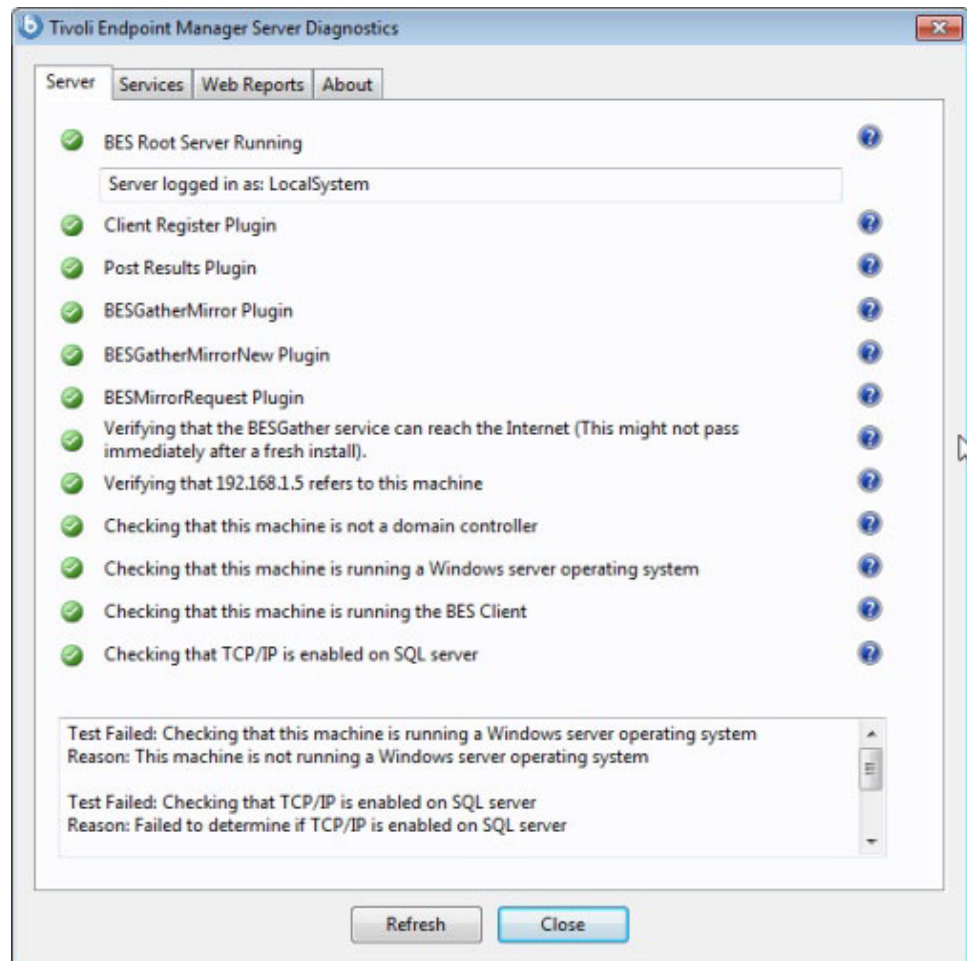
## Running the IBM Endpoint Manager Diagnostics tool

The IBM Endpoint Manager Diagnostics tool verifies that the server components are working correctly. 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.

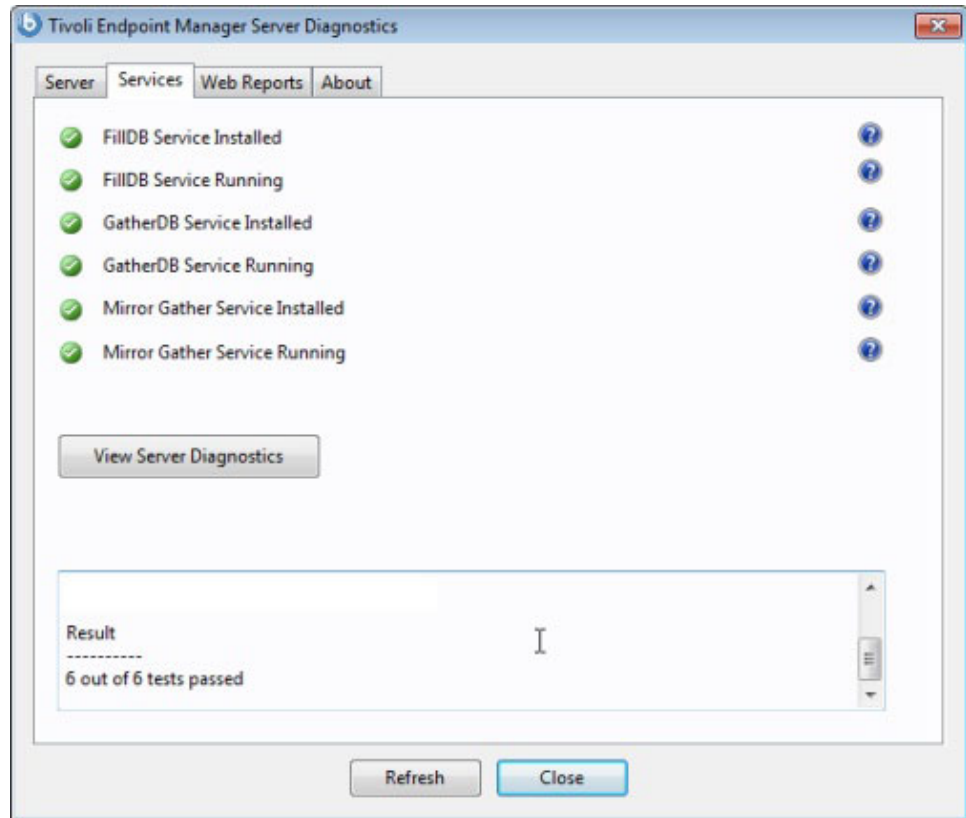
**Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Diagnostics Tool.** The program analyzes the server components and creates a report.

2. For more in-depth information, click the **Full Interface**. The IBM Endpoint Manager Diagnostic control panel is displayed. This window has tabs corresponding to the categories of server diagnostics, including **Services** and **Web Reports**.



**Note:** If the message Verifying that the BESGather service can reach the Internet is displayed after a fresh install and you have a proxy, ensure that you configured it as described in “Setting up a proxy connection” on page 107. If you have not yet installed the client, a warning light is shown. It becomes green as soon as you install the client.

3. In the **Services** tab check if the database and gathering services are correctly installed and running.



If a red light is glowing next to an item, it indicates a failure of that component. You must address the stated problem before you can be sure that the 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 IBM 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 IBM Endpoint Manager server is now successfully installed and responds to messages and requests from the relay, client, and console computers using a variety of components.

To better understand what the server does, read the descriptions of some of the components.

### 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 IBM Endpoint Manager database through the FillDB service and then becomes viewable in the console. Other state changes are also 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 IBM Endpoint Manager traffic.

## Installing the console

The IBM 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 HTTPS port 52311 to the server. Except in testing or evaluation environments, do not 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 > IBM Endpoint Manager > IBM Endpoint Manager Installation Guide**). Click **Install IBM Endpoint Manager Components**.
2. From the next panel, click **Install Console**.
3. When prompted, enter the 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.
4. 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.

For more details about using the console program, see the *IBM Endpoint Manager Console Users Guide*.



## Installing the clients

Install the IBM Endpoint Manager Client on every computer in your network that you want to administer, including those computers that are running the server and the console. This allows those computers to receive important Fixlet messages such as security patches, configuration files, or upgrades.

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

If you run the Client Deploy Tool (BESClientDeploy.exe), you can deploy the clients in three ways:

### Find computers using Active Directory

The IBM 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 is 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 host names. 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.

## Using the Client Deploy Tool:

In 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 IBM 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 IBM 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 reports **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 IBM Endpoint Manager Client Deploy Tool is created by the Installation Generator. You can launch the tool from the Installation Guide. Click the **Install IBM Endpoint Manager Components > Install IBM Endpoint Manager Clients > Install Remotely** button or launch it directly from **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Client Deploy**.
2. The resulting dialog offers three ways to deploy the Clients:

#### **Find computers using Active Directory**

The IBM Endpoint Manager Client Deploy tool contacts the Active Directory server to get a list of all 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 is 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 **user name** 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 IBM 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 choose to push the files.

#### Connection Method

You can connect to the remote computers either using the **Service Control Manager (SCM)**, which is recommended, or 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 IBM Endpoint Manager support site.

#### Installing the client manually:

You can install the IBM Endpoint Manager client manually by running the Client installer on each computer. Use this method to install the client on a small number of computers.

1. You can install the client using one of the following methods:
  - Log on to the computer with administrator privileges and copy the **BES Installers\Client** folder from the installation computer to the local hard drive. Or
  - Run the Installation Guide (available at **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Installation Guide**) and click the button marked **Browse Install Folders** to open the **IBM Endpoint Manager Installers** folder and display 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 IBM Endpoint Manager Client application is now installed and will automatically begin working in the background. Repeat this process on every computer in your network that you want to place under IBM 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 /T=TransformList /qn`

The `/qn` command performs a silent installation.

- `msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi INSTALLDIR="c:\myclient" /T=TransformList`

This command installs the program in the given directory.

**Note:** `/T=TransformList` specifies what transform files (.mst) must be applied to the package. *TransformList* is a list of paths separated by semicolons. The following table describes the supplied transform files, the resulting language, and the numerical value to use in the **msiexec** command line.

Table 2.

Language	Transform File name	Value
U.S. English	1033.mst	1033
German	1031.mst	1031
French	1036.mst	1036
Spanish	1034.mst	1034
Italian	1040.mst	1040
Brazilian Portuguese	1046.mst	1046
Japanese	1041.mst	1041
Korean	1042.mst	1042
Simplified Chinese	2052.mst	2052
Traditional Chinese	1028.mst	1028

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](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 computers on which you want to install have the tool enabled, you can use the tool to deploy an installation package for the Client.

**Note:** This is the most effective way to deploy to an enterprise because the infrastructure and deployment procedure is already in place

## Using Group Policies:

You can use Active Directory Group Policy Objects (GPO), define a policy requiring 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. For more details consult your Active Directory administrator.

## Using Login Scripts:

In an NT or AD domain, you can write login scripts that check for the presence of the client. When the user 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 about how to use login scripts to install the Client.

If you plan to add new computers to your network from time-to-time, this approach ensures that the Server discovers and manages new machines automatically. However, in some networks using Windows 2000 or XP, users must log in with Administrator privileges for this technique to work.

The login scripts pass arguments to the Windows Installer-based setup. For more information about command line options for setup.exe, see the InstallShield's support website at [http://kb.flexerasoftware.com/doc/Helpnet/isxhelp12/IHelpSetup\\_EXECmdLine.htm](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 directory C:\, run 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 fails and 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 steps:

*For Windows operating systems:*

1. Install the client on the computer to be imaged. The IBM 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.

2. Stop the client by opening the Windows Services dialog and stopping the **BES Client service**.
3. Delete the computer-specific identifier (computer ID) by opening the registry to HKLM\Software\BigFix\EnterpriseClient\GlobalOptions (on 64-bit systems the registry is HKLM\Software\Wow6432Node\BigFix\EnterpriseClient\GlobalOptions) and deleting the values ComputerID, RegCount, and ReportSequenceNumber.

The IBM 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 3 again**. The Server has built-in conflict detection and resolution so if for any reason you fail to delete the ID, the Server can detect that there are multiple Clients with the same ComputerID and forces the Client to re-register to ensure that everything works 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 Linux operating systems:*

1. Install the client on the computer to be imaged.
2. Stop the client by running `/etc/init/besclient stop`.
3. Delete the computer-specific identifier from the `.config` file to prevent all copies of the machine from registering with the same client ID to the server.

The IBM Endpoint Manager Client is now ready to be imaged.

*For Macintosh operating systems:*

1. Install the client on the computer to be imaged.
2. Stop the client by using **sudo systemstarter stop BESClient**.
3. Delete the computer-specific identifier to prevent all copies of the machine from registering with the same client ID to the server.
  - If they exist, remove **RegCount**, **ReportSequenceNumber**, and **ComputerID** from the client preferences folder: `/Library/Preferences/com.bigfix.besagent.plist`.
  - Delete the `__BESData` folder. The default location is `\Library\Application Support\BigFix\BES Agent`.

The IBM Endpoint Manager Client is now ready to be imaged.

### 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. Using email is an effective method 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 become 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 for.
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 IBM Endpoint Manager Administration Tool

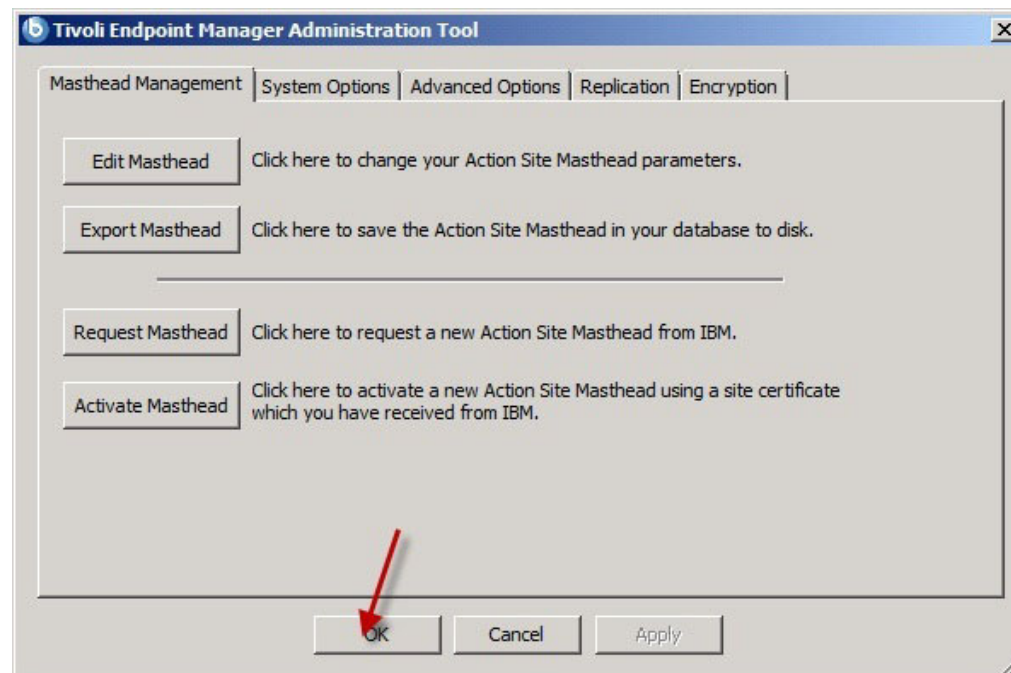
The Installer automatically creates the IBM Endpoint Manager Administration Tool when it installs the other components of the Console program. This program operates independently of the Console and is intended for Administrative Operators only. You can find it from the Start menu: **Start > All Programs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

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

**Note:** To perform the user management tasks you must use the Console.

### Masthead Management:

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

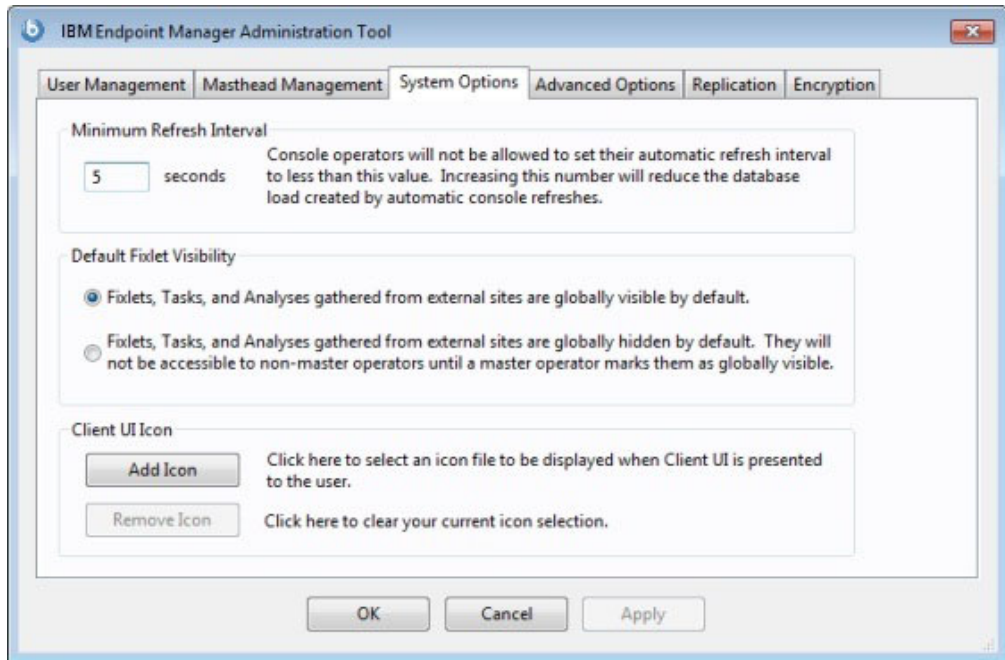


If you do not yet have a masthead, which is required to run the Console, this dialog provides an interface to **Request** and subsequently **Activate** a new masthead. If you have an existing masthead, you can edit it to change gathering intervals and locking. For more information about managing your masthead, see “Editing the Masthead on Windows systems” on page 159. You can also export your masthead, which can be useful if you want to extend your IBM 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.



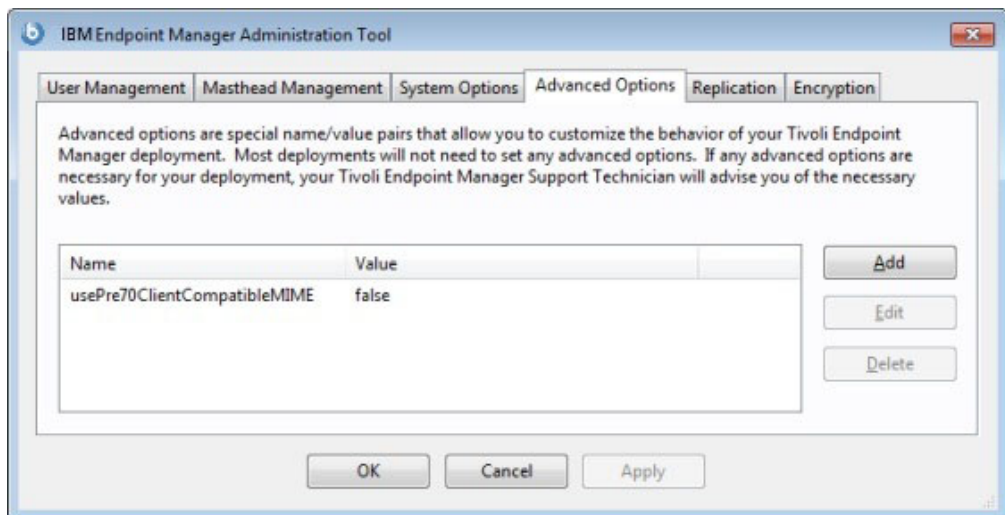


Use this dialog to set the default visibility of external sites. These sites are, by default, globally visible to all Console operators. To give you extra control, you can set the visibility to hidden, and then adjust them individually through the Console. You must be an administrator or a master operator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

Use this dialog to 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.



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. Use this dialog to visualize your replication servers. For more information, see “Managing Replication (DSA) on Windows systems” on page 122.

**Encryption:**

The final tab opens the **Encryption** dialog. Use this dialog to generate a new encryption key or to disable encryption altogether. For more information, “Managing Client Encryption” on page 132.



---

## Chapter 7. Installing on Linux systems

After understanding the terms and the administrative roles, you are ready to actually get authorized and install the programs.

Because IBM Endpoint Manager is powerful, you might 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 by getting a **License Authorization** file, which will have a name like `CompanyName.BESLicenseAuthorization`.

The installation program collects further information about your deployment and then creates a file called the **action site masthead**. This file establishes a chain of authority from the IBM 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) together with a public key used to verify the digital signatures.

---

### Installing and configuring DB2

Depending on which version of DB2 you want to install, you install DB2 either before installing the Endpoint Manager server or at the same time:

- **DB2 V10.1 Enterprise Server Edition:** you must install this version of DB2 before installing the Endpoint Manager server. Install it on the local workstation where you want to install the Endpoint Manager server or on a remote workstation. For information about how to install and verify DB2 server installation on Red Hat Enterprise Linux server 64-bit, see DB2 servers and IBM data server clients. Before installing the Endpoint Manager server ensure that the DB2 V10.1 Enterprise Server Edition has been installed and started as follows:
  - If the DB2 V10.1 Enterprise Server Edition is installed locally:
    1. Switch to the local DB2 Administrative user (default: `db2inst1`) by running the following command:

```
su - db2inst1
```
    2. Verify that the DB2 instance is active by running the command `db2start`. If the DB2 instance is running, you get this message:

```
SQL1026N The database manager is already active
```

otherwise the DB2 instance is started. You can also verify it by checking that the `db2sysc` process is active using the following command:

```
ps -ef | grep db2sysc
```
  - If the DB2 V10.1 Enterprise Server Edition is installed remotely:
    1. Install a DB2 10.1 client locally and connect it to the DB2 10.1 server installed on the remote workstation. No additional DB2 configurations (such as the catalog of the remote database) are required.
    2. On the remote DB2, ensure that the DB2 administrative server `db2admin` is started to enable remote administration. To start `db2admin`, run the following commands:

```
# su - dasusr1
# $ db2admin start
```

- **DB2 V10.1 Workgroup Server Edition:** you can install this version of DB2 either before installing the Endpoint Manager server by following the previous steps or together with the Endpoint Manager server installation after downloading it. You download it to the local workstation where you want to install the Endpoint Manager server. During the Endpoint Manager server installation, you must provide the following information:

#### **DB2 Setup Location**

The path where you downloaded the DB2. The default is  
../wser/db2setup.

#### **DB2 Administrative User Password**

The password of the DB2 Administrative user.

All the steps to configure DB2 are then performed by the Endpoint Manager server installation program.

To automatically start the DB2 instance after a reboot, perform the following steps:

1. Run the following command::

```
/opt/ibm/db2/V10.1/bin/db2iauto -on db2inst1
```

or create a shell script in the /etc/init.d directory, such as db2auto.sh, containing the following code:

```
#!/bin/sh
for i in `ls /opt/ibm/db2/V10.1/bin/db2i*`;
do
su - $i -c "db2start"
done
```

2. Give execution rights 3 to the script and add it to the Linux **Startup Applications** from **System -> Preferences -> Startup Applications**.

For information about database requirements, see “Database requirements” on page 19 and Installation requirements for DB2 database products.

---

## **Installation Steps**

To install the Endpoint Manager Server perform the following steps:

1. Download IBM Endpoint Manager.
2. Install the Server using the License Authorization file (\*.BESLicenseAuthorization) you created in the License Key Center or, in the case of a Proof-of-Concept evaluation, that was provided to you by your IBM Technical Sales Representative. During the installation you request the license and create the masthead file.

**Note:** Before running the installation ensure that DB2 is up and running

3. Verify that the installation completed successfully.

### **Step 1 - Downloading IBM Endpoint Manager**

Download IBM Endpoint Manager from IBM's Passport Advantage portal.

You can download IBM Endpoint Manager also from the support site at <http://support.bigfix.com/bes/install/downloadbes.html> or from the

DeveloperWorks trial site at <http://www.ibm.com/developerworks/downloads/tiv/endpoint/>. The demonstration trial installer is the same installer program for a normal production installation.

To install the server component, download the following e-images from Passport Advantage:

*Table 3. Parts required for installing Endpoint Manager Server*

Software Name	Part Number	Content
IBM Endpoint Manager Platform Install V9.0.0 Multiplatform Multilingual (CIGP2ML)	CIGP2ML	<ul style="list-style-type: none"><li>• DB2_10_limited_CD_Linux_x86-64.tar.gz</li><li>• IBMIM_win32.exe</li><li>• IEM_Pltfm_Install_V90.zip</li><li>• IEM_V90_QS.zip</li></ul>

To extract the Endpoint Manager Linux Server installation files, perform the following steps:

1. Copy the Endpoint Manager Server compressed zip file IEM\_Pltfm\_Install\_V90.zip on your Linux Server.
2. Expand the compressed zip file using the following command:  

```
unzip IEM_Pltfm_Install_V90.zip
```
3. From the linux\_server folder, expand the ServerInstaller\_9.0.586.0-rhel.tgz file on your Red Hat Enterprise Linux Server by using the following command:  

```
tar -zxvf ServerInstaller_9.0.586.0-rhel.tgz
```

You can find the install.sh file to install the Linux Server in the ServerInstaller\_9.0.586.0-rhel folder.

## Step 2 - Installing the Server

Before running the installation procedure ensure you have Korn Shell (KSH) installed on your workstation. For the complete list of installation prerequisites, see “Server requirements” on page 18.

**Note:** The installation program installs all prerequisites using Yum. For information about how to configure Yum and Yum repositories see Configuring Yum and Yum Repositories.

To install the Endpoint Manager Server in your production environment, perform the following steps:

1. From the shell where you extract the server package, move to the installation directory, ServerInstaller\_n.n.nnn.n-rhel and enter the following command:  

```
./install.sh
```
2. After reading the License Agreement, enter 1 to accept it and continue.
3. To install the Production, enter 2:  
Select Install Type  
[1] Evaluation: Request a free evaluation license from IBM Corp. This license allows you to install a fully functional copy of the IBM Endpoint Manager on up to 30 clients, for a period of 30 days.  
[2] Production: Install using a production license or an authorization for a production license  
Choose one of the options above or press Enter to accept the default

4. To install all the components, enter 1:  
 Select the IBM Endpoint Manager Features you want to install:  
 [1] All Components (Server, Client, and WebReports)  
 [2] Server and Client Only  
 [3] WebReports Only  
 Choose one of the options above or press <Enter> to accept the default: [1]
5. Enter 1 to create a Master database for later replication or if you only need a single database in your deployment.  
 Select Database Replication:  
 [1] Single or Master Database  
 [2] Replicated Database  
 Choose one of the options above or press <Enter> to accept the default: [1]

If you enter 2, you create a replica of an existing master. For additional information see, “Understanding replication” on page 27.

6. To use a local database, enter 1:  
 Select Database:  
 [1] Use Local Database  
 [2] Use Remote Database  
 Choose one of the options above or press <Enter> to accept the default: [1]

The local database name of Endpoint Manager server is BFENT. The local database name of Web Reports is BESREP0R.

**Note:** To use an external database for IBM Endpoint Manager, you must perform the following steps:

- a. Install the DB2® server on the remote workstation.
  - b. Install a DB2 client on the workstation from where you run the Endpoint Manager Server installation
  - c. Connect the DB2 server to the DB2 client installed on the workstation from where you run the installation, that is, the port of the DB2 database (default 50000) must be reachable by the workstation where the installation is running.
7. Enter the user name for the local DB2 Administrative user. The default is db2inst1.
  8. Enter the DB2 Local Administrative user password.
  9. Enter the user ID and the password to define the initial administrative user. The user name default is: IEMAdmin.
  10. To run the installation using a BES license authorization file, enter 1.  
 Choose the setup type that best suits your needs:  
 [1] I want to install with a BES license authorization file  
 [2] I want to install with a Production license that I already have  
 [3] I want to install with an existing masthead

**Note:** If you already ran the first installation, or part of it, and you have the authorization file, you can specify option 1, 2 or 3, with an existing production license (license.crt, license.pvk) or an existing masthead (masthead.afxm) and perform only some of the installation steps.

11. Specify where to copy the generated license authorization file:  
 License Authorization Location  
 Enter the location of the license authorization file that you received from IBM or press <Enter> to accept the default:  
 ./license/LicenseAuthorization.BESLicenseAuthorization
12. If there is a proxy or a firewall that requires a username and password every time an internet request is made, set a proxy connection to enable the



Endpoint Manager server or relay to connect to the internet as described in "Setting up a proxy connection" on page 107.

13. Specify the DNS name or ip address of the machine on which to install the server. This name is saved in your license and will be used by clients to identify the Endpoint Manager server. It cannot be changed after a license is created.
14. Specify the related Site Admin Private Key Password.
15. Specify the size in bits of the key used to encrypt the credentials:  
Key Size Level  
Provide the key size that you want to use:  
[1] 'Min' Level (2048 bits)  
[2] 'Max' Level (4096 bits)  
Choose one of the options above or press <Enter> to accept the default: [1]
16. Enter the License folder where the installation generates and saves license.crt, license.pvk and masthead.afxm.  
Choose License Folder:  
Specify a folder for your private key (license.pvk), license certificate (license.crt), and site masthead (masthead.afxm) or press <Enter> to accept the default: ./license
17. After you specify where to save the files to be generated, you can submit the request to IBM for getting the license certificate by choosing one of the following options depending on if your machine is connected to Internet:  
[1] Submit request from this machine over the Internet. The request will be redeemed for a license certificate (license.crt) and saved in your credential folder.  
[2] Save request to a file and send it to IBM at the URL:  
'http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html'.  
This method might be necessary if your deployment is isolated from the public Internet.

If you choose 1, you can continue with the next installation step.

If you choose 2, the request.BESLicenseRequest request is generated. You can continue the installation by importing the certificate specifying the location of the license certificate (such as: ./license/license.crt) or exit from the installation and rerun it at a later time as described in the installation procedure:

```
Info: The following License Request file was successfully generated:
./license/request.BESLicenseRequest
#####
Import License Certificate
[1] Continue with the installation importing the certificate (license.crt).
[2] Exit from the installation, I will import the certificate at a later time.
```

If you exit the installation you can rerun ./install.sh later and repeat all the steps specifying that you want to use the generated license or masthead with option 2 or 3:

```
Choose the setup type that best suits your needs:
[1] I want to install with a BES license authorization file
[2] I want to install with a Production license that I already have
[3] I want to install with an existing masthead
```

To import the files, you need to specify the license certificate file (./license/license.crt) and the Site Admin Private Key (./license/license.pvk) to administer the database:

```
License Certificate Location
Enter the location of the license certificate file or
press <Enter> to accept the default: ./license/license.crt
```

Site Admin Private Key:  
Specify the site Level Signing Key file (license.pvk) for the database you want to administer or press <Enter> to accept the default: ./license/license.pvk

18. Accept the default masthead values:

Server Port Number: 52311  
Use of FIPS 140-2 compliant cryptography: Disabled  
Gather Interval: 1 Day  
Initial Action Lock: Unlocked  
Action Lock Controller: Console  
Action Lock exemptions: Disabled

or change them by entering 2:

- [1] Use Defaults Values
- [2] Use Custom Values

You can change the following masthead parameters:

**Server Port Number**

Specify the number of the server port. The default value is: 52311.

**Note:** Do not use port number 52314 for the network communication between the Endpoint Manager components because it is reserved for proxy agents.

**Enable use of FIPS 140-2 compliant cryptography**

Enter 1 to enable it, 2 to disable it. The default value is 2.

**Gathering Interval**

Specify the interval time to use by entering one of the following values:

- [1] Fifteen Minutes
- [2] Half Hour
- [3] One Hour
- [4] Eight Hours
- [5] Half Day
- [6] One Day
- [7] Two Days
- [8] One Week
- [9] Two Weeks
- [10] One Month
- [11] Two Months

The default value is: 6 (one day).

**Initial Action Lock**

You can choose to lock, to lock for a time, or unlock:

- [1] Locked
- [2] Lock Duration
- [3] Unlocked

The default value is: 3 (unlocked).

**Enable Lock Exemptions**

- [1] Lock Exemption Enabled (fairly unusual)
- [2] Lock Exemption Disabled

The default value is 2 (disable lock exemption).

19. Enter the location where the downloaded files for the Clients are stored:

Choose the Web Server's Root Folder:  
Specify the location for the Web Server's Root Folder or press <Enter> to accept the default: /var/opt/BESServer

20. Enter the location where the WebReports Server stores its files:  
Choose the WebReports Server's Root Folder:  
Specify the location for the WebReports Server's Root Folder or  
press <Enter> to accept the default: /var/opt/BESWebReportsServer
21. Enter the WebReports Server port:  
Choose the WebReports Server's Port:  
Specify the Port Number or press <Enter> to accept the default: 80

The default is 80, but if IIS is installed, the installation program chooses port 52312.

The IBM Endpoint Manager Server installation is now complete. You can now install the IBM Endpoint Manager Console on a Windows System and log on with the account you created during the installation of the server.

You can see installation errors in the BESinstall.log and the BESAdmin command line traces in the BESAdminDebugOut.txt files under the /var/log directory.

### Step 3 - Verifying Server Installation

To verify that an installation has completed successfully, perform the following steps:

1. Ensure that the following message is displayed to the standard output or in the installation log file /var/log/BESInstall.log:  
The installation of IBM Endpoint Manager was completed successfully.  
You can now proceed to install the IEM Console on a Windows System and log on as 'EvaluationUser', the user just created.  
The IEM Console installer is available in the folder '/var/opt/BESInstallers
2. Ensure that the services associated with each installed components are up and running by entering the following commands:  

```
/etc/init.d/besserver status
/etc/init.d/besfilldb status
/etc/init.d/besgatherdb status
/etc/init.d/besclient status
/etc/init.d/beswebreports status
```
3. Ensure that local or remote databases are created by switching to the local DB2 Administrative user (default: db2inst1) and running the list database command:  

```
su - db2inst1
db2 list db directory
```

Check that the following databases are created:

- Server component: BFENT
  - WebReports component: BESREPOR
4. Launch the IBM Endpoint Manager Console and provide the credentials of the first IBM Endpoint Manager user created at installation time to ensure that the Console connects to the Server. User default values are: EvaluationUser for the evaluation Installation and IEMAdmin for the production installation. Ensure that the client installed by default on the server machine is registered.
  5. Ensure that you can log on to the Web Reports from the Console by selecting **Tools -> Launch WebReports** and providing the credentials of the first user created at installation time.

---

## Installation Command Options

You can run the Production or Evaluation installation in interactive or silent mode. The full command to run any type of installation is the following:

```
./install.sh [ -f <input_response_file> ] [ -g <output_response_file> ]  
[ -upgrade | -upgradeNoClient ] [ -reuseDb ]
```

where:

**-f <input\_response\_file>**

Specifies the full path and file name of the response file to use.

**-g <output\_response\_file>**

Generates a response file.

**-upgrade**

Runs the script to upgrade all the components.

**-upgradeNoClient**

Runs the script to upgrade all the components except for the Client.

**-reuseDb**

Allows you to use an existing database.

---

## Silent installation

Use the silent mode to install the Evaluation server or to run problem determination on a failed installation.

To run a silent installation run the following command:

```
./install.sh -f response_file
```

where *response\_file* is the file containing the parameter values to use during the installation.

This is an example of response file:

```
##IEM GENERATED RESPONSE FILE  
LA_ACCEPT="true"  
IS_EVALUATION="false"  
COMPONENT_SRV="true"  
COMPONENT_WR="true"  
SINGLE_DATABASE="true"  
LOCAL_DATABASE="true"  
DB2_ADMIN_USER="db2inst1"  
DB2_ADMIN_PWD="Bigfix11"  
BES_WWW_FOLDER="/var/opt/BESServer"  
WR_WWW_FOLDER="/var/opt/BESWebReportsServer"  
WR_WWW_PORT="80"  
TEM_USER_NAME="IEMAdmin"  
TEM_USER_PWD="Bigfix11"  
CONF_FIREWALL="yes"  
BES_SETUP_TYPE="authfile"  
BES_AUTH_FILE="/tmp/ServerInstaller_9.0-rhel  
/offlic/LicenseAuthorization.BESLicenseAuthorization"  
SRV_DNS_NAME="temtest03"  
BES_LICENSE_PVK_PWD="Bigfix11"  
PVK_KEY_SIZE="min"  
BES_LIC_FOLDER="/tmp/ServerInstaller_9.0-rhel/offlic"
```

```
SUBMIT_LIC_REQUEST="yes"
USE_PROXY="false"
ADV_MASTHEAD_DEFAULT="true"
DB2_PORT="50000"
```

You can create a response file during an installation by redirecting the installation parameters in a response file using the following command:

```
./install.sh -g response_file
```

---

## Installation Folder Structure

After the Endpoint Manager installation, you can see the following folder structure:

### Server Folder Structure:

```
/var/opt/BESInstallers
/var/opt/BESInstallers/Client (Client installer)
/var/opt/BESInstallers/Console (Console installer)

/var/opt/BESServer
  besserver.config (Configuration file)
  besserver.config.default (Default configuration file)

/var/opt/BESServer/FillDBData/FillDB.log (FillDB service log)

/var/opt/BESServer/GatherDBData/GatherDB.log (GatherDB service log)

/opt/BESServer
/opt/BESServer/bin (Server binaries)
/opt/BESServer/reference (Rest API xsd templates)

/etc/opt/BESServer
  actionsite.afxm (Masthead file)

/etc/init.d
  besserver (Server service)
  besfilldb (FillDB service)
  besgatherdb (GatherDB service)
```

### WebReports Folder Structure:

```
/var/opt/BESWebReportsServer
  beswebreports.config (Configuration file)
  beswebreports.config.default (Default configuration file)

/opt/BESWebReportsServer
/opt/BESWebReportsServer/bin (WebReports binaries)

/etc/opt/BESWebReportsServer
  actionsite.afxm (Masthead file)

/etc/init.d
  beswebreports (WebReports service)
```

### Client Folder Structure:

```
/var/opt/BESClient
  besclient.config (Configuration file)
  besclient.config.default (Default configuration file)

/opt/BESClient
/opt/BESClient/bin (Client binaries)

/etc/opt/BESClient
```

```
actionsite.afxm (Masthead file)

/etc/init.d
besclient (besclient service)
```

#### Install Log Files:

```
/var/log/
  BESInstall.log      (Installer log file)
  BESAdminDebugOut.txt (Administrator Tool debug information)
  BESRelay.log        (Relay log file)
```

---

## Configuration, Masthead, and Log Files

At the end of the installation you can find the following Endpoint Manager files containing the settings of the installed components and the installation messages:

*Table 4. Configuration and Log Endpoint Manager Files*

Component	File
Server	<ul style="list-style-type: none"><li>• Configuration file: /var/opt/BESServer/besserver.config</li><li>• Masthead file: /etc/opt/BESServer/actionsite.afxm</li><li>• Log files: /var/log/BESInstall.log, /var/log/BESAdminDebugOut.txt</li></ul>
Web Report	<ul style="list-style-type: none"><li>• Configuration file: /var/opt/BESWebReportsServer/beswebreportsserver.config</li><li>• Masthead file: /etc/opt/BESWebReportsServer/actionsite.afxm</li></ul>
Client	<ul style="list-style-type: none"><li>• Configuration file: /var/opt/BESClient/besclient.config</li><li>• Masthead file: /etc/opt/BESClient/actionsite.afxm</li></ul>
Relay	<ul style="list-style-type: none"><li>• Configuration file: /var/opt/BESRelay/besrelay.config</li></ul>

The configuration files contain settings for traces, database connection, and proxy configuration. The BESServer, BESFillDB, and BESGatherDB services search for the configuration parameters first on besclient.config and then on besserver.config. The BESWebReportServer service searches for the configuration parameters first in besclient.config and then in beswebreportsserver.config.

---

## Managing the Endpoint Manager Services

You can start, stop, restart, or query the status of Linux Endpoint Manager services using the following commands:

```
service service stop
service service start
service service restart
service service status

/etc/init.d/service stop
/etc/init.d/service start
/etc/init.d/service restart
/etc/init.d/service status
```

where *service* is one of the following services:

```
besfilldb  
besgatherdb  
besserver  
beswebreports
```

---

## Changing the DB2 password

After you install the DB2 database of the Endpoint Manager server, you can change the database password by performing the following steps:

1. Stop the berserver service:

```
service besserver stop
```

2. Open the configuration file: /var/opt/BESServer/besserver.config

3. Go to [Software\BigFix\EnterpriseClient\Settings\Client\\_BESServer\_Database\_Password] and change:

```
value = ""
```

with the new DB2 password, such as

```
value = "db2newpassword"
```

4. Open the configuration file: /var/opt/BESWebReportsServer/beswebreports.config

5. Go to [Software\BigFix\Enterprise Server\FillAggregatedDB] and change:

```
value = ""
```

with the new DB2 password, such as

```
value = "db2newpassword"
```

6. Restart the besserver service:

```
service besserver restart
```

At restart passwords are obfuscated and substituted again with "" in the configuration files.

---

## Changing the DB2 port

When you install DB2 with a port different from the standard one (50000), to allow the database replication on secondary DSA server, you must configure the database port by setting it in the besserver.config file of the primary server as follows:

1. Stop the berserver service:

```
service besserver stop
```

2. Open the configuration file: /var/opt/BESServer/besserver.config

3. Go to [Software\BigFix\EnterpriseServer\FillDB] and add the new port number as follows:

```
ReplicationPort = "50025"
```

4. Restart the besserver service:

```
service besserver restart
```

At restart the port number is updated.



---

## Removing the Primary Server on Linux systems

To uninstall the IBM Endpoint Manager Server, you must stop the services and remove the Server, the Client, and Web Reports components, and the related databases.

To uninstall the primary server on Linux systems, perform the following steps:

1. Remove the Server, the Client, and Web Reports rpms files:

```
rpm -e BESRootServer-xxxx_rhel.i686
rpm -e BESClient-xxxxxx_rhel.x86-64
rpm -e BESWebReports-xxxx-rhel.i686
```

2. Remove the following directories:

```
rm -fr /var/opt/BESClient
rm -fr /etc/opt/BESClient
rm -fr /var/opt/BESServer
rm -fr /etc/opt/BESServer
rm -fr /var/opt/BESWebReportsServer
```

3. Remove the BFENT and BESREPOR local databases:

```
su - db2inst1
db2 drop db BFENT
db2 drop db BESREPOR
```

or the the BFENT and BESREPOR remote databases:

```
db2 uncatalog db BFENT
db2 uncatalog db BESREPOR
db2 uncatalog node TEM_RER
```

---

## Authenticating Additional Servers (DSA)

Multiple servers can provide a higher level of service for your IBM 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 using DSA.

Your servers can communicate with each other using the DB2 inter-server authentication option.

Before installing the additional Linux Servers, install the DB2 server on each machine that you want to add to your deployment. The version of the DB2 server must be the same as the DB2 server installed on the Master Server.

### Using DB2 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 configuration file on each Server. To authenticate your Servers using DB2 Authentication, follow these steps:

1. Choose a single login name (for example, db2inst1), and a single password to be used by all servers in your deployment for inter-server authentication.
2. On the Master Server, open the `/var/opt/BESServer/besserver.config` file.

3. Add or modify the following keywords in the [Software\BigFix\Enterprise Server\FillDB] section:

```
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 DB2-authenticated servers. Also, all IBM Endpoint Manager Servers in your deployment must be running the same version of DB2 Server.

---

## Installing Additional Linux Servers (DSA)

Before installing the DSA servers, determine your authentication method and complete the steps described in “Authenticating Additional Servers” on page 54.

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

1. Ensure that each Server uses the same DB2 Server version being used by the Master Server.
2. Copy the license.pvk and masthead.afxm files from the master server to a folder on each machine that you are installing.
3. Run the install.sh script on each machine that you want to configure as an additional Server. Use the same domain administration that you used for the local DB2 Server install (so you have sa authority).
4. On the Select Install Type prompt, choose:  
[2] Production: Install using a production license or an authorization from a production license
5. On the Select the IBM Endpoint Manager Features you want to install prompt, choose either to install All Components, or Server and Client only.
6. On the Select Database Replication prompt, choose:  
[2] Replicated Database.
7. On the Select Database prompt, choose [1] Use Local Database (typical for most applications).
8. On the DB2 Local Administrative User prompt, assuming you chose Use Local Database earlier, enter the user name and password of the DB2 administrative user for the database on the computer where the installation script is running.
9. Enter the folders of the Web Servers Root and WebReports Server Root
10. Enter the port number of the WebReports Server.
11. Define the credentials of the WebReports administrative user. The default is: IEMAdmin.
12. Specify the location of license.pvk and its password.
13. Specify the location of the existing masthead.afxm file that was generated when installing the master server.
14. On the Secondary Server DNS Name prompt, enter the DNS name of the new server. This name must be resolvable by other servers and by clients.
15. On the DB2 Connection prompt, enter the port number of the local DB2 instance where the installer is running.
16. Enter information about the master server DB2 instance to allow the new server to connect to DB2 on the master server:

On the Master Server Database Hostname prompt, specify the hostname of the system where the Master Server Database is located.

On the Master Server Database Port prompt, specify the database port number of the system where the Master Server Database is located.

On the Master Server Database Administrative User prompt, specify the username of the DB2 Administrative user of the system where the Master Server Database is located.

On the Master Server Database Administrative User Password prompt, specify the password of the DB2 administrative user of the system where the Master Server Database is located.

---

## Understanding the server components

The IBM Endpoint Manager server is now successfully installed and responds to messages and requests from the relay, client, and console computers using a variety of components.

To better understand what the server does, read the descriptions of some of the components.

### 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 IBM Endpoint Manager database through the FillDB service and then becomes viewable in the console. Other state changes are also 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 IBM Endpoint Manager traffic.

---

## Installing the Console

You can install the IBM Endpoint Manager console on any Windows computer that can make a network connection via HTTPS port 52311 to the Server. Except in testing or evaluation environments, it is not recommended to run the Console on the Server computer due to the performance and security implications of having the publisher key credentials on a computer that is running a database or web server. Using the IBM Endpoint Manager console you can monitor and fix problems on all managed computers across the network.

To install the console, follow these steps:

1. Go to /var/opt/BESInstallers directory.
2. Copy the Console folder to a Windows workstation. Use the Console folder of the same build level.
3. From the Console directory on the Windows workstation run: setup.exe

**Note:** By default the local operating system firewall is enabled. To allow the Console to connect to the IBM Endpoint Manager Server, ensure that the firewall is configured to allow tcp and udp communications through the Server port (default 52311) and tcp communications through Web Reports Ports (default 80).

If you need to manually configure the local firewall you can run the following commands:

```
iptables -I INPUT -p tcp --dport < Server_Port > -j ACCEPT
iptables -I INPUT -p udp --dport < Server_Port > -j ACCEPT
iptables -I INPUT -p tcp --dport < WebReports_Port > -j ACCEPT
service iptables save
```

For more details about using the Console program see the *IBM Endpoint Manager Console Users Guide* .

---

## Installing the Client Deploy Tool

The Client Deploy Tool is used to deploy Windows Clients. This tool is also available on Linux Server and is wrapped into the Endpoint Manager Console image for Linux.

To install this tool in a Linux server deployment, perform the following steps:

1. Go to /var/opt/BESInstallers directory.
2. Copy the Console folder to a Windows workstation that will be also used as Endpoint Manager Console.
3. From the Console directory on the Windows workstation, run setup.exe to install the Console together with the Deploy Tool. To start the tool, from the C:\Program Files\BigFix Enterprise\BES Console\BESClientDeploy directory, run the BESClientDeploy.exe program.

---

## Installing the clients

Install the IBM Endpoint Manager Client on every computer in your network that you want to administer, including those computers that are running the server and the console. This allows those computers to receive important Fixlet messages such as security patches, configuration files, or upgrades.

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

If you run the Client Deploy Tool (BESClientDeploy.exe), you can deploy the clients in three ways:

**Find computers using Active Directory**

The IBM 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 is 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 host names. 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.

## Using the Client Deploy Tool

In 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 IBM 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 IBM 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 reports **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. From the C:\Program Files\BigFix Enterprise\BES Console\BESClientDeploy directory, run the BESClientDeploy.exe program.
2. The resulting dialog offers three ways to deploy the Clients:
  - **Find computers using Active Directory.** The IBM 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 IBM 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 IBM Endpoint Manager support site.

## Installing the Client Manually

The IBM 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. Log on to the computer with administrator privileges and copy the **BES Installers\Client** folder from the installation computer to the local hard drive.
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 IBM 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 IBM 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 /T=TransformList /qn`

The `/qn` command performs a silent installation.

- `msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi INSTALLDIR="c:\myclient" /T=TransformList`

This command installs the program in the given directory.

**Note:** `/T=TransformList` specifies what transform files (.mst) must be applied to the package. *TransformList* is a list of paths separated by semicolons. The following table describes the supplied transform files, the resulting language, and the numerical value to use in the **msiexec** command line.

Table 5.

Language	Transform File name	Value
U.S. English	1033.mst	1033
German	1031.mst	1031
French	1036.mst	1036
Spanish	1034.mst	1034
Italian	1040.mst	1040
Brazilian Portuguese	1046.mst	1046



Table 5. (continued)

Language	Transform File name	Value
Japanese	1041.mst	1041
Korean	1042.mst	1042
Simplified Chinese	2052.mst	2052
Traditional Chinese	1028.mst	1028

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](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>.

---

## Running the IBM Endpoint Manager Administration Tool

The installation script `install.sh` automatically downloads the IBM Endpoint Manager Administration Tool bash shell script, `BESAdmin.sh`, in the `/opt/BESServer/bin` directory. With this tool you can edit the masthead file, check the signatures of the objects in the database, reset the epoch of the database to the current date, resign all of the users content in the database, rotate the server private key.

To run this script from the command prompt, you must specify the private key file (`license.pvk`) and your private key password, as follows:

```
./BESAdmin.sh -service -sitePvkLocation=<path+license.pvk>
-sitePvkPassword=<password> [arguments]
```

where:

`service` can be one of the following:

```
editmasthead
findinvalidsignatures
reissuemanagementrights
reportencryption
resetdatabaseepoch
resignsecuritydata
rotateserversigningkey
```

**-sitePvkLocation=<path+license.pvk>**

Specifies a private key file (`filename.pvk`). The private key file and its password are required to run the Administration Tool. Only users with access to this file and its password are able to create new Endpoint Manager operators.

**Note:** The notation `<path+license.pvk>` used in the command syntax stands for `path_to_license_file/license.pvk`.

**-sitePvkPassword=<password>**

Specifies the password associated to the private key file (`filename.pvk`).

Each service has the following *arguments* :

### **editmasthead**

You can edit the masthead file by specifying the following parameters:

advRequireFIPSCompliantCrypto (optional, boolean)  
advGatherSchedule (optional, integer)

values:

0=Fifteen Minutes,  
1=Half Hour, 2=Hour,  
3=Eight Hours,  
4=Half day,  
5=Day,  
6=Two Days,  
7=Week,  
8=Two Weeks,  
9=Month,  
10=Two Months

advController (optional, integer)

values:

0=console,  
1=client,  
2=nobody

advInitialLockState (optional, integer)

values:

0=Locked,  
1=timed (specify duration),  
2=Unlocked

advInitialLockDuration (optional, integer)

values:

( duration in seconds )

advActionLockExemptionURL (optional, string)

The syntax to run this service is:

```
./BESAdmin.sh -editmasthead -sitePvkLocation=<path+license.pvk>  
-sitePvkPassword=<password> [ -advRequireFIPSCompliantCrypto=<true|false> ]  
[ -advGatherSchedule=<0-10> ] [ -advController=<0-2> ]  
[ -advInitialLockState=<0|2> | -advInitialLockState=1  
-advInitialLockDuration=<num> ]  
[ -advActionLockExemptionURL=<url> ]
```

### **findinvalidsignatures**

You can check the signatures of the objects in the database by specifying the following parameters:

**-resignInvalidSignatures (optional)**

Removes invalid signatures.

**-deleteInvalidlySignedContent (optional)**

Deletes contents with invalid signatures.

For additional information about invalid signatures see <http://www-01.ibm.com/support/docview.wss?uid=swg21587965>. The syntax to run this service is:

```
./BESAdmin.sh -findinvalidsignatures -sitePvkLocation=<path+license.pvk>  
-sitePvkPassword=<password>  
{ -resignInvalidSignatures | -deleteInvalidlySignedContent }
```

### **reissuemanagementrights**

#### **reportencryption**

You can enable Message Level Encryption by running:

```
./BESAdmin.sh -findinvalidsignatures -sitePvkLocation=<path+license.pvk>  
-sitePvkPassword=<password>
```

#### **resetdatabaseepoch**

You can reset the epoch of the database to the current date. The action site epoch is a timestamp from when the database is created that is used to synchronize your deployment with a particular instance of the database.

The syntax to run this service is:

```
./BESAdmin.sh -resetdatabaseepoch
```

### **resignsecuritydata**

You can resign all of the users content in the database to enable user login to the Console. You can specify the following parameter:

```
-mastheadLocation=<path+/actionsite.afxm>
```

The syntax to run this service is:

```
./BESAdmin.sh resignsecuritydata -sitePvkLocation=<path+license.pvk>  
-sitePvkPassword=<password> -mastheadLocation=<path+/actionsite.afxm>
```

### **rotateserversigningkey**

You can rotate the server private key to have the key in the file system match the key in the database.

The syntax to run this service is:

```
./BESAdmin.sh rotateserversigningkey -sitePvkLocation=<path+license.pvk>  
-sitePvkPassword=<password>
```



---

## Chapter 8. Post-installation configuration steps

After having run the installation, make sure that you read the following topics and run the requested activities if needed.

---

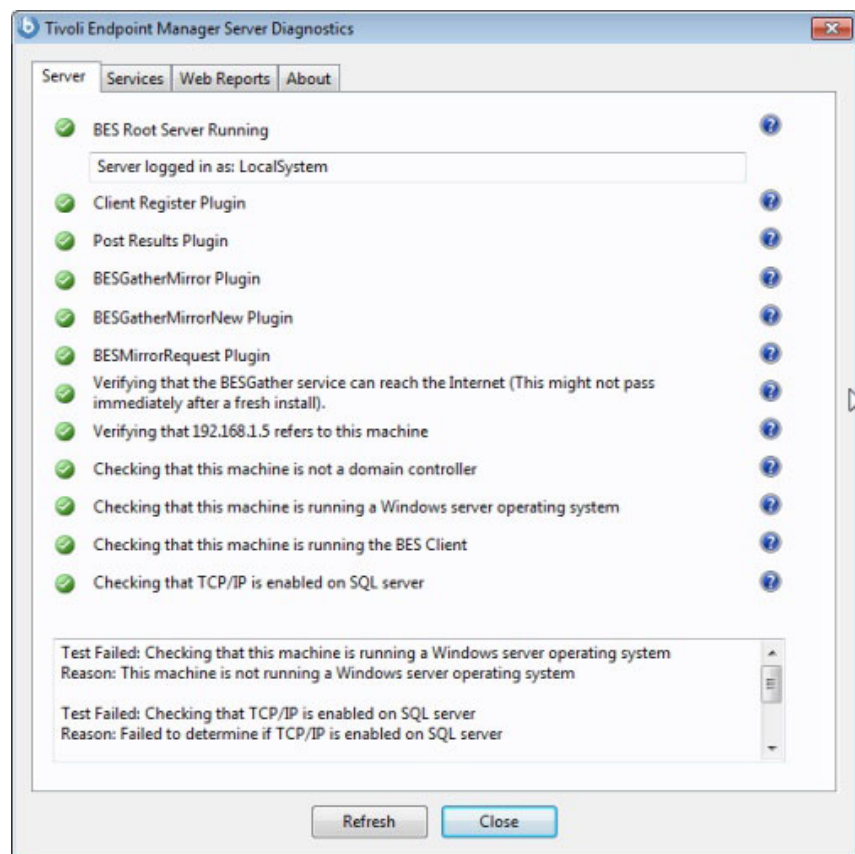
### Post-installation steps

After you install the product, perform these steps to verify that the installation run successfully and to complete the basic configuration steps.

1. Run the following step to verify that the installation run successfully:

#### On Windows:

From **Start > All Programs > Tivoli Endpoint Manager** run the IBM Endpoint Manager Server Diagnostics tool to verify that all the installation and configuration steps completed successfully.



If all the buttons are green, click **Close** to exit the Diagnostic tool, otherwise address the problem to be sure that the server is working correctly.

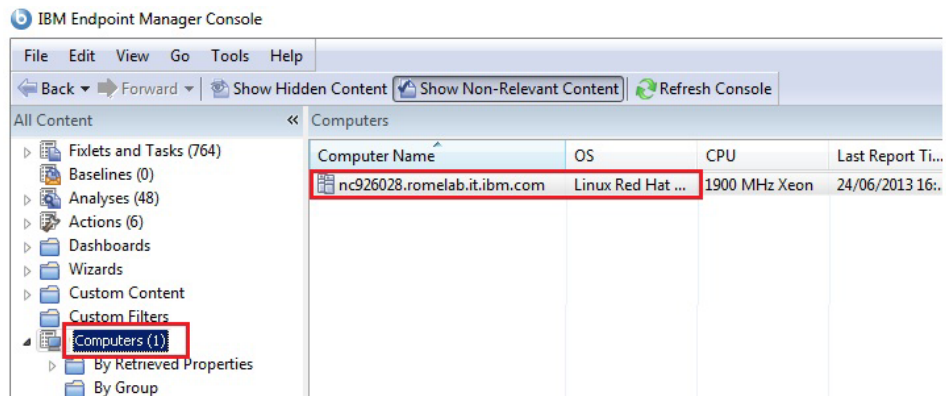
#### On Linux:

Ensure that the following services are up and running:

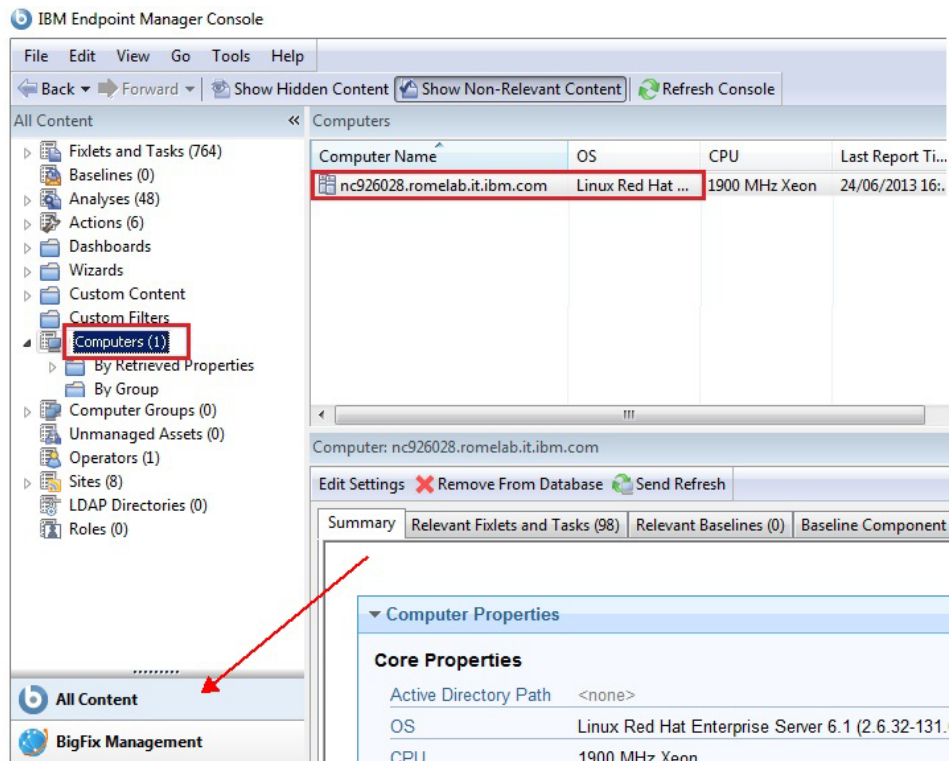
```
besfilldb  
besgatherdb  
besserver  
beswebreports
```

Use the command `service service status` to check the status of the services.

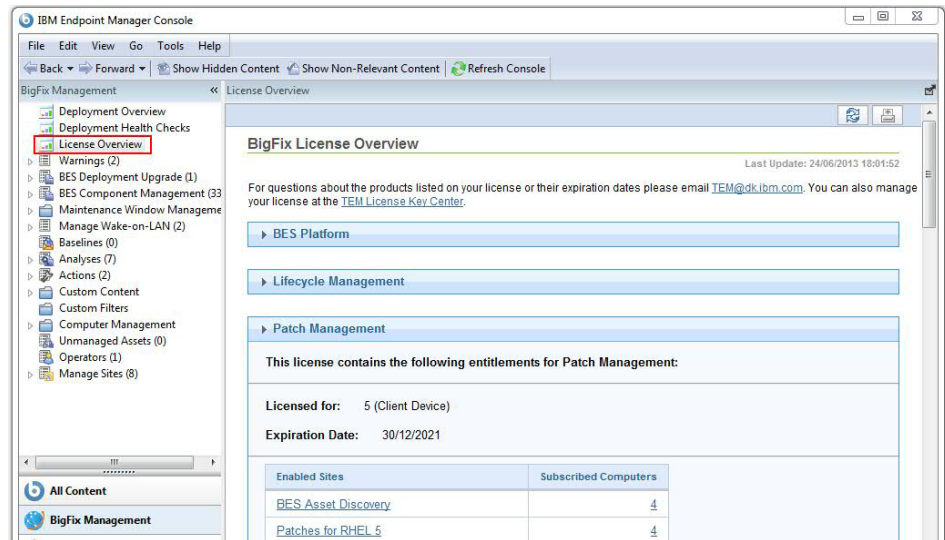
2. Open the Endpoint Manager console and verify that the client is registered.



3. From the console, verify that the **All Content** and **BigFix Management** domains have been created.

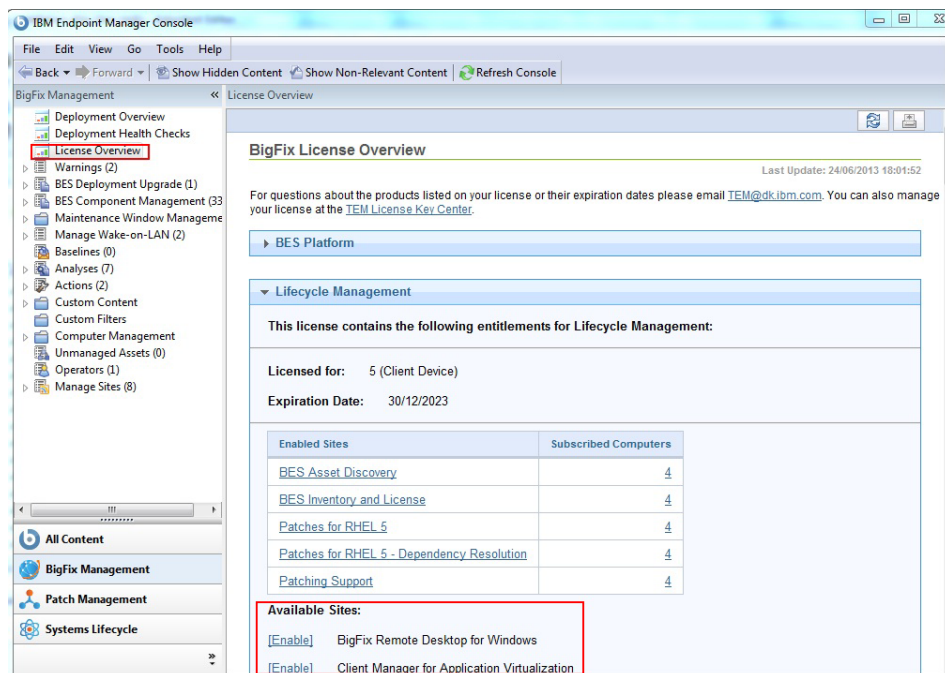


4. After installation, the program is automatically set up to subscribe to certain management and maintenance sites. Depending on the terms of your license, you might have subscriptions to other sites as well. In this way content from those Sites automatically flows into your enterprise and is evaluated for relevance on all computers running the Endpoint Manager client. Subscribe to these sites from the **BigFix Management** domain, by selecting the **License Overview** dashboard:



The License Overview dialog appears, listing available sites.

5. Enable the entitled sites by clicking the **Enable** button associated with the site to which you want to subscribe:



6. Enter your password to subscribe to the site. The new site is now listed in the **Manage Sites** node of the domain panel. You can also subscribe to a site by using a masthead file. For additional information see *Subscribing with a masthead* of the Console Guide.
7. Open the **Manage Sites** node and select your newly subscribed site.
8. From the site dialog, click the **Computer Subscriptions** tab to assign the site to the appropriate computers
9. From the **Operator Permissions** tab, select the operators you want to associate with this site and their level of permission.
10. Click Save Changes when you are done.



You can now use the product.

---

## Subscribing to Fixlet Sites

Sites are collections of Fixlet messages that are created internally by you, by IBM, or by 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. You can subscribe to a site also by using the Licensing Dashboard.

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 might include a set of 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 into 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 IBM Endpoint Manager client. These sites, in turn automatically register with an appropriate domain, providing a simple way to divide the content into functional sections.

### Subscribing with a Masthead

To subscribe to a site using a masthead file, 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 start 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 following ways:

- Double-click the masthead, or
- Select **Add External Site Masthead** from the **Tools** menu, browse the folder containing the masthead, and click **Open**.

2. You are prompted for your private key password. Type it in and click **OK**.

The masthead is propagated to all Clients, which immediately begin to evaluate the Fixlet messages from the new site.

## Subscribing with the Licensing Dashboard

You can subscribe to a Fixlet Site also by using the Licensing Dashboard in BigFix Management, found in the Domain Panel:

1. Open the **BigFix Management** domain and scroll to the top to view the associated dashboards.
2. From the **Licensing Dashboard**, select the sites you want to subscribe to.

---

## 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 and server network traffic. Relays work by:

- **Relieving downstream traffic.** The IBM Endpoint Manager server has many tasks, one of the most cumbersome being the distribution of 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 efficiency.
- **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, 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 IBM 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.

**Note:** A recommended configuration is the connection of 500 - 1000 clients to each relay and the use of a parent child relay configuration.

IBM Endpoint Manager is quite powerful; it is easy to deploy an action causing hundreds of thousands of clients to download very large files. 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 IBM 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 and 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, a relay uses minimal resources and does not have a noticeable impact on the performance of the computer running it. The IBM 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 IBM 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 the same time, 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:

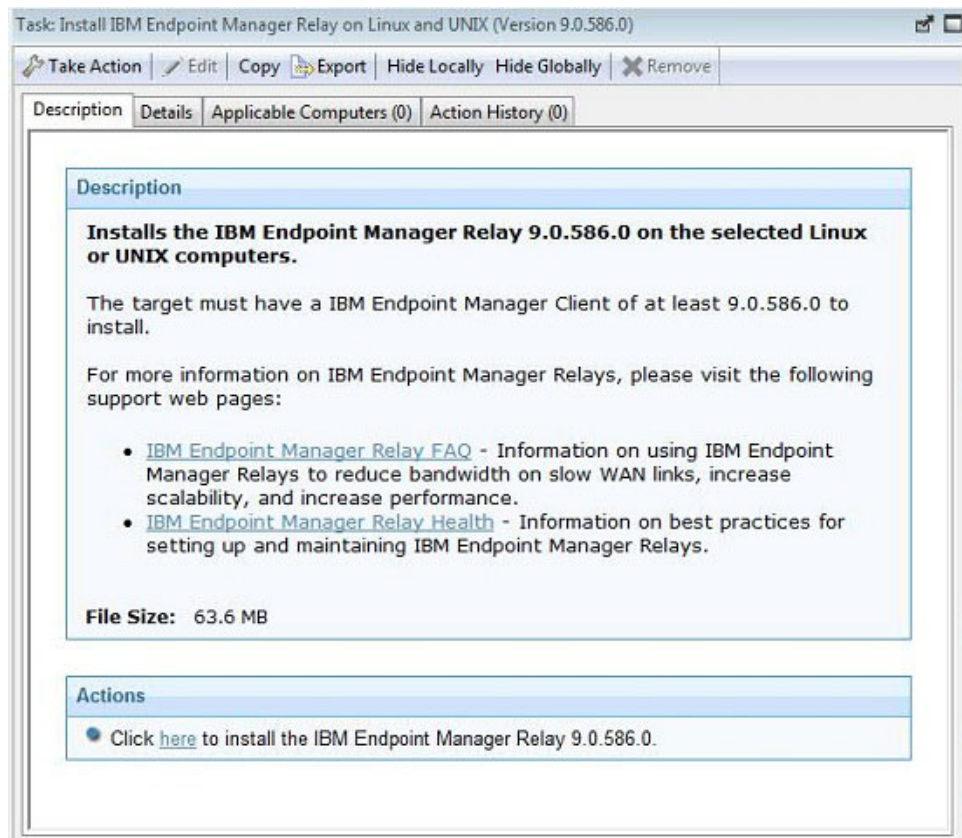
- The IBM Endpoint Manager relay must have a two-way TCP connection to its parent (which can be a server or another relay).
- The IBM Endpoint Manager relay can be installed on an ordinary workstation, but if many clients simultaneously download files, it might slow the computer down. Also, for the relay 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 IBM Endpoint Manager. Most companies already have partially used servers in the appropriate places throughout their networks. If you need to purchase a new computer for the task, the relay requirements are low.
- 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 IBM Endpoint Manager support site.

- The IBM Endpoint Manager relay cache size can be configured, 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 relays

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 IBM 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 click **Tasks Only** to see a list of all tasks.
2. Find the task with the title **Install IBM 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.



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 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 **Relay Selection Method**.
5. Click **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. Set this up by completing the following steps:

1. 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. Clear the **Expires On** box.
7. Click **OK**.

As new Clients are installed, they now automatically find and connect to the closest relay without any further action.

## Notes about Automatic Relay Discovery

The IBM 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 example, might indicate a problem with their relays.
- More information about relays, automatic relay selection, and troubleshooting relays can be found at the IBM Endpoint Manager support site.

## Assigning a relay when the server is unreachable

After you install the client, it connects to and registers with the main Endpoint Manager server.

After the client registers with the main server, a master operator can assign the client to a primary relay as well as configure it to fail over to a secondary relay if the primary relay becomes unavailable.

In some cases, when the client is installed, it might be unable to reach the main server directly across the local area network or Internet. For example, if the client workstation is in a remote office and cannot make a connection through the enterprise firewall to reach the main server. In this case you must set up a DMZ relay that has been given access through a hole in the firewall. For more information, see *Setting Internet Relays*.

You must also deploy the remote office client installer with a configuration file to set the client primary relay during installation. Specify the primary relay in the configuration file to register the client with a relay that it can connect to (such as the DMZ relay). For more information see *Assigning Relay at Client Installation Time*.

### Setting internet relays

You can configure your relays to manage clients that are only connected to the Internet without using VPN as if they were within the corporate network.

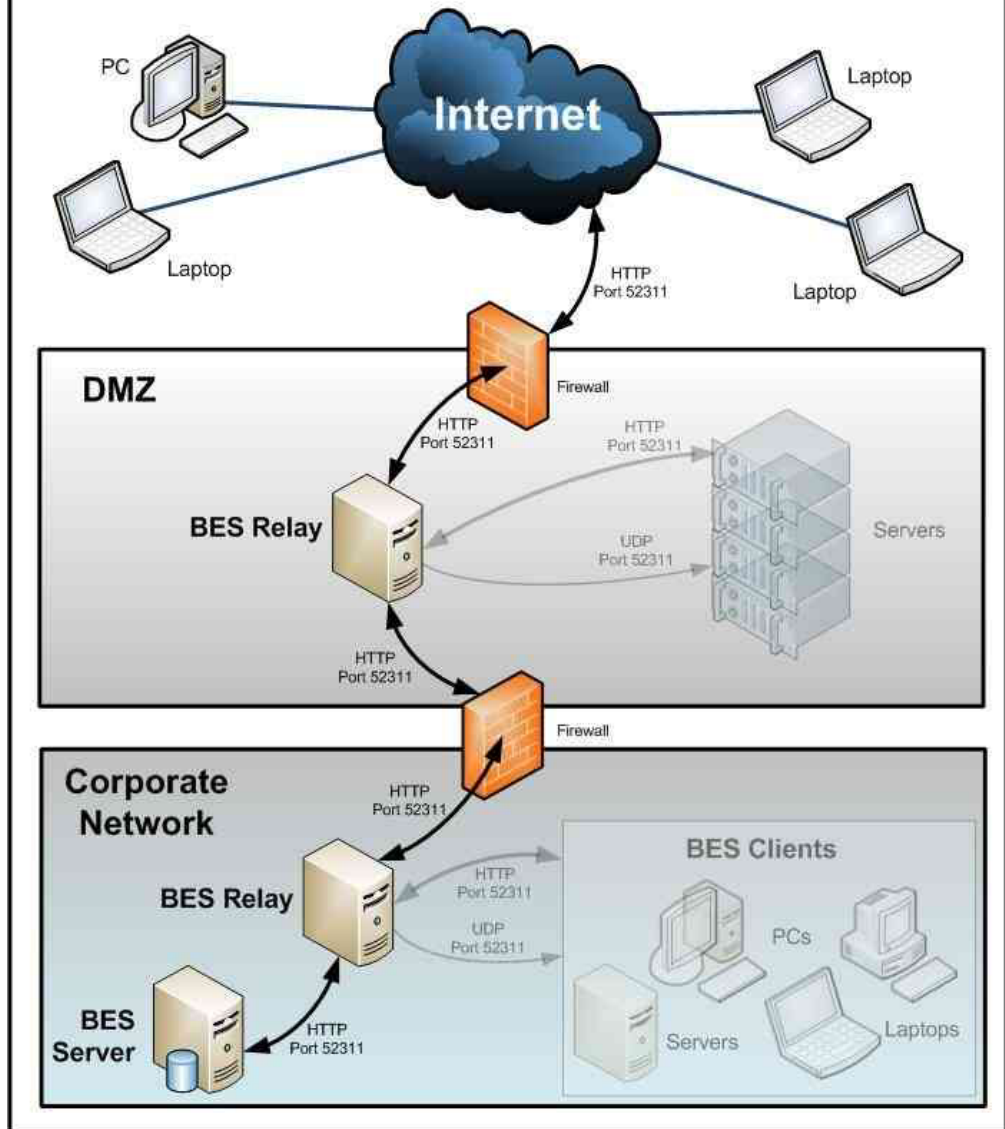
Using this approach, you can manage computers that are outside the corporate network (at home, in airports, at coffee shops, and so on.) using Endpoint Manager to:

- Report their updated properties and Fixlet status.
- Enforce new security policies defined by a Console operator.
- Accept new patch or application deployments.

This configuration is especially useful for managing mobile devices that might often be disconnected from the corporate network. The following picture shows a typical Internet-based relay, as it might exist in a DMZ network:



## Typical Internet-Based BES Relay Architecture



Setting up an Internet-facing relay enables external clients to find and connect to a relay. In our picture the clients can select the following types of relay:

- **Manual Relay Selection:** Clients can be configured using the console to manually select the Internet-facing relay DNS-alias (or IP address) as their primary, secondary, or failover relay. For more details about the failover relay setting see Configuration Settings.
- **Automatic Relay Selection:** If ICMP traffic has been allowed from the Internet to a DMZ-based Internet relay, then automatic relay selection can be leveraged to allow clients to find the closest relay as they move from location to location (either within a corporate network or on the Internet). For external clients on the Internet, the only relay they are able to find and connect to is the Internet-facing relay (because ICMP traffic from the Internet would be blocked to the relays within the corporate network).



**Note:** You can use the feature relay Affiliation to configure clients to find the most appropriate relay. For more details see Relay Affiliation

This is how the relays, clients, and firewalls are configured in a typical internet-based Endpoint Manager relay architecture:

1. A relay is deployed in a DMZ and the internal DMZ firewall allows only Endpoint Manager traffic (HTTP Port 52311) between the DMZ relay and a designated relay within the corporate network. The design above suggests bidirectional traffic as opposed to only allowing the Internet-facing relay to initiate network connections to the relay within the internal corporate network. This enables quicker client response times because immediate notifications of new content are made to the Internet-facing relay thus maintaining a real-time synchronization of content. If the bidirectional communication between the Internet-facing Endpoint Manager relay and the relay in the corporate network is not allowed, the Internet-facing relay must be configured to periodically poll its parent (the relay within the corporate network) for new content. For more details about configuring command polling see Configuration Settings .
2. After relay communication is established between the DMZ and the internal corporate network, the external firewall also has to be opened to allow Internet-based client traffic (HTTP port 52311) to reach the DMZ relay. In addition, allowing ICMP traffic through the external firewall to the Internet-facing relay can aid in the external client auto-relay selection process.
3. A DNS-alias (or IP address) is assigned to the relay that enables external clients to find the DMZ-based Internet relay. The DNS-alias must be resolvable to a specific IP address.
4. To make the relay aware of the DNS-alias (or IP address) deploy the BES Relay Setting: Name Override Fixlet to the DMZ-based Internet relay.
5. With the entire Endpoint Manager communication path established from the Internet through the DMZ-based Internet relay and ultimately to the main server, the next step depends on the various relay selection methods available in a given Endpoint Manager infrastructure.
6. Dynamic Policy Settings can be applied to Internet-based clients to allow for configurations better suited to external agents. For example, because the normal notification method (a UDP ping on port 52311) for new content might not reach external clients, dynamic settings can be used to have clients check for new content more frequently than the default period of 24 hours. For more information on setting up command-polling see <http://www-01.ibm.com/support/docview.wss?uid=swg21505846> .

**Note:** Disable the relay Diagnostics (<http://relayname:port/rd>) for Internet relays by setting the client setting `_BESRelay_Diagnostics_Enable` to zero.

## Assigning relay at client installation time

By default, the Endpoint Manager clients are configured to connect to the main Endpoint Manager server at installation time.

If you want you can configure the Endpoint Manager client to assign a specific Endpoint Manager relay at the time of client installation. Depending on the client operating system, you must perform different steps as described in the following topics:

- “Windows Clients” on page 104
- “UNIX Clients” on page 104
- “Mac Clients” on page 104

## Windows Clients:

Create a three line file called `clientsettings.cfg`, with the following content, and include this file in the Endpoint Manager client installation folder (`setup.exe`) to set a primary and backup relay:

```
IP:http://besrelayserver.domain.com:52311/bfmirror/downloads/  
__RelayServer1=http://relay.domain.com:52311/bfmirror/downloads/  
__RelayServer2=http://relay2.domain.com:52311/bfmirror/downloads/
```

**Note:** This technique does NOT work for the MSI version of the Endpoint Manager client installation package.

### *Adding More Settings:*

To add other client settings during the installation of the new client, include a line for each client setting to be set during client installation, for example, the file might look similar to:

```
__RelayServer1=http://relay.domain.com:52311/bfmirror/downloads/  
__BESClient_Inspector_ActiveDirectory_Refresh_Seconds=43200  
__BESClient_Log_Days=10  
...
```

For more information about the client settings you can set, see <http://www-01.ibm.com/support/docview.wss?uid=swg21506065>)).

## Mac Clients:

The `clientsettings.cfg` file is used also by the Mac client installer to create settings on the Mac client.

To set the relay, add the following lines to the `clientsettings.cfg` file:

```
IP:http://besrelayserver.domain.com:52311/bfmirror/downloads/  
__RelayServer1=http://relay.domain.com:52311/bfmirror/downloads/
```

Before running the installation, from the shell, add the `clientsettings.cfg` file to the Mac client installer package in `BESAgent.pkg/Contents/Resources`.

In the Finder, right-click `BESAgent.pkg` file and choose `Show Package Contents` to navigate within the package.

The installation package is created with the `BEAgent Installer Builder` app, which builds it into a read-only compressed `.dmg` file. If you need to edit the package, copy it out of this read-only disk image.

## UNIX Clients:

To assign a relay to your UNIX client at installation time, perform the following steps:

1. Create the `besclient.config` file under `/var/opt/BESClient/` with the following lines:

```
[Software\BigFix\EnterpriseClient]  
EnterpriseClientFolder = /opt/BESClient  
  
[Software\BigFix\EnterpriseClient\GlobalOptions]  
StoragePath = /var/opt/BESClient  
LibPath = /opt/BESClient/BESLib
```

```
[Software\BigFix\EnterpriseClient\Settings\Client\__RelayServer1]
effective date = [Enter current date and time in standard format]
value = http://relay.domain.com:52311/bfmirror/downloads/
```

```
[Software\BigFix\EnterpriseClient\Settings\Client\__RelayServer2]
effective date = [Enter current date time in standard format]
value = http://relay2.domain.com:52311/bfmirror/downloads/
```

```
[Software\BigFix\EnterpriseClient\Settings\Client\__RelaySelect_Automatic]
effective date = [Enter current date time in standard format]
value = 0
```

2. Ensure that the directory and file are owned by root and are not writable by anyone else. In this way, when you run the UNIX client installer to install the client, the installer does not re-create or overwrite /var/opt/BESClient/besclient.config with the following settings:

```
[Software\BigFix\EnterpriseClient]
EnterpriseClientFolder = /opt/BESClient
```

```
[Software\BigFix\EnterpriseClient\GlobalOptions]
StoragePath = /var/opt/BESClient
LibPath = /opt/BESClient/BESLib
```

3. In effective date = [Enter current date and time in standard format] set the date and time. An example of the standard format of the date and time is the following:

```
Wed, 06 Jun 2012 11:00:00 -0700
```

You cannot specify effective date = {now} because the {} brackets imply the use of inline relevance, and **now** is a keyword.

4. In value = http://relay.domain.com:52311/bfmirror/downloads/ modify relay.domain.com to be your desired relay.

**Tip:** You can obtain and verify the current content of the besclient.config by assigning a relay manually for a particular Linux client, and then copying the particular lines from its besclient.config file to use on other systems.

**Note:** For more information about troubleshooting clients that have problems in choosing an Endpoint Manager relay, see <http://www-01.ibm.com/support/docview.wss?uid=swg21506065>.

## 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 IBM 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 applies only 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
```

.

Set the client setting 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
```

Set also Client setting 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 used only 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 IBM Endpoint Manager. Observe the following naming rules:

- 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 IBM 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 the Console and select the **BigFix Management** Domain. From the Computer Management folder, click **Computers** 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 **OK** .

## 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 **Computers** to see a list of clients.
3. Look in 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 IBM 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 IBM Endpoint Manager support site.

## Monitoring relay health

IBM Endpoint Manager allows you to monitor your client and 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 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.

---

## Setting up a proxy connection

If your enterprise uses a proxy to access the Internet, you must set a proxy connection to enable the IBM Endpoint Manager server to gather content from sites.

The proxy connection is also used by the IBM Endpoint Manager server or a relay to do component-to-component communication or to download files.

The following configurations are the most common proxy configurations that you might need to set up:

**The IBM Endpoint Manager server must connect to the Internet through a proxy to gather content.**

To set this configuration, which is run on the server, complete the steps that are described in “Setting a proxy connection on the server” on page 110. On Windows systems, the debug tool informs you if the communication through a proxy does not work.

**Important:** Skipping this step would prevent your environment from working properly. A symptom of this misbehavior is that the site contents are not displayed on the console.

**A relay needs to connect to the Internet through a proxy to download files and to communicate with its parent relay.**

To set this configuration, which is run on the relay, complete the steps that are described in “Setting up a proxy connection on a relay” on page 112.

**A client needs to connect to the Internet through a proxy to communicate with its parent relay.**

To set this configuration, complete the following steps:

- Run on the relay the steps that are described in “Setting up a proxy connection on a relay” on page 112.
- Run on the client the steps that are described in “Setting up a proxy connection on a client or a child relay using the console” on page 112.

**A relay needs to connect to the Internet through a proxy to communicate with a child relay.**

To set this configuration, complete the following steps:

- Run on the parent relay the steps that are described in “Setting up a proxy connection on a relay” on page 112.
- Run on the child relay the steps that are described in “Setting up a proxy connection on a client or a child relay using the console” on page 112.

For information about the settings that you can use to configure your IBM Endpoint Manager environment, see configure the server in the knowledge base at the IBM Endpoint Manager support site.

**Note:** You can also maintain a physical disconnect from the Internet with an air-gapped implementation. For more information about this implementation, see “Downloading files in air-gapped environments” on page 128.

The steps to follow to configure the communication through a proxy are different depending on whether you set up the configuration for the first time on an IBM Endpoint Manager version 9.0 Patch 5 or on an earlier version.

The following tables list, for each component, the steps to complete to set up the proxy configuration on version 9.0 Patch 5 or later.

*Table 6. . Steps to configure communication through a proxy on an IBM Endpoint Manager server*

Server	
Linux	Windows

**Table 6. (continued).** Steps to configure communication through a proxy on an IBM Endpoint Manager server

Server	
<p>In the <code>besserver.config</code> file set, add the following keys:</p> <pre>Proxy ProxyUser ProxyPass ProxyExceptionList</pre> <p>For details, see “Setting a proxy connection on the server” on page 110.</p>	<p>Run the BESAdmin command as described in “Setting a proxy connection on the server” on page 110.</p>
or	
<p>Set the concatenated key</p> <pre>Proxy = [ProxyUser:ProxyPass@]hostname[:port]</pre> <p>as described in “Setting a proxy connection on the server” on page 110.</p>	

**Table 7. .** Steps to configure communication through a proxy on an IBM Endpoint Manager relay

Relay	
Linux and Windows	
To communicate with the parent component (relay or server):	To download files from the Internet:
<p>Set the client connection settings that are specified in “Setting up a proxy connection on a client or a child relay using the console” on page 112.</p> <p>Optionally, specify the <code>ProxyExceptionList</code> setting to specify local computers or domains that must be reached without using the proxy.</p>	<p>Set</p> <pre>_BESGather_Download_CheckInternetFlag = 1 _BESGather_Download_CheckParentFlag = 0</pre> <p>as described in “Setting up a proxy connection on a relay” on page 112.</p>

**Table 8. .** Steps to configure communication through a proxy on an IBM Endpoint Manager client

Client
Linux and Windows
<p>Set the client connection settings that are specified in “Setting up a proxy connection on a client or a child relay using the console” on page 112.</p> <p>Optionally, specify the <code>ProxyExceptionList</code> setting to specify local computers or domains that must be reached without using the proxy.</p>

**Note:** The configuration settings that are used in IBM Endpoint Manager version 9.0 Patch 5 or later do not use the `BESGatherService`, which is deprecated.

The configuration to communicate through a proxy might differ if you upgrade to version 9.0 Patch 5 or later an existing configuration. For example, in version 8.2 the `BESGatherService`, which is deprecated in version 9.X, was used to configure the communication through a proxy. If you upgrade your IBM Endpoint Manager version 8.2 environment to version 9.0 Patch 5 or later, your proxy configuration



continues to use the BESGatherService for backward compatibility. In this case, however, you cannot exploit the new features, for example ProxyExceptionList, until you use the proxy configuration that is supported by the r IBM Endpoint Manager version installed.

## Setting a proxy connection on the server

On the IBM Endpoint Manager server 9.0 Patch 5 or later, depending on which platform your sever is installed, you have the following behavior:

### On Windows systems:

The BES components that access the internet run, by default, as SYSTEM account on the Windows server.

The proxy configuration is managed in the registry by the key HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\Enterprise Server\Proxy.

Run the following command to create or modify the HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\Enterprise Server\Proxy key in the registry:

```
BESAdmin /setproxy /proxy:{hostname|IP_Address}[:port] /user:username  
/pass:password [/exceptionlist:exceptionlist]
```

### On Linux systems:

The BES components that access the internet run, by default, as root on the Linux server.

The proxy configuration is defined in the [SOFTWARE\BigFix\Enterprise Server\Proxy] section of the besserver.config file.

These are the values to specify when configuring the communication through a proxy:

**Proxy** = {hostname|IP\_address}[:port]

It is the hostname or IP address and, optionally, the port number of the proxy machine.

**ProxyUser** = username

It is the username that is used to authenticate with the proxy if the proxy requires authentication.

If you installed your IBM Endpoint Manager server on a Windows system and your proxy requires Kerberos Authentication, use the following syntax ProxyUser = *jdoe@example.com* replacing *jdoe@example.com* with your user and domain. The user that you specify must log in to the server and configure its Internet Options to use the proxy.

If you installed your IBM Endpoint Manager server on a Windows system and your proxy requires NTLM Authentication, use the following syntax ProxyUser = *jdoe* replacing *jdoe* with the NTLM user. If your proxy requires the domain/realm, the user may need to be specified as *jdoe@example.com* or as *domain/jdoe*. The user that you specify must log in to the server and configure its Internet Options to use the proxy.

If you installed your IBM Endpoint Manager server on a Linux system and your proxy requires NTLM Authentication, specify the NTLM user as *proxyuser*. On IBM Endpoint Manager on Linux the NTLM authentication does not work if FIPS is enabled.

**ProxyPass** = password

It is the password that is used to authenticate with the proxy if the proxy

requires authentication. The value that is assigned to the password is encrypted in the registry on Windows systems or obfuscated in the configuration file on Linux systems.

**ProxyExceptionList** = "hostname1, hostname2, IP\_Addr\_A, IP\_Addr\_B, domain\_Z, domain\_Y, ..."

This is an optional setting that you can use to specify computers, domains and subnetworks that must be reached without passing through the proxy.

Each name in this list is matched as either a domain, which contains the hostname, or the hostname itself. For example, example.com would match example.com, example.com:80, and www.example.com, but not www.notanexample.com.

Examples:

```
ProxyExceptionList = example.com
ProxyExceptionList = example.com,8.168.117.0
ProxyExceptionList = "example.com, 8.168.117.0"
```

To prevent diverting internal communications towards the proxy agent, specify the following value in the **ProxyExceptionList** key:

```
ProxyExceptionList = "localhost, 127.0.0.1"
```

The setting **ProxyExceptionList** was introduced in version 9.0.835.0 (Patch 5) for Windows and Linux systems. If you are using IBM Endpoint Manager version 9.0 and you have problems using content that downloads files from the local server, upgrade to IBM Endpoint Manager version 9.0.835.0.

On IBM Endpoint Manager version 8.1, 8.2, and 9.0 for builds earlier than 9.0.835.0, the proxy settings are picked up from the Internet Explorer proxy settings.

**Important:** Ensure that you restart the BESRootServer component on the server after you create or modify the settings to communicate through a proxy.

Examples:

1. This example uses a concatenated key notation to specify the proxy settings:

```
[Software\BigFix\Enterprise Server\Proxy]
Proxy = [proxyuser:password@]{hostname|IP_address}[:port]
```

2. This example defines the communication through a non-authenticating proxy:

```
[Software\BigFix\Enterprise Server\Proxy]
Proxy = hostname:port
```

3. This example shows how to exclude from the communication through the proxy:

- The IBM Endpoint Manager client that is installed on the system where you are defining the proxy connection.
- The host with IP address **8.168.117.0**.
- The hosts that belong to the domain **example.com**.

```
[Software\BigFix\Enterprise Server\Proxy]
Proxy = username:password@hostname
ProxyExceptionList = "localhost, 127.0.0.1, 8.168.117.0, example.com"
```

For more information about proxy configuration, see Proxy Server Settings.

## Setting up a proxy connection on a relay

On the system where the relay is installed, run the following steps to allow the relay to communicate with its parent components:

1. Open the console and go to **Computer** section under the **All Content** domain.
2. Select the computer where the relay is installed.
3. Right-click the computer and select **Edit Settings**.
4. Select **Add** to create custom settings.
5. Enter the **Setting Name** and **Setting Value** listed in Table 9 on page 113.
6. Click **OK** to send out the configuration settings, which take effect immediately.

Specify the setting: **ProxyExceptionList** = "*hostname1, hostname2, IP\_Addr\_A, IP\_Addr\_B, domain\_Z, domain\_Y, ...*" if the relay must communicate to its parent relays without passing through the proxy. Depending on which platform the relay is installed, add this setting:

### On Windows systems:

In the registry in the HKEY\_LOCAL\_MACHINE\SOFTWARE\BigFix\Enterprise Server\Proxy key.

### On Linux systems:

In the besrelay.config file in the [SOFTWARE\BigFix\Enterprise Server\Proxy] section.

Run the following steps if you want to allow your relay to download files through the proxy:

1. Open the console and go to **Computer** section under the **All Content** domain.
2. Select the computer where the relay is installed.
3. Right-click the computer and select **Edit Settings**.
4. Select **Add** to create the following custom settings:  
`_BESGather_Download_CheckInternetFlag = 1`  
`_BESGather_Download_CheckParentFlag = 0`
5. Click **OK** to send the configuration settings, which take effect immediately.

**Note:** If the relay is installed on a Linux platform, the configuration file in which the settings are stored is called besrelay.config.

## Setting up a proxy connection on a client or a child relay using the console

If a client or a relay must communicate through a proxy with its parent component (relay or server) for Internet requests and for component-to-component communication, set the proxy connection on that system as follows:

1. Open the console and go to **Computer** section under the **All Content** domain.
2. Select the computer where the client or the child relay is installed.
3. Right-click the computer and select **Edit Settings**.
4. Select **Add** to create a custom setting.
5. Enter the **Setting Name** and **Setting Value** from the configuration table below:

Table 9. Proxy client configuration settings

Setting Name	Setting Value	Details
_Enterprise Server _ClientRegister _ProxyServer	Sets the hostname that is used to reach the proxy.	Default Value: None Setting Type: String Value Range: N/A Task Available: No
_Enterprise Server _ClientRegister _ProxyPort	Sets the port that is used by the proxy server.	Default Value: None Setting Type: String Value Range: N/A Task Available: No
_Enterprise Server _ClientRegister _ProxyUser	Sets the user name that is used to authenticate with the proxy if the proxy requires authentication.	Default Value: None Setting Type: String Value Range: N/A Task Available: No
_Enterprise Server _ClientRegister _ProxyPass	Sets the password that is used to authenticate with the proxy if the proxy requires authentication.	Default Value: None Setting Type: String Value Range: N/A Task Available: No

6. Click **OK** to make the setting active.

Depending on which platform the computer is installed, the following settings are stored:

**On Windows systems:**

In the registry.

**On Linux systems:**

In the `besclient.config` file if you configured a client; in the `besrelay.config` file if you configured a child relay.

All notifications to clients use the UDP protocol, which a standard proxy does not forward. If there is a proxy between the client and a relay, configure upstream communication on the client with the following settings:

Table 10. Proxy client polling configuration settings

Setting Name	Setting Value	Details
_BESClient_Comm _CommandPollEnable	Enables the client to poll its parent relay for new actions.	Default Value: 0 (disabled) Setting Type: Boolean Value Range: 1 (enable), 0 (disable) Task Available: Yes
_BESClient_Comm _CommandPollInterval Seconds	Determines how often the client checks with its parent relay for gathering or refresh of content if <code>_BESClient_Comm_CommandPollEnable</code> is enabled. To prevent performance degradation avoid specifying settings that are less than 900 seconds.	Default Value: 900 Setting Type: Numeric (seconds) Value Range: 0-4294967295 Task Available: Yes

If you set this configuration, the client queries its relay for new instructions instead of waiting for the UDP ping regarding new actions.

## Best practices to consider when defining a proxy connection in version 9.0

Consider the following tips and tricks to avoid common problems:

- Starting from version 9.0 the use of the BESGather service is deprecated. However if you use it, ensure that you define the user account exploited by your proxy configuration as follows:

**Provision a single user account that has both domain administrator and local administrator rights to the IBM Endpoint Manager server machine.**

Reason: The BESRootServer.exe process needs to have local administrator rights to the server machine to properly propagate site content from the database to the server's file system. The BESRootServer.exe needs to have domain administrator rights to negotiate all the LDAP transactions between the console and Active Directory to authenticate users.

**Ensure that the user account also has permission to make requests through the proxy to the Internet as a service account.**

Reason: The BESRootServer.exe service gathers the site content from public content and site servers.

**Ensure that the user has Database Owner (DBO) rights to the BFEnterprise database.**

Reason: The user needs to access the BFEnterprise and BESReporting databases as owner with DBO rights.

Use this userid to log in with BES Root Server and BES Gather services.

- After you set the communication through the proxy on a Windows server, use the IBM Endpoint Manager Diagnostic Tools to verify that the server, still reported as BESGatherService, can successfully reach the Internet.
- Check the GatherDB.log file that is located in the BES Server\GatherDBData folder to verify that the server can gather from the Internet.
- Check in the firewall rules if there are any file types that are blocked. In this case, if the content to gather from a site contains at least one file with this file type, then the entire content of that site is not gathered.
- Ensure that the password specified in ProxyPass on the server, or in \_Enterprise Server\_ClientRegister\_ProxyPass on the client or relay has not expired.
- Make sure that the proxy allows the downloading of arbitrary files from the Internet (for example, it does not block .exe downloads or does not block files with unknown extensions).
- Most of files in IBM Endpoint Manager are downloaded from bigfix.com or microsoft.com using HTTP port 80, but it is recommended that you allow the proxy service to download from any location using HTTP, HTTPS, or FTP because there are some downloads that use these protocols.
- On Windows systems, verify whether Internet Explorer can reach the Internet using the credentials that are specified in the IBM Endpoint Manager proxy configuration, and test the connectivity with the esync.bigfix.com servers (for example, <http://esync.bigfix.com/cgi-bin/bfgather/bessupport>).
- Make sure that the proxy is bypassed for internal network and component-to-component communications because this might cause problems with how the IBM Endpoint Manager server works and is inefficient for the proxy. Use the **ProxyExceptionList** setting, if needed, to exclude local systems from the communication through the proxy.
- The setting ProxyExceptionList was introduced in IBM Endpoint Manager version 9.0.835.0 for Windows and Linux systems. If you are using IBM Endpoint Manager version 9.0 and you have problems using content that downloads files from the local server, upgrade to IBM Endpoint Manager version 9.0 Patch 5 (9.0.835.0).

- By default the HTTP and HTTPS connections time out after 10 seconds, DNS resolution time included. When this happens the HTTP 28 error is logged. In your environment, if the proxy server or the DNS server takes a longer time to establish the TCP connection, you can increase the number of seconds before the connection times out by editing the setting `_HttpRequestSender_Connect_TimeoutSecond`. The `_HttpRequestSender_Connect_TimeoutSecond` setting affects all the IBM Endpoint Manager, including the Console and the Client, running on the machine for which this setting is set. No other IBM Endpoint Manager component running on other machines in the deployment is affected by the setting. As a best practice, be careful when increasing the value of this setting and try to keep it as low as possible to avoid opening too many sockets concurrently risking socket exhaustion and eventual loss of service.

---

## Managing operators and permissions

There are three basic classes of users and each of them has different responsibilities and restrictions.

### Site Administrator

Installs and maintains the software, including the IBM Endpoint Manager Server, Console, and Client programs. The site administrator cannot create operators. The site administrator has administrative access to the Server computer as well as access and the password to the site-level signing keys. For more information, see “Site administrator responsibilities.”

### Master Operators

Have access to all IBM Endpoint Manager computers and the authority to create and manage the other console operators. Any master operator can create, distribute, and revoke publisher keys and management rights that allow console operators to deploy actions. For more information, see “Operators permissions” on page 116.

### Operators

Manage the day-to-day operations of IBM Endpoint Manager, including Fixlet management and action deployment, typically on a subset of computers subject to the management rights assigned by the master operator. For more information, see “Operators permissions” on page 116.

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.

**Note:** When you define an operator, ensure that the user name does not contain any of the following characters: `:`, `@`, and `\`.

## Site administrator responsibilities

The site administrator has the following primary responsibilities:

### Obtaining and securing the Action Site Credentials

To install IBM Endpoint Manager, the site administrator must generate a private key, receive a license certificate from IBM, and create a masthead with the digital signature and configuration information. This is a special key and must be used only for site-level tasks such as:

- Setting global system options

- Editing Mastheads
- Administering Distributed Server Architecture (DSA)

For day-to-day console operations, the site administrator must create a master operator key.

### Preparing the Server

The IBM Endpoint Manager Server must be correctly set up to communicate externally with the Internet and internally with the Clients. The Server also needs to be configured to host the IBM Endpoint Manager database (or another computer can be used as the SQL Server database).

### Installing the various components

The site administrator installs the IBM Endpoint Manager Client, Server, Relay, and Console modules.

### Maintaining the Server

The IBM Endpoint Manager server runs an SQL Server database and several specific services. Standard maintenance tasks such as upgrades or fixes are managed using Fixlet technology or can be performed manually by the site administrator.

## Operators permissions

The master operator creates other operators and assigns permissions to them from the IBM Endpoint Manager console. The authorizations associated to an operator are set in the Permissions area of the Details tab of the operator's description.

Permissions		
	Explicit Permissions	Effective Permissions
Master Operator	No	No
Show Other Operators' Actions	Yes	Yes
Custom Content	Yes	Yes
Unmanaged Assets	Show All	Show All

This table associates the activities that an operator can perform with the type of operator:

Table 11. Master operator and operator authorizations

Activities	Master Operator	Operator
Initialize Action Site	Yes	No
Manage Fixlet Sites	Yes	No
Change Client heartbeats	Yes	No
Create Fixlets	If Custom Content is set to YES	If Custom Content is set to YES
Create Tasks	If Custom Content is set to YES	If Custom Content is set to YES
Create Analyses	If Custom Content is set to YES	If Custom Content is set to YES
Create Baselines	If Custom Content is set to YES	If Custom Content is set to YES
Create Groups	Yes	Manual Groups Only



Table 11. Master operator and operator authorizations (continued)

Activities	Master Operator	Operator
Activate/Deactivate Analyses	All	Administered
Take Fixlet/Task/Baseline Action	All	Administered
Take Custom Action	If Custom Content is set to YES	If Custom Content is set to YES
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	Administered
View Actions	All	Administered
Make Comments	All	Administered
View Comments	All	Administered
Globally Hide/Unhide	Yes	No
Locally Hide/Unhide	Yes	Yes
Use Wizards	If Custom Content is set to YES	If Custom Content is set to YES
Remove computer from database	All	Administered
Create Manual Computer Groups	Yes	Yes
Delete Manual Computer Groups	Yes	No
Create Automatic Computer Groups	Yes	If Custom Content is set to YES
Delete Automatic Computer Groups	Yes	If Custom Content is set to YES 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 console.		

## 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.

## Adding console operators

The master operator can add operators at any time by launching **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Console**.

These are the types of operators that can be created:

- Local operator (local IBM Endpoint Manager account). For information about how to add local operators, see *Adding Local Operators*.
- LDAP operator (operator whose credentials are authenticated via Active Directory or LDAP). For information about how to add LDAP operators, see *Adding LDAP Operators*.
- LDAP Group to a role. For information about how to assign a LDAP group to an existing role, see *Associating an LDAP group*.
- IBM Endpoint Manager server running on a Red Hat Enterprise Linux 6 system can integrate with an Active Directory. As a consequence, you can add as operators, users defined in the Active Directory domain. To run the integration, configure the Kerberos protocol as described in *Configuration 4 – Kerberos/LDAP of Integrating Red Hat Enterprise Linux 6 with Active Directory*.

**Note:** For LDAP operator and LDAP Group, you must first add an Active Directory or LDAP domain to IBM Endpoint Manager.

For information about additional operations that can be run against operators, see the *IBM Endpoint Manager Console Operator's guide*.

## Integrating Linux Server with Active Directory

You can integrate the Linux Endpoint Manager server with Active Directory using the Kerberos protocol, downloaded as a prerequisite with the Linux Endpoint Manager server installation.

These are the steps to integrate the Linux Endpoint Manager server with the Windows Active Directory domain using LDAP with Kerberos authentication:

1. Install and configure the NSS and PAM libraries
2. Configure the Kerberos LDAP security and authentication
3. Modify the local LDAP name

### Installing and configuring the NSS and PAM libraries

Ensure that the following NSS and PAM packages are installed:

```
nss-pam-ldapd-0.7.5-18.2.el6_4.x86_64.rpm  
pam_krb5-2.3.11-9.el6.x86_64.rpm
```

**Note:** If you have a valid RHN subscription, run yum as shown in the following example:

```
yum install nss-pam-ldapd.x86_64 pam_krb5.x86_64
```

### Configuring the PAM library:

To configure the PAM libraries, edit the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` files and add the `pam_krb5.so` library entries:

```
auth      sufficient                                pam_krb5.so use_first_pass
...
account   [default=bad success=ok user_unknown=ignore] pam_krb5.so
...
password  sufficient                                pam_krb5.so use_authtok
...
session   optional                                  pam_krb5.so
```

**Note:** Remove the entries for the SSSD libraries (`pam_sss.so`).

### Configuring the NSS library:

To use the LDAP database to authenticate users on a Linux system edit the `/etc/nsswitch.conf` and change `passwd`, `shadow` and `group` entries from the SSSD daemon (`sss`) to LDAP:

```
passwd: files sss
shadow: files sss
group:  files sss
```

to LDAP (**ldap**):

```
passwd: files ldap
shadow: files ldap
group:  files ldap
```

For additional information on RedHat integration see Integrating Red Hat Enterprise Linux 6 with Active Directory

## Configuring Authentication

To configure the Kerberos protocol, the LDAP security and the authentication files for Active Directory integration, you can use one of the following methods:

- **system-config-authentication** graphical tool
- **authconfig** command-line tool

### Using the system-config-authentication graphical tool:

To configure the authentication with the `system-config-authentication` tool, perform the following steps:

1. Run the **system-config-authentication** graphical tool to define LDAP as the user account database for user authentication.
2. In **Identity & Authentication**, from the **User Account Database** drop-down list, select **LDAP**. Selecting the **LDAP** option allows the system to be configured to connect to the Windows Active Directory domain using LDAP with Kerberos authentication.

**Authentication Configuration**

**Identity & Authentication** | Advanced Options

**User Account Configuration**

User Account Database: LDAP

LDAP Search Base DN: dc=tem,dc=test,dc=co

LDAP Server: ldap://winserver.tem.test.com

☐ Use TLS to encrypt connections

Download CA Certificate...

**Authentication Configuration**

Authentication Method: Kerberos password

Realm: TEM.TEST.COM

KDCs: winserver.tem.test.com:88

Admin Servers: winserver.tem.test.com:749

☐ Use DNS to resolve hosts to realms

☐ Use DNS to locate KDCs for realms

Revert Cancel Apply

3. In **LDAP Search Base DN** specify to retrieve the user information using the listed Distinguished Name (DN), such as dc=tem,dc=test,dc=com.
4. In **LDAP Server** specify the address of the LDAP server such as ldap://winserver.tem.test.com
5. In **Authentication Method** select **Kerberos password**.

6. Configures the realm for the Kerberos server in **Realm**, such as TEM.TEST.COM
7. Specify the *Key Distribution Center* (KDC) in **KDCs** for issuing Kerberos tickets, for example, winserver.tem.test.com
8. Specify the administration servers running kadmind in the **Admin Servers**, such as winserver.tem.test.com
9. Click **Apply**.

For more information about how to use this tool, see *Launching the Authentication Configuration Tool UI*.

### Using the **authconfig** command-line tool:

To update all of the configuration files and services required for system authentication, you can run the **authconfig** command-line tool, as shown in the following example:

```
authconfig --enableldap --ldapserver=ldap://winserver.tem.test.com:389
--ldapbasedn="dc=tem,dc=test,dc=com" --enablekrb5
--krb5realm TEM.TEST.COM --krb5kdc winserver.tem.test.com:88
--krb5adminserver winserver.tem.test.com:749 --update
```

where:

#### **--enableldap**

Specifies to configure to connect the system with the Windows Active Directory domain using LDAP with Kerberos authentication.

#### **--ldapserver**

Specifies the address of the LDAP server such as ldap://winserver.tem.test.com

#### **--ldapbasedn**

Specifies to retrieve the user information using the listed Distinguished Name (DN), such as dc=tem,dc=test,dc=com

#### **--enablekrb5**

Enables the Kerberos password authentication method.

#### **--krb5realm**

Configures the realm for the Kerberos server, such as TEM.TEST.COM.

#### **--krb5kdc**

Specifies the *Key Distribution Center* (KDC) for issuing Kerberos tickets, such as winserver.tem.test.com.

#### **--krb5adminserver**

Specifies the administration servers running kadmind, such as winserver.tem.test.com.

#### **--update**

Applies all the configuration settings.

For more information about how to use this command, see *Configuring Authentication from the Command Line*.

## Modifying the local LDAP name

To modify the local LDAP name, perform the following steps:

1. Make a backup copy of the LDAP configuration file as follows:

- ```
cp -p /etc/nsld.conf /etc/nsld.conf.bk
```
2. Modify the value of the base and uri settings in the /etc/nsld.conf file as in the following example:

```
base dc=tem,dc=test,dc=com
uri ldap://winserver.tem.test.com
```
  3. Restart the local LDAP name service daemon:

```
service nsld restart
```
  4. Ensure that the local LDAP name service daemon (nsld) is set to start with the server:

```
chkconfig nsld on
```

---

## Managing Replication (DSA) on Windows systems

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 IBM Endpoint Manager Administration Tool. Here you can see the current settings for your servers and make the appropriate changes.

### Changing the replication interval on Windows systems

1. Start up the **IBM 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 on Windows systems

By default, server 0 (zero) is the master server. The Administration Tool allows you to perform certain administrative tasks (such as creating and deleting users) only 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 **IBM Endpoint Manager Administration Tool**.
2. Select the **Advanced Options** tab and click **Add**.
3. Type **masterDatabaseServerID** as the name, and then enter the other server ID as the value.
4. Click **OK**.

After the value has successfully replicated to the new server, it becomes the 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 Windows 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:

```
call dbo.delete_replication_server(n)
```

where *n* is the identifier of the server to delete.

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 IBM Endpoint Manager support site.

---

## Managing Replication (DSA) on Linux systems

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 `iem` command line. Here you can see the current settings for your servers and make the appropriate changes.

### Changing the replication interval on Linux systems

To change the replication interval, perform the following steps:

1. From the `/opt/BESServer/bin` command prompt, start the command line:  

```
./iem login --server=servername:serverport --user=username  
--password=password
```
2. From the `/opt/BESServer/bin` command prompt, run the following command:  

```
./iem get replication/server/0 > /appo/replicationServer0.xml
```
3. In the `/appo/replicationServer0.xml` file, edit the following keyword:  

```
<ReplicationIntervalSeconds>300</ReplicationIntervalSeconds>
```

to change the value in seconds of the replication interval. Using longer replication intervals means that the servers replicate data less often, but have more data to transfer each time.

```
<?xml version="1.0" encoding="UTF-8"?>  
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
        xsi:noNamespaceSchemaLocation="BESAPI.xsd">  
  <ReplicationServer Resource="http://9.87.126.68:52311/api/replication  
    /server/0">  
    <ServerID>0</ServerID>  
    <URL>http://nc926068.romelab.it.ibm.com:52311</URL>  
    <DNS>nc926068.romelab.it.ibm.com</DNS>  
    <ReplicationIntervalSeconds>300</ReplicationIntervalSeconds>  
    <ReplicationLink Resource="http://9.87.126.68:52311/api/replication  
      /server/0/link/3">  
      <SourceServerID>0</SourceServerID>  
      <DestinationServerID>3</DestinationServerID>  
      <Weight>1</Weight>  
      <IsConnected>0</IsConnected>  
      <LastReplication>Fri, 01 Mar 2013 11:17:12 +0000  
      </LastReplication>  
      <LastError>19NoMatchingRecipient - Fri, 01 Mar 2013 11:17:12 +0000  
      </LastError>
```



```

</ReplicationLink>
<ReplicationLink Resource="http://9.87.126.68:52311/api/replication/server/
3/link/0">
    <SourceServerID>3</SourceServerID>
    <DestinationServerID>0</DestinationServerID>
    <Weight>1</Weight>
    <IsConnected>1</IsConnected>
    <LastReplication>Fri, 01 Mar 2013 11:17:18 +0000
    </LastReplication>
</ReplicationLink>
</ReplicationServer>
</BESAPI>

```

4. Upload the modified file by running the following command:  
`./iem post /appo/replicationServer0.xml replication/server/0`

## Switching the master server on Linux systems

By default, server 0 (zero) is the master server. To switch the master to another server, set the deployment option **masterDatabaseServerID** to the other server ID as follows:

1. From the /opt/BESServer/bin command prompt, start the command line:  
`./iem login --server=servername:serverport --user=username --password=password`
2. From the /opt/BESServer/bin command prompt, run the following command:  
`./iem get admin/fields > /appo/switchmaster.xml`
3. In the /appo/switchmaster.xml file, add or edit the following keyword and its value:

```

<Name>masterDatabaseServerID</Name>
<Value>0</Value>

```

to switch the master server to another master server:

```

<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="BESAPI.xsd">
    <AdminField Resource="http://9.87.126.68:52311/api/admin/field
/masterDatabaseServerID">
        <Name>masterDatabaseServerID</Name>
        <Value>3</Value>
    </AdminField>
</BESAPI>

```

4. Upload the modified file by running the following command:  
`./iem post /appo/switchmaster.xml admin/fields`

After the value has successfully replicated to the new server, it become the 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.

## Uninstalling a Linux 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:

```
call dbo.delete_replication_server(n)
```

where  $n$  is the identifier of the server to delete.

---

## HTTPS Configuration

To provide more security to Web Reports, you can use HTTPS. First, you need to request a Secure Socket Layer (SSL) certificate from a vendor such as Verisign, and then you need to set its location.

To register a certificate, you need a valid configuration file such as the following one:

```
[ req ]
default_bits = 1024
default_keyfile = keyfile.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
prompt = no
output_password = mypasswd
[ req_distinguished_name ]
C = US
ST = California
L = City
O = BigCo
OU = Development
CN = Common
emailAddress = janedoe@bigco.com

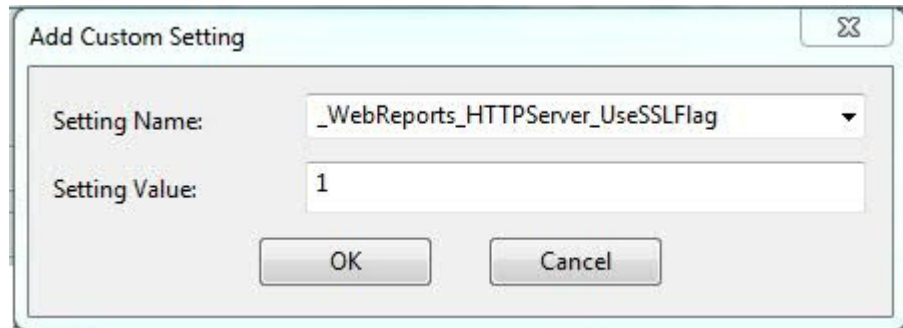
[ req_attributes ]
challengePassword = bigcopasswr
```

To use HTTPS:

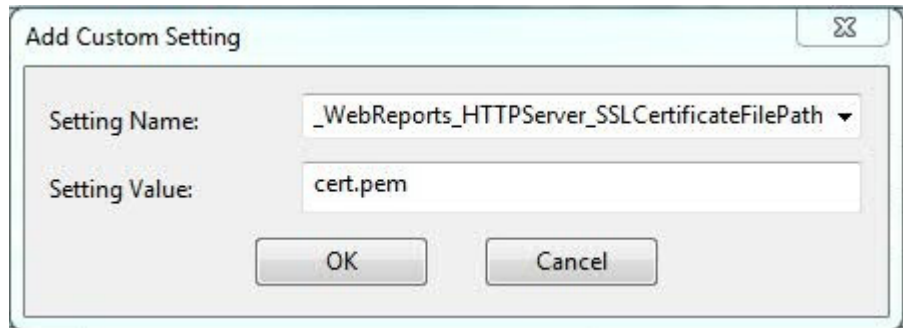
1. Install OpenSSL if it is not already available.
2. Save your configuration file as something like `mynewconfig.conf`, and issue your certificate request. This also generates a private key (in the file named `keyfile.pem`). On Windows you can use this command:  
`openssl req -new -config "mynewconfig.conf" > cert.csr`
3. Remove the password from your private key file:  
`openssl rsa -in keyfile.pem -out nopwdkey.pem`
4. Create a certificate file:  
`openssl x509 -in cert.csr -out cert.pem -req -signkey nopwdkey.pem -days 365`
5. Open `nopwdkey.pem` in a text viewer, copy the contents, and paste them below the certificate in `cert.pem`.
6. Save this file; it is your SSL certificate.

Next, you need to store the path for this file and add or modify sub-keys for the HTTPS flag, for the location of the SSL certificate, for the HTTPS port number, for a listening for HTTP connections and for redirecting the client to HTTPS on the SSL port as follows:

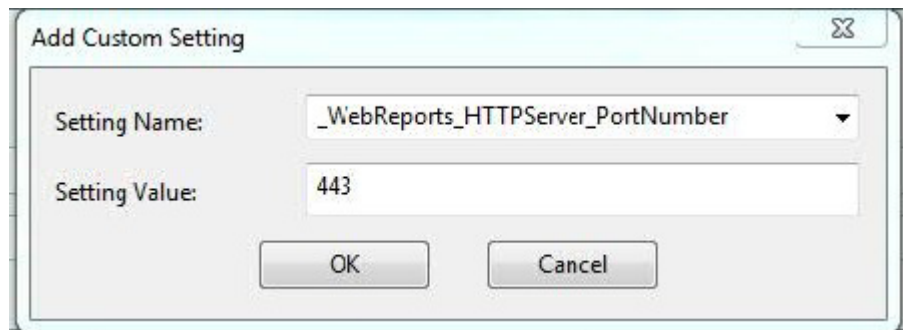
1. From the Endpoint Manager Console select the **Computers** tab.
2. Select the computer to configure and **Edit Computer Settings** from the **Edit** menu.
3. Look for **\_WebReports\_HTTPServer\_UseSSLFlag** setting. If it exists, do not create a second one, but edit its value to 1 to enable HTTPS. If it does not exist, add it:



4. Look for **\_WebReports\_HTTPServer\_SSLCertificateFilePath** setting. If it exists, do not create a second one, but edit its value to the full path name of the SSL certificate (cert.pem). If it does not exist, add it:



5. Look for **\_WebReports\_HTTPServer\_PortNumber**. If it exists, do not create a second one, but edit its value to the port number you would like to use (typically 443). If it does not exist, add it:



6. When SSL is enabled define the forwarding port by setting the following:  
 \_WebReports\_HTTPRedirect\_Enabled to 1 and  
 \_WebReports\_HTTPRedirect\_PortNumber to the port listening for HTTP connection and redirecting the client to HTTPS.
7. Restart the **BESWebReports** service.  
 On Windows, open **Services**, select **BESWebReports** and on the **Action** menu, click **Restart**.  
 On Linux run from the prompt: service beswebreports restart or /etc/init.d/beswebreports restart

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 intervention. If the certificate does not meet the trust

requirements of the browser, then you are prompted with a dialog asking if it is OK to proceed with the connection, and giving you access to information about the certificate.

Typically, a trusted certificate is one that 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 from your CA. If you do not require authentication back to a trusted root, you can also generate a self-signed certificate using OpenSSL utilities.

## Configuring HTTPS manually on Windows systems

When you have an SSL certificate (a .pem file), place it on the computer running Web Reports (usually the server) and follow these steps:

1. Run **regedit** and locate HKEY\_LOCAL\_MACHINE\Software\BigFix\EnterpriseClient\Settings\Client for x32 systems and HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\BigFix\EnterpriseClient\Settings\Client x64 systems.  
You need to add or modify subkeys for the HTTPS flag, for the location of the SSL certificate, for the HTTPS port number, and for the redirection to HTTPS.
2. Create a subkey of **Client** called `_WebReports_HTTPServer_UseSSLFlag` (it might already exist).
3. Create a string value (reg\_sz) for the key `_WebReports_HTTPServer_UseSSLFlag` called **value** and set it to 1 to enable HTTPS.
4. Create a subkey of **Client** called `_WebReports_HTTPServer_SSLCertificateFilePath` (it might already exist).
5. Create a 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 subkey of **Client** called `_WebReports_HTTPServer_PortNumber` (it might already exist).
7. Create a string value (reg\_sz) for the key `_WebReports_HTTPServer_PortNumber` called **value** and set it to the port number you want to use (typically 443).
8. Create a subkey of **Client** called `_WebReports_HTTPRedirect_Enabled` (it might already exist).
9. Create a string value (reg\_sz) for the key `_WebReports_HTTPRedirect_Enabled` called **value** and set it to 1 to enable the browser redirection to HTTPS.
10. Create a subkey of **Client** called `_WebReports_HTTPRedirect_PortNumber` (it might already exist).
11. Create a string value (reg\_sz) for the key `_WebReports_HTTPRedirect_PortNumber` called **value** and set it to the number of the port listening for HTTP connection and redirecting the client to HTTPS.
12. Restart the **BESWebReports** service.

## Configuring HTTPS manually on Linux systems

When you have an SSL certificate (a .pem file), place it on the computer running Web Reports and customize the keywords in the `besclient.config` file if a client is installed together with Web Reports or in the `beswebreports.config` file if only Web Reports is installed.

To define the port number you want to use:

```
[Software\BigFix\EnterpriseClient\Settings\Client
\WebReports_HTTPServer_PortNumber]
value = 443
```

To define the full path name of the SSL certificate (cert.pem):

```
[Software\BigFix\EnterpriseClient\Settings\Client
\WebReports_HTTPServer_SSLCertificateFilePath]
value = /tmp/CERT/cert.pem
```

To enable HTTPS:

```
[Software\BigFix\EnterpriseClient\Settings\Client
\WebReports_HTTPServer_UseSSLFlag]
value = 1
```

To enable client redirection from an HTTP connection to an HTTPS connection:

```
[Software\BigFix\EnterpriseClient\Settings\Client
\WebReports_HTTPRedirect_Enabled]
value = 1
```

To define the number of the port listening for the HTTP connection and redirecting the Client to HTTPS:

```
[Software\BigFix\EnterpriseClient\Settings\Client
\WebReports_HTTPRedirect_PortNumber]
value = portnumber
```

---

## Downloading files in air-gapped environments

In an air-gapped environment where a secure network is physically isolated from insecure networks, such as the public Internet or an insecure local area network, and the computers on opposite sides of the air gap cannot communicate, to download and transfer files to the main Endpoint Manager server you can use the Airgap utility and the BES Download Cacher utility.

This utility can also help download patch contents in a Fixlet site or single file downloads from a url.

To be able to gather across the network from the main Endpoint Manager the clients must be air-gapped together with the main Endpoint Manager server.

## On Windows systems

In addition to the Endpoint Manager server, which is being configured on the isolated network, you need a computer that has access to the public Internet to download Fixlet site content using the BESAirgapTool.exe utility, and to download files referenced in Fixlet action scripts. Both the downloaded site content and the files are transferred to the Endpoint Manager server on the isolated network. This computer cannot be an Endpoint Manager server or an Endpoint Manager relay.

### Step 1: Setting up the network

When the Endpoint Manager server, Endpoint Manager console, and Endpoint Manager client installations are complete, perform an initial gathering of the BES Support site content using the BESAirgapTool.exe utility to obtain a list of all Fixlet sites for which you are licensed. After the initial gathering is performed, start the Endpoint Manager console and navigate to the **BigFix Management** domain, License Overview dashboard and enable each Fixlet site as you choose.

## Step 2: Transferring Fixlet content

To make Fixlet content and product license updates available in the isolated network, the utility must be transferred from a computer with internet connectivity using the following steps:

1. From the Endpoint Manager server installation directory (C:\Program Files\BigFix Enterprise\BES Server), run the BESAirgapTool.exe on the Endpoint Manager server computer to create a Fixlet update request file. This file is saved to a portable drive together with the BESAirgapTool.exe, and the following dlls: libBEScrypto\_1\_0\_0\_1.dll, and libBEScrypto\_1\_0\_0\_5.dll. BESAirgapTool.exe does not run successfully without these two dll files included in the same directory as the BESAirgapTool.exe tool.
2. Bring the portable drive to a computer with Internet connectivity and run the BESAirgapTool.exe. This exchanges the request file for a response file.
3. Take the portable drive back to the Endpoint Manager server computer and run the BESAirgapTool.exe again. This imports the response file with Fixlet content and license updates into your deployment.

To update the Fixlet content on the main Endpoint Manager server, repeat these steps periodically. You can join the new Fixlet mailing list to receive notifications when Fixlets are updated.

## On Linux

In an air-gapped environment where a secure network is physically isolated from insecure networks, such as the public Internet or an insecure local area network, and the computers on opposite sides of the air gap cannot communicate, to download and transfer files to the main Endpoint Manager server running on a Linux system, you can use the Airgap utility.

This utility can also help download patch contents in a Fixlet site or single file downloads from a url.

**Note:** The AirGap utility does not support a configuration where the clients are air-gapped separately from the main Endpoint Manager server. The clients must be air-gapped together with the main Endpoint Manager server to be able to gather across the network from the main Endpoint Manager server.

In addition to the Endpoint Manager server which is being configured on the isolated network, you need a Windows computer that has access to the public Internet, to download Fixlet site content using the BESAirgapTool.exe utility. The downloaded site content and files are transferred to the Endpoint Manager server on the Linux computer.

To run the Airgap utility on Linux servers, you must have a Windows computer with the following environment:

- It must be connected to the Internet to download contents from the Fixlet sites. For additional information, see the Administration Tool documentation.
- The BESAirgapTool.exe tool must be installed. You can download the Windows Airgap utility from TEM Utilities.
- The following libraries must be copied to the Windows computer, in the same directory as BESAirgapTool.exe:

```
libBEScrypto_1_0_0_1.dll  
libBEScrypto_1_0_0_5.dll
```

You can copy these libraries from the folder where you installed the Endpoint Manager console. The default folder is C:\Program Files\Bigfix Enterprise\BES Console.

Perform these steps to run the Airgap utility on the Linux Endpoint Manager server:

1. Ensure that on the Linux computer, the Airgap utility is in the path where you installed the Endpoint Manager server. The default path is /opt/BESServer/bin.
2. Open the Linux Terminal, and type these commands to create a tar file named airgap.tar, containing the AirgapRequest.xml based on the information about the Endpoint Manager database:

```
# cd /opt/BESServer/bin
# ./Airgap.sh -run
```

**Note:** The complete syntax of Airgap.sh is the following:

```
Airgap { -run | -remotedir directory | -proxy proxy | -help }
```

where:

**-run** Runs Airgap to generate the tar file with the request in the local folder.

**-remotedir *directory***  
Runs Airgap to generate the tar file with the request in the specified folder.

**-proxy *proxy***  
Specifies the proxy name if needed.

**-help** Lists the Airgap usage.

3. On the Linux computer, extract the airgap.tar file with the following command under the airgap sub-folder::

```
# tar -xf airgap.tar
```

.

4. Copy the file AirgapRequest.xml, created in the airgap folder, to the folder containing the BESAirgapTool.exe file of the Windows computer.
5. On the Windows computer, run BESAirgapTool.exe to download the data related to the AirgapRequest.xml request into the AirgapResponse file.
6. Copy the AirgapResponse file, generated by BESAirgapTool.exe, from the Windows computer to the airgap folder of the Linux workstation.
7. On the Linux computer, from the airgap folder, run the Airgap tool to load the data on the database:

```
# cd /opt/BESServer/bin
# ./Airgap.sh -run
```

To download patches and other files from the Internet and deploy Fixlets on the main Endpoint Manager server see Transferring Downloaded Files.

## Transferring Downloaded Files

Deploying Fixlets on the main Endpoint Manager server requires downloaded patches and other files from the Internet. Included in the BES Air Gap Package is the BES Download Cacher utility. This utility helps:

- Download and transfer files to the main Endpoint Manager server.
- Download patch contents in a Fixlet site or single file downloads from a url.



You can download the current utility from <http://software.bigfix.com/download/bes/utl/BESDownloadCacher.exe>. The BES Download Cacher utility can only be run on a machine that has the BESRELAY service installed and running.

Some sites require additional steps to download content from patch vendors that restrict access. For additional information see the following Knowledge documents that describe using a tool to manually download patches for Solaris, Red Hat Enterprise Linux, SuSE Linux Enterprise, and AIX.

These sites require a three step process:

1. Run the BESAirgapTool.exe to download Fixlets and Tasks for each site.
2. Run the BES Download Cacher utility to download any site tools from IBM Endpoint Manager.
3. Run the download tool for each vendor to download patch contents.

## Transferring all files from Fixlet sites

To transfer files from Fixlet sites, perform the following steps:

1. Locate the .efxm file for the site from which you want to gather downloads, for example, BES Asset Discovery.efxm.
2. Run the BES Download Cacher utility with the following command:  
`BES_Download_Cacher.exe -m BES Asset Discovery.efxm -x downloads`

**Note:** This might take a very long time because it downloads every file referenced in the Fixlet site and puts the files into the downloads folder. If the files already exist in the downloads folder, they are not re-downloaded. Files are named with their sha1 checksum.

3. When the download finishes, copy the contents of the downloads folder (just the files, not the folder) into the sha1 folder on the main Endpoint Manager server. The default location for the sha1 folder is C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1. The Endpoint Manager server will use these files instead of trying to download them from the Internet.

**Note:** If you run the BES Download Cacher utility later, you can look at the modification time of the files to see which files are the newest. Using this method, you transfer only the newest files to the Main Endpoint Manager server instead of copying every file each time.

You might need to increase the size of the cache on the main Endpoint Manager server so that it does not try to delete any files from the cache. Run the BES Download Cacher utility to increase the size of the cache with the following command:

```
BES_Download_Cacher.exe -c 1024
```

The default size of the cache is 1024 MB.

After the files are cached in the Endpoint Manager server sha1 folder, they are automatically delivered to the Endpoint Manager relays and Endpoint Manager clients when you click an action in the Fixlet message that references a downloaded file. If the file is not cached, the Endpoint Manager console gives you a status of Waiting for Mirror Server after you deploy an action. For additional information about how the Endpoint Manager cache works, see How does the TEM Server and TEM Relay cache work.

## Transferring a single file

To transfer a single file from a Fixlet site, perform the following steps:

1. Run the BES Download Cacher utility with the following command:  
`BES_Download_Cacher.exe -u -x downloads`
2. When the download finishes, copy the contents of the downloads folder (just the file, not the folder) into the sha1 folder on the main Endpoint Manager server. The default location for the sha1 folder is `C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1`.

You might need to increase the size of the cache on the main Endpoint Manager server so that it does not try to delete any files from the cache. Run the BES Download Cacher utility to increase the size of the cache with the following command:

```
BES_Download_Cacher.exe -c 1024
```

The default size of the cache is 1024 MB.

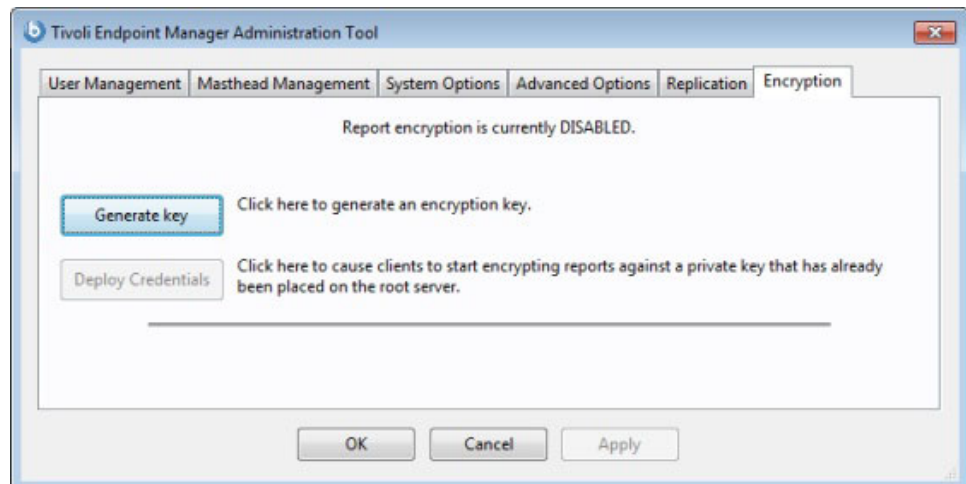
After the files are cached in the Endpoint Manager server sha1 folder, they are automatically delivered to the Endpoint Manager relays and Endpoint Manager clients when you click an action in the Fixlet message that references a downloaded file. If the file is not cached, the Endpoint Manager console gives you a status of "Waiting for Mirror Server" after you deploy an action. For additional information about how the Endpoint Manager cache works see *How does the TEM Server and TEM Relay cache work?*.

---

## 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 value is set in the console and is described in "Enabling encryption on Clients" on page 65. The key is generated from the **Encryption** tab of the IBM Endpoint Manager Administration Tool:

1. Launch the IBM Endpoint Manager Administration Tool by selecting **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Administration Tool**.
2. Select the **Encryption** tab.



At the top of the dialog is a statement of the current state (in this example: **Report encryption is currently DISABLED**). 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). The state is set to **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. The state is set to Enabled. 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 the state to Pending (unless you choose to deploy immediately as described in the next section). You can also click **Disable** to move back to the Disabled state.

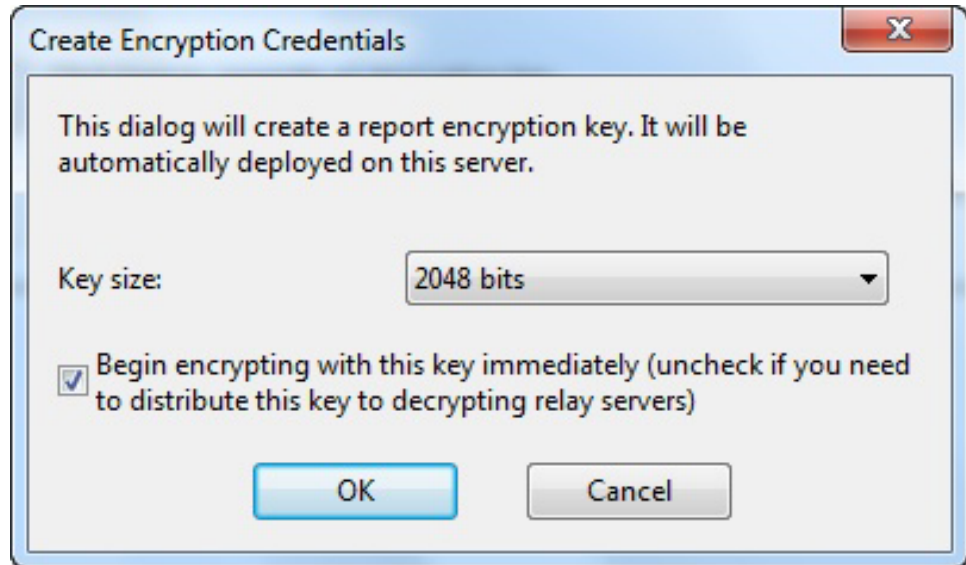
#### **Pending Rotation**

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 generate a new key from the **IBM Endpoint Manager Administration Tool**.

1. Launch the IBM Endpoint Manager Administration Tool by selecting **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Administration Tool**.
2. Select the **Encryption** tab.
3. Click the **Generate key** button. The Create Encryption Credentials dialog opens.



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 about encryption key sizes and server requirements, see the knowledge-base article on server requirements at the IBM 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:

On Windows systems:

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

On Linux systems:

```
var/opt/BES Server/Encryption Keys
```

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

On Windows systems:

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

On Linux systems:

```
var/opt/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 actionsite for any reason.

When you use top-level encryption, consider the following best practices:

- 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 that you must not move the key over the internet because anyone listening might be able to make a copy of your private key file. Instead, 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 gives you time to transfer the new key file to the relays before clients start posting encryption messages with that key.

---

## 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 IBM 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.

---

## Changing the Client Icon

By default, the icon in the upper left corner of the client UI is the IBM 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. Follow these steps to change the icon:

- On Windows systems:

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

On Linux systems:

1. Identify the path of the new icon, for example: `/TEM/newicon.ico`.
2. From the `/opt/BESServer/bin` command prompt, start the command line:  
`./iem login --server=servername:serverport --user=username --password=password`
3. From the `/opt/BESServer/bin` command prompt, run the following command:  
`./iem post /TEM/newicon.ico admin/icon`

where: `/TEM/newicon.ico` represents the full path of the new icon and `admin/icon` is the parameter to use to upload the new icon.

The icon is propagated 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.

---

## Chapter 9. Running backup and restore

You can schedule periodic backups (usually nightly) of the Endpoint Manager Server and database files. When a problem occurs, you can restore the database and the Endpoint Manager Server files on the Endpoint Manager Server computer or another computer.

---

### Backing up on Windows systems

If you back up the database and the Endpoint Manager Server files, when needed you can restore the Endpoint Manager environment on a Windows computer.

#### Backup Procedure

1. Using SQL Server Enterprise Manager, establish a maintenance plan for nightly backups for the BFEnterprise and BESReporting databases. Multiple backup copies allow for greater recovery flexibility. Consider backing up to a remote system to allow for higher fault tolerance.
2. Back up the following files and folders used by the Endpoint Manager Server:
  - [TEM Server folder]\BESReportsData\ArchiveData -- Archived Web Reports.
  - [TEM Server folder]\BESReportsServer\wwwroot\ReportFiles -- Support files for custom Web Reports.
  - [TEM Server folder]\Encryption Keys -- Private encryption keys (if using Message Level Encryption).
  - [TEM Server folder]\wwwrootbes\Uploads -- Contains custom packages that were uploaded to the system for distribution to clients.
3. If any of the following files and folders, used by the Endpoint Manager Server, can be rebuilt automatically by the server if a failure occurs, back them up for faster recovery.
  - [TEM Server folder]\Mirror Server\Inbox\bfemapfile.xml. Information necessary for IBM Endpoint Manager Agents to get actions and Fixlets.
  - [TEM Server folder]\wwwrootbes\bfsites. Information necessary for Endpoint Manager Agents to get actions and Fixlets.
  - [TEM Server folder]\wwwrootbes\bfmirror\bfsites. Information necessary for Endpoint Manager Agents to get actions and Fixlets.
  - [TEM Server folder]\wwwrootbes\bfmirror\downloads. Contains the download cache.
4. Securely back up site credentials, license certificates, and publisher credentials, and the masthead file.

The license.pvk, license.crt, and publisher.pvk files are critical to the security and operation of Endpoint Manager. If the private key (pvk) files are lost, they cannot be recovered. The masthead file is an important file that must be used for recovery. It contains the information about the Endpoint Manager server configuration. This file can be exported via the Masthead Management tab of the Administration tool.
5. If you have an LDAP configuration, complete the following steps to back up the decrypted server signing key [IEM Server folder]\EncryptedServerSigningKey.pvk:



- a. Copy the [IEM Server folder]\EncryptedServerSigningKey.pvk to a backup folder.
- b. Change directory to the backup folder.
- c. Click here to download the server key tool.
- d. Download the server key tool at the following link <https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/Server%20signing%20key%20Tool>.
- e. Run the following command to decrypt the server signing key:  
`ServerKeyTool.exe decrypt UnencryptedServerKey.pvk`

## Recovery procedure

1. Using either the previous Endpoint Manager Server computer or a new computer, install SQL server (use the same version of SQL server as was previously used). Remember to enable Mixed Mode Authentication for your new SQL installation if you were using it on the primary Endpoint Manager server.
2. If you are restoring the server on a new computer, run the following steps:
  - a. Ensure that the new Endpoint Manager server computer can be reached on the network using the same URL that is in the masthead file. (For example: `http://192.168.10.32:52311/cgi-bin/bfgather.exe/actionsite` OR `http://bigfixserver.company.com:52311/cgi-bin/bfgather.exe/actionsite`).
  - b. Copy in a folder on the new server the information that you backed up on the original server and the server signing key tool `ServerKeyTool.exe`.

**Note:** To avoid issues when the Endpoint Manager clients connect to the Endpoint Manager server before it is fully restored, ensure that the Endpoint Manager server is not available on the network until the recovery is complete.

3. Restore the BFEEnterprise and BESReporting databases from backup.
4. Restore the backed up files and folders creating the directory structure.
5. Change directory to the folder where you saved the decrypted server signing key and the server signing key tool.
6. Run the following command to encrypt the server signing key:  
`ServerKeyTool.exe encrypt UnencryptedServerKey.pvk`
7. Copy the encrypted key `EncryptedServerSigningKey.pvk` under the `C:\Program Files\BigFix Enterprise\BES Server` directory.
8. Install the Endpoint Manager Server component using the masthead file and specifying the same path used in the original install option.
9. If you need to resign all existing content using the new key, change directory to the Endpoint Manager server directory and run `BESAdmin.exe /rotateServerSigningKey`.

**Note:** If you enabled the HTTPS protocol, ensure that you restore the server settings for Web Reports.

## Verifying restore results

To ensure that your Endpoint Manager Server has been restored, perform the following steps:

1. Check the Endpoint Manager Diagnostics to verify that all services are started.

2. Log in to the Endpoint Manager Console and verify that the logins work and that the database information was restored.
3. Ensure that the Endpoint Manager clients and Endpoint Manager relays connect to the server when it is available and report data to it. Full recovery with all agents reporting might take from a few minutes to many hours (depending on the size of the deployment and how long the server was unavailable). At least some agents should be reporting updated information within an hour.
4. After verifying that some agents are reporting to the server, send a blank action: **Tools > Take Custom Action** to all computers. The blank action does not make any changes to the agent computers, but the agents report that they received the blank action.
5. Log in to the web reports and ensure that the data was restored.

---

## Backing up on Linux systems

If you back up the database and the Endpoint Manager Server files, when needed you can restore the Endpoint Manager environment on a Linux computer.

### Backup procedure

To back up the Endpoint Manager Server, perform the following steps:

1. Stop the Endpoint Manager services using the following commands:

```
/etc/init.d/besfilldb stop
/etc/init.d/besgatherdb stop
/etc/init.d/besserver stop
/etc/init.d/beswebreports stop
/etc/init.d/besclient stop
```
2. Stop the DB2 database using the db2stop command.
3. Back up the BFENT and BESREPOR databases using the following commands:

```
db2 backup db BFENT
db2 backup db BESREPOR
```

Optionally add an absolute path with the commands:

```
db2 backup db BFENT to /AbsolutePathExample
db2 backup db BESREPOR to /AbsolutePathExample
```

4. Manually back up the following folders:

```
/var/opt/BESClient
/var/opt/BESServer
/var/opt/BESWebReportsServer
/opt/BESWebReportsServer
```

and the following files:

```
/etc/opt/BESClient/actionsite.afxm
/etc/opt/BESServer/actionsite.afxm
/etc/opt/BESWebReportsServer/actionsite.afxm
```

5. In /etc/init.d back up the following files:

```
besclient
besfilldb
besgatherdb
besserver
beswebreports
```

6. Back up site credentials and license certificates. The license.pvk and license.crt files are critical to the security and operation of Endpoint Manager. If the private key (pvk) file is lost, it cannot be recovered.

## Recovery procedure

1. Stop all the Endpoint Manager processes and databases.
2. Remove the Endpoint Manager rpm files.
3. Remove the following folders:  
/var/opt/BESClient  
/var/opt/BESServer  
/var/opt/BESWebReportsServer  
/opt/BESWebReportsServer

and the following files:

```
/etc/opt/BESClient/actionsite.afxm  
/etc/opt/BESServer/actionsite.afxm  
/etc/opt/BESWebReportsServer/actionsite.afxm  
/etc/init.d/besclient  
/etc/init.d/besfilldb  
/etc/init.d/besgatherdb  
/etc/init.d/besserver  
/etc/init.d/beswebreports
```

4. Remove the BFENT and BESREPOR databases by running  
db2 drop db BFENT  
db2 drop db BESREPOR
5. Install the Endpoint Manager to register the Endpoint Manager rpm files.
6. Stop the Endpoint Manager processes and the installed databases.
7. Uninstall the BFENT and BESREPOR databases.
8. Restore the previously saved folders and files:

```
/var/opt/BESClient  
/var/opt/BESServer  
/var/opt/BESWebReportsServer  
/opt/BESWebReportsServer  
  
/etc/opt/BESClient/actionsite.afxm  
/etc/opt/BESServer/actionsite.afxm  
/etc/opt/BESWebReportsServer/actionsite.afxm  
/etc/init.d/besclient  
/etc/init.d/besfilldb  
/etc/init.d/besgatherdb  
/etc/init.d/besserver  
/etc/init.d/beswebreports
```

9. Restore the previously saved BFENT and BESREPOR as follows:  
db2 restore db BFENT  
db2 restore db BESREPOR

If saved with an absolute path, use the following command:

```
db2 restore db BFENT from /AbsolutePathExample  
db2 restore db BESREPOR from /AbsolutePathExample
```

10. Start the databases and then the Endpoint Manager processes.
11. Log on to the Console. If the following error is displayed: Connection to server could not be completed. Diagnostic Message: Unexpected server error: Bad sequence parameter, delete the Console cache on the disk where the Console is installed by searching for Enterprise Console string. Under this directory, remove the directory whose name is the same as the Endpoint Manager Server hostname, then log on again.

## Verifying restore results

To ensure that your Endpoint Manager Server has been restored, perform the following steps:

1. Check the Endpoint Manager Diagnostics to verify that all services are started.
2. Log in to the Endpoint Manager Console and verify that the logins work and that the database information was restored.
3. Ensure that the Endpoint Manager clients and Endpoint Manager relays connect to the server when it is available and report data to it. Full recovery with all agents reporting might take from a few minutes to many hours (depending on the size of the deployment and how long the server was unavailable). At least some agents should be reporting updated information within an hour.
4. After verifying that some agents are reporting to the server, send a blank action: **Tools > Take Custom Action** to all computers. The blank action does not make any changes to the agent computers, but the agents report that they received the blank action.
5. Log in to the web reports and ensure that the data was restored.



---

## Chapter 10. Upgrading on Windows systems

You can upgrade outdated versions of the IBM Endpoint Manager Server, IBM Endpoint Manager Console, IBM Endpoint Manager Relay, and IBM Endpoint Manager Client by using a Fixlet message in the BES Support content site from your Console or manually (for Remote Databases) from your Installers.

**Note:** Using the upgrade Fixlets is the preferred and simplest way to upgrade all of the IBM Endpoint Manager components (Installation Generator, Server, and Console). Generally the only time not to use the Fixlets would be to upgrade an IBM Endpoint Manager Server that uses a remote database.

You must upgrade the IBM Endpoint Manager Server and all the IBM Endpoint Manager Consoles at the same time (Consoles with a version earlier than or later than the Server version are not allowed to connect to the Server and Database).

Other IBM Endpoint Manager components (IBM Endpoint Manager Clients and IBM Endpoint Manager Relays) can work with the upgraded version of the IBM Endpoint Manager Server without problems. However, it is recommended that you upgrade the IBM Endpoint Manager Clients and relays whenever possible to take advantage of the new functions.

When new versions of Tivoli Endpoint Manager are released, the upgrade Fixlet messages are released in a planned roll-out process so it might take a few days before the upgrade Fixlet messages become relevant immediately after the upgrade. First you will see a Fixlet message relevant to upgrade your IBM Endpoint Manager Server and IBM Endpoint Manager Consoles. After the IBM Endpoint Manager Server is upgraded, Fixlet messages to upgrade the IBM Endpoint Manager Clients and IBM Endpoint Manager Relays will become relevant the next time the IBM Endpoint Manager Clients register.

---

### Upgrade Paths to V9.0

The following tables describe the upgrade paths to IBM Endpoint Manager V9.0:

- **Server upgrade**

*Table 12. Server Upgrade*

| Upgrade from | Windows Upgrade |
|--------------|-----------------|
| 7.x          | No              |
| 8.x          | Yes             |

- **Client upgrade**

*Table 13. Client Upgrade*

| Upgrade from | Windows Upgrade | UNIX Upgrade | Mac Upgrade |
|--------------|-----------------|--------------|-------------|
| 7.x          | Yes             | Yes          | Yes         |
| 8.x          | Yes             | Yes          | Yes         |

---

## Before upgrading

Before upgrading follow the steps below:

1. Close all IBM Endpoint Manager consoles.
2. Back up your IBM Endpoint Manager server and database.
3. Upgrade SQL Databases. SQL 2000 database is no longer supported.
4. Back up your `license.pvk` and `license.crt` to a separate location on the Endpoint Manager server or to a USB key.
5. Increase the replication interval to prevent the replication from failing repeatedly during the upgrade. For additional information, see “Changing the replication interval on Windows systems” on page 122.
6. Upgrade the Endpoint Manager components according to the following order:
  - a. Servers and consoles. These components must match their versions and must be upgraded at the same time.
  - b. Relays
  - c. Clients

Servers, relays, and clients do not need to match versions and the upgrade of these components can occur at different times. Older clients can continue to report to newer relays or servers, but they might not have all the functionality of the new release.

7. For DSA servers, upgrade first one DSA server to ensure the upgrade is successful and then the other DSA servers.
8. After the upgrade, run the Endpoint Manager Administration Tool to update a remote database.

### Note:

- For large deployments, the server upgrade might take several minutes.
- Post-upgrade your deployment might be slow because the upgrade downtime can create a backlog of client reports, and it can take several hours for the IBM Endpoint Manager server to process this backlog after the upgrade has completed.

---

## Upgrading the Installation Generator

1. From the computer where you installed the IBM Endpoint Manager Installation Generator, download and run the new IBM Endpoint Manager Installation Generator from <http://support.bigfix.com/bes/install/downloadbes.html>
2. Click **Yes** when you are prompted to upgrade and follow the installer instructions.

This step can also be accomplished via BES Support site Fixlet content such as 'Updated Windows Installation Folders - Tivoli Endpoint Manager version 9.0.xxx.x. Now Available!'.

---

## Upgrading the Server

1. Copy the IBM Endpoint Manager Server installation folder (default location is `C:\Program Files\BigFix Enterprise\BES Installers\Server`) to the IBM Endpoint Manager Server computer.
2. Run the IBM Endpoint Manager Server installer (`setup.exe`) on the IBM Endpoint Manager Server computer.



**Note:** If you have a remote database, prior to upgrading see the article <http://www-01.ibm.com/support/docview.wss?uid=swg21506063>.

3. Follow the installer instructions to upgrade. For troubleshooting information see `C:\besserverupgrade.log`
4. To upgrade the Trend Core Protection Module Server for the 8.0 release, see <http://www-01.ibm.com/support/docview.wss?uid=swg21506219>.

---

## Upgrading the Console

1. Copy the IBM Endpoint Manager Console installation folder (default location is `C:\Program Files\BigFix Enterprise\BES Installers\Console`) to all computers that are running the IBM Endpoint Manager Console.
2. Run the IBM Endpoint Manager Console installer (`setup.exe`) on all the computers currently running the IBM Endpoint Manager Console.
3. Follow the installer instructions to upgrade.

---

## Upgrading the Relays

IBM Endpoint Manager Relays can be upgraded individually by downloading and running the IBM Endpoint Manager Relay upgrade file that can be found at: <http://www.ibm.com/developerworks/downloads/tiv/endpoint/>

---

## Upgrading the Clients

- IBM Endpoint Manager Clients can be upgraded individually by copying the IBM Endpoint Manager Client installation folder (default location is `C:\Program Files\BigFix Enterprise\BES Installers\Client`) to each computer that is running the IBM Endpoint Manager Client, and then running `setup.exe`.
- IBM Endpoint Manager Clients can also be upgraded by using the Tivoli Endpoint Manager Client Deployment Tool, with a login script, or with another deployment technology. Run the new IBM Endpoint Manager Client installer on the computer that has the old IBM Endpoint Manager Client.

---

## Upgrading the Web Reports

To upgrade Web Reports, run the BES Server installer or to upgrade stand-alone Web reports, run `BESServerUpgrade.exe`, which detects Web Reports installation and offers to upgrade it for you.

**Note:** If you have a remote database, run the upgrade as a user with DBO permissions to the database.



---

## Chapter 11. Upgrading on Linux systems

You can upgrade outdated versions of the IBM Endpoint Manager server, IBM Endpoint Manager console, IBM Endpoint Manager relay, and IBM Endpoint Manager client by using a Fixlet message in the BES Support content site from your console or manually.

**Note:** Using the upgrade Fixlets is the preferred and simplest way to upgrade all the IBM Endpoint Manager components. It is recommended that you upgrade the IBM Endpoint Manager clients and IBM Endpoint Manager relays whenever possible to take advantage of the new functions.

The upgrade Fixlet on Linux also manages all the components including remote databases.

When new versions of IBM Endpoint Manager are released, the upgrade Fixlet messages are released in a planned roll-out process so it might take a few days before the upgrade Fixlet messages become relevant after the upgrade. First you see a Fixlet message relevant to upgrade your IBM Endpoint Manager server. After the IBM Endpoint Manager server is upgraded, Fixlet messages to upgrade the IBM Endpoint Manager clients and IBM Endpoint Manager relays become relevant the next time that the IBM Endpoint Manager clients register.

---

### Upgrade types and paths

You can upgrade the Endpoint Manager components automatically by running the upgrade Fixlets from the console or manually by running the upgrade program locally on the workstations to upgrade. If you run the manual upgrade, you can see when it completes and any potential server status or error message.

The following tables show the IBM Endpoint Manager upgrade paths.

- **Server upgrade**

*Table 14. Server Upgrade*

| Upgrade from | UNIX Upgrade |
|--------------|--------------|
| 7.x          | No           |
| 8.x          | No           |
| 9.x          | Yes          |

- **Client upgrade**

*Table 15. Client Upgrade*

| Upgrade from | Windows Upgrade | UNIX Upgrade | Mac Upgrade |
|--------------|-----------------|--------------|-------------|
| 7.x          | Yes             | Yes          | Yes         |
| 8.x          | Yes             | Yes          | Yes         |
| 9.x          | Yes             | Yes          | Yes         |

---

## Before upgrading

Before running the upgrade, perform the following tasks:

- Close all IBM Endpoint Manager consoles.
- Back up your IBM Endpoint Manager server and database.
- Back up your `license.pvk` and `license.crt` to a separate location on the Endpoint Manager server or to a USB key.
- With version 9.0.777.0 (9.0 Patch 2), the IBM Endpoint Manager underlying protocol on Linux systems changed from SSL to Kerberos. If you integrated with Active Directory, before upgrading from version 9.0.586.0 (9.0) or 9.0.649.0 (9.0 Patch 1) to version 9.0.777.0 (9.0 Patch 2), run the following steps to continue the integration:
  1. Take notice note of the Active Directory-related configuration on IBM Endpoint Manager.
  2. Remove the Active Directory integration.
  3. Upgrade IBM Endpoint Manager to 9.0.777.0.
  4. On the Console, select Tools -> Add LDAP directory to add again the integration with Active Directory.
  5. Set again the Active Directory-related configuration on IBM Endpoint Manager.
- If your server is configured in a DSA environment, increase the replication interval to prevent the replication from failing repeatedly during the upgrade. For additional information, see “Changing the replication interval on Linux systems” on page 123.
- Upgrade the Endpoint Manager components according to the following order:
  1. Servers and consoles (console and server must have the same version and must be upgraded at the same time.
  2. Relays
  3. Clients

Servers, relays, and clients do not need to match versions and the upgrade of these components can occur at different times. Older clients can continue to report to newer relays or servers, but they might not have all the functions of the new release.

- For DSA servers, upgrade first one DSA server to ensure the upgrade is successful and then the other DSA servers.

### Note:

- For large deployments, the server upgrade might take several minutes.
- After an upgrade your deployment might be slow because the upgrade downtime can create a backlog of client reports, and it can take several hours for the IBM Endpoint Manager server to process this backlog after the upgrade has completed.

---

## Upgrading the server

1. Copy the IBM Endpoint Manager server installable image to the Endpoint Manager server computer and extract it to a folder.
2. On the IBM Endpoint Manager server computer run the IBM Endpoint Manager server upgrade script:  
`./install.sh -upgrade`

This program upgrades all the components it detects on the local server.

**Note:** For troubleshooting information see `/var/log/BESInstall.log` and `/var/log/BESAdminDebugOut.txt`

---

## Upgrading the console

1. Copy the Endpoint Manager console installable image to a folder on all computers that are running the Endpoint Manager console.
2. Run the Endpoint Manager console installer (`setup.exe`) on all the computers currently running the Endpoint Manager console.
3. Follow the installer instructions to upgrade.

---

## Upgrading the relays

IBM Endpoint Manager relays can be upgraded individually by downloading and running the IBM Endpoint Manager relay upgrade file that can be found at: <http://www.ibm.com/developerworks/downloads/tiv/endpoint/>.

---

## Upgrading the Clients

- Endpoint Manager clients can be upgraded individually by copying the Endpoint Manager client installable image to each computer that is running the Endpoint Manager client, and then running the setup program.
- Endpoint Manager clients can also be upgraded by using the Endpoint Manager Client Deployment Tool, with a log in script, or with another deployment technology. Simply run the new Endpoint Manager Client installer on the computer with the old Endpoint Manager client.

---

## Upgrading the Web Reports

To upgrade a stand-alone Web Reports server, run the `install.sh` server upgrade script:

```
./install.sh -upgrade
```



---

## Chapter 12. Additional configuration steps

These topics explain additional configuration steps that you can run in your environment.

---

### Optimizing the servers

IBM 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 IBM 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 IBM Endpoint Manager database. Consider changing it to 60-120 seconds or more if there are many console operators. The IBM 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 BFEEnterprise 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 IBM 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 IBM 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 IBM 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 have 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 “Remote Citrix / Terminal Services Configuration” on page 13).
- **Delete old actions.** The IBM 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 IBM Endpoint Manager support site.

---

## Managing Bandwidth

File downloads consume the bulk of the bandwidth in a typical installation. You can control the bandwidth by throttling, which limits the number of bytes per second. You can specify the bandwidth throttling on either the server, 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.

---

## 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 IBM 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, IBM 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.

**Note:** 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 IBM Endpoint Manager **Client settings**:

```
_BESClient_Download_DynamicThrottleEnabled  
_BESClient_Download_DynamicThrottleMaxBytesPerSecond  
_BESClient_Download_DynamicThrottleMinBytesPerSecond  
_BESClient_Download_DynamicThrottlePercentage
```

The IBM 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.

---

## Managing Downloads

The IBM 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 IBM 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 you can change it 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 delete these files manually.

The caches are stored as subfolders of the program folder, which is created by default at C:\Program Files\BigFix Enterprise on Windows systems and

/var/opt/BES Server on Linux systems. 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 IBM 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 that is contained in the following file:

### On Windows systems:

<Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt

### On Linux systems:

<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.

---

## 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, 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 system 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:



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

---

## Geographically locating clients

Because 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 IBM Endpoint Manager using the **Location Property Wizard**.

1. In the console, go to the **BigFix Management** domain, click **Computer Management**, and then click **Location Property Wizard**. 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 IBM 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, including 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 IBM 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.

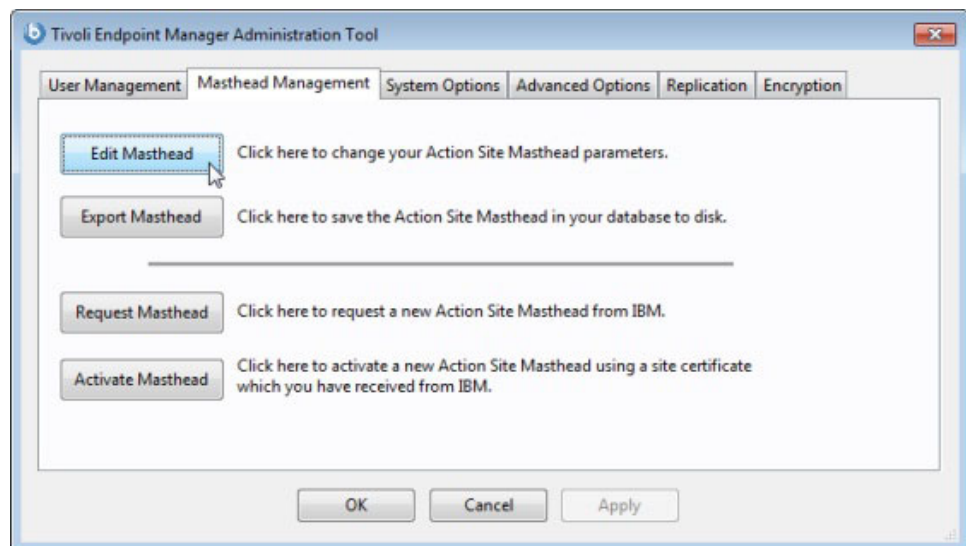
Although the console does not provide an explicit interface for setting an expiration date on the lock, you can create a custom action to do this. For more information, see the *Action Guide*.

---

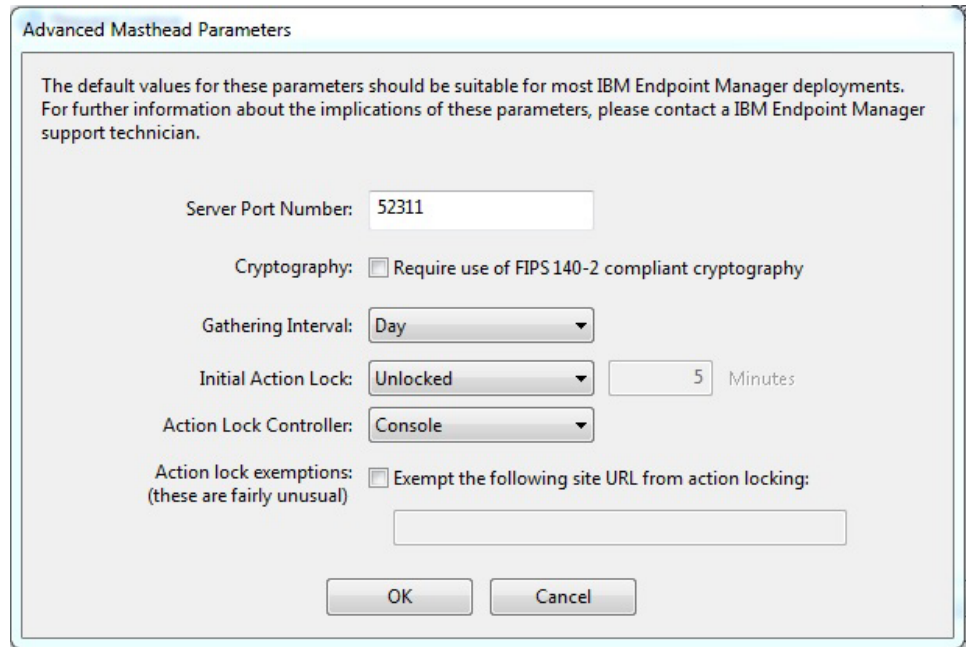
## Editing the Masthead on Windows systems

You can change certain default parameters stored in the masthead by using the **IBM Endpoint Manager Administration Tool**:

1. Launch the program from **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Administration Tool**.
2. Browse to the location of your site license and click **OK**.
3. Select the **Masthead Management** tab and click **Edit Masthead**.



4. Enter the parameters of the masthead file that contains configuration and license information together with a public key that is used to verify digital signatures. This file is saved in your credential folder.



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

Server Port Number:

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

Gathering Interval:

Initial Action Lock:   Minutes

Action Lock Controller:

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

You can edit the following options:

#### Server Port Number:

In general, you do not need to change this number. 52311 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 can use a reserved port number (ports 1-1024), but this might reduce the ability to monitor or restrict traffic correctly and it prevents you from using port numbers for specific applications. If you do decide to change this number *after* deploying the clients, IBM Endpoint Manager will not work correctly. For additional information, see *Modifying port numbers* in the next section.

#### Cryptography:

Check this box to implement the Federal Information Processing Standard 140-2 in your network. This changes the masthead so that every IBM 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 a few 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 servers perspective, a smaller interval becomes necessary to get a timely response from the clients. Higher gathering rates only slightly affect the performance of the server, because only the differences are gathered; a client does not gather information that it already has.

#### Initial Action Lock:

You can specify the initial lock state of all clients, if you want to lock a client automatically after installation. 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 want 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 clients 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.

**Exempt the following site URL from action locking:**

In rare cases, you might need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL.

**Note:** You can specify only one site URL and it must begin with `http://`.

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

**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.

---

## Editing the Masthead on Linux systems

To modify the masthead, run the following command:

```
./BESAdmin.sh -editmasthead
-sitePvkLocation=<path+license.pvk> -sitePvkPassword=<password>
[ -advRequireFIPSCompliantCrypto=<true|false> ] [ -advGatherSchedule=<0-10> ]
[ -advController=<0-2> ] [ -advInitialLockState=<0|2> ]
-advInitialLockState=1 -advInitialLockDuration=<num> ]
[ -advActionLockExemptionURL=<url> ]
```

where:

**-sitePvkLocation=<path+license.pvk>**

Specifies a private key file (*filename.pvk*). This site level signing key and its password are required to run the Administration Tool. Only users with access to the site level signing key and password are able to create new Endpoint Manager operators.

**Note:** The notation `<path+license.pvk>` used in the command syntax stands for *path\_to\_license\_file/license.pvk*.

**-sitePvkPassword=<password>**

Specifies the password associated to the private key file (*filename.pvk*).

**advRequireFIPSCompliantCrypto (optional, boolean)**

Implements the Federal Information Processing Standard on your network. This changes the masthead so that every IBM 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 a few seconds to the client startup time

**advGatherSchedule (optional, integer)**

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 servers perspective, a smaller interval becomes necessary to get a timely response from the clients. Higher gathering rates only slightly affect the performance of the Server, because only the differences are gathered; a client does not gather information that it already has. Valid values are:

```
0=Fifteen Minutes,
1=Half Hour, 2=Hour,
3=Eight Hours,
4=Half day,
5=Day,
6=Two Days,
7=Week,
8=Two Weeks,
9=Month,
10=Two Months
```

**advController (optional, integer)**

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 user, you can select **Client**, but this is not recommended. Valid values are:

```
0=console,
1=client,
2=nobody
```

**advInitialLockState (optional, integer)**

Specifies 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 want 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. Valid values are:

```
0=Locked,
1=timed (specify duration),
2=Unlocked
```

**advInitialLockDuration (optional, integer)**

Defines the period of time in seconds the clients must be locked.

**advActionLockExemptionURL (optional, string)**

In rare cases, you might need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL.

**Note:** You can specify only one site URL and it must begin with http://.

---

## Modifying Global System Options

To modify a few basic system defaults, such as the minimum refresh time and the Fixlet visibility perform the following steps:

On Windows systems:

1. Launch the Administration Tool from **Start > Programs > IBM Endpoint Manager > IBM 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 increase 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 except Master Operators.

On Linux systems:

1. From the /opt/BESServer/bin command prompt start the command line:  
./iem login --server=servername:serverport --user=username --password=password
2. From the /opt/BESServer/bin command prompt run the following command:  
./iem get admin/options > /appo/options.xml
3. In the /appo/options.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <SystemOptions Resource="https://nc926065:52311/api/admin/options">
    <MinimumRefreshSeconds>15</MinimumRefreshSeconds>
    <DefaultFixletVisibility>Visible</DefaultFixletVisibility>
  </SystemOptions>
</BESAPI>
```

edit the following keywords to set the minimum refresh time in seconds and the external sites as visible to all the console operators or to only the Master operators:

```
<MinimumRefreshSeconds>15</MinimumRefreshSeconds>
<DefaultFixletVisibility>Visible</DefaultFixletVisibility>
```

4. Upload the modified file by running the following command:  
./iem post /appo/options.xml admin/options

---

## Scheduling replication

On Windows systems if you have multiple servers in your deployment, you can schedule when each one replicates. The default is five minutes, but you can shorten the time for greater recoverability or increase it to limit network activity:

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

To schedule replication on Linux systems see Managing Replication on Linux systems.

---

## Extending the IBM 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, IBM Endpoint Manager warns you, giving you sufficient time to renew your license. When you are coming close to the expiration date, IBM Endpoint Manager notifies you by using a Fixlet message. Similarly, if you start to exceed the number of clients allocated by your license, IBM 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 **License Overview** node, and click the **Check for license update**.

---

## Re-creating Site Credentials

Private and public key encryption creates a chain of signing authority from the IBM 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 about 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 and 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 IBM 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 IBM Endpoint Manager Site Administrator can change the password of the site-level key, if they know the current password.

---

## Chapter 13. 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 IBM 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. IBM 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 IBM Endpoint Manager **Diagnostics Tool** performs a complete test on the server components and can be run any time you experience problems. “Running the IBM Endpoint Manager Diagnostics tool” on page 57.
- Check the **BigFix Management** domain often. There are a number of Fixlets available that can detect problems with any of your IBM Endpoint Manager components. This can often prevent problems before they ever affect your network.
- Check the IBM Endpoint Manager Knowledge Base at Tivoli Endpoint Manager Support site. 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 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





---

## Appendix A. Upload and archive manager settings

You can collect multiple files from Endpoint Manager clients into an archive and move them through the relay system to the server. This allows the Endpoint Manager Administrator to automatically log data from specific managed computers.

To do this, a new component called the **Archive Manager** has been added to the Endpoint Manager Client which can collect files periodically or on command. It passes the resultant compressed tar-ball to the **Upload Manager** on the Endpoint Manager Client. The Upload Manager has an input directory that queues the files for uploading.

The Upload Manager performs one upload operation at a time, moving the data in manageable chunks to reduce network traffic. It sends these chunks to the nearest Endpoint Manager relay or server, where the **PostFile** program reassembles the chunks back into the original file.

PostFile then passes the file up the chain, to the next Endpoint Manager relay or to its ultimate destination at the Endpoint Manager server. It again uses the Upload Manager to slice the file into chunks and send them on to the next PostFile program in the hierarchy. When the file finally arrives at the Endpoint Manager server, it is saved in a special directory location based on the ID of the client computer.

Along the way, both the Upload Manager and the PostFile program can alter the chunk size or throttle the upload speed to smooth out network traffic.

**Note:** When it encounters an unregistered Endpoint Manager Client, the Upload Manager pauses. This can happen for a variety of reasons, including a downed network, a busy server, or a disconnected client. As soon as the Endpoint Manager client can register with the Endpoint Manager system again, it restarts the Upload Manager and continues from where it stopped.

---

### Editing the archive manager settings

A typical archive is a collection of logs and configuration files that are compiled regularly and posted to the server. There are many settings available to help you customize your logging needs.

To initialize the various archive settings, follow these steps:

1. Start the Endpoint Manager Console.
2. Select the **Computers** tab.
3. From the filter/list, select the set of computers that you want to start archiving.
4. Select **Edit Computer Settings** from the **Edit** menu. Typically, you select multiple computers, so you see a tabbed dialog box.
5. Select the **Settings** tab.
6. Check the **Custom Setting** box.
7. Enter the **Names** and corresponding **Values** of the desired settings.

---

## Creating a Custom Action

You can create custom actions that can post attributes about the Endpoint Manager client to an archive file.

To create a custom action:

1. Start the Endpoint Manager Console.
2. Select the **Computers** tab.
3. From the filter/list, select the set of computers that you want to target for the action.
4. Select **Take Custom Action** from the **Tools** menu.
5. Select the **Action Script** tab.
6. Enter the desired **Action Script** in the text box provided.

---

## Archive Manager

Archive Manager is a component of the Endpoint Manager Client that can collect files periodically or on command. It passes the resultant compressed tar-ball to the Upload Manager on the Endpoint Manager Client.

### Archive Manager Settings

These are the settings of the Archive Manager component:

#### **\_BESClient\_ArchiveManager\_OperatingMode**

The OperatingMode dictates the style of archiving, allowing periodic or triggered archiving. The following modes are available:

- 0:** Disable all archival operations (default value).
- 1:** Automatic, with a period = `_BESClient_ArchiveManager_IntervalSeconds`.
- 2:** Enables the `<uicontrol>archive now</uicontrol>` action command.

To allow a custom action to post client attributes to an archive file, make sure the OperatingMode is set to 2.

The default value of 0 disables archiving.

#### **\_BESClient\_ArchiveManager\_FileSet-<tag>**

This setting (actually a group of settings with optional tags) specifies the files to be archived. This technique lets you specify multiple named batches of files. Each setting starts with `"_BESClient_ArchiveManager_FileSet-"` and ends with a batch name (the `<tag>` part).

The value of each setting is a path on the client file system. It can be a single file, in which case that file is part of the archive; a single directory, in which case all files in the directory will be part of the archive; or a directory path ending with wild cards, in which case all files in the directory matching the wild cards will be part of the archive.

For example, the setting `_BESClient_ArchiveManager_FileSet-(log)`, representing all the log files in a temporary log folder, could have a value like `c:\temp\log`.

Everything after the dash (-) is used as the default prefix of the files as they are unpacked on the root server. Therefore a file named x.log in the c:\temp\log folder would be unpacked as (Log)x.log.

#### **\_BESClient\_ArchiveManager\_SendAll**

This setting allows you to send just the archives that have changed, avoiding redundant uploads. There are two possible values for this setting:

- 0: Only send files that have changed since the last archive operation (default).
- 1: Send all files, even if they have not changed.

The default value of 0 is recommended for most applications.

#### **\_BESClient\_ArchiveManager\_MaxArchiveSize**

This setting limits the size (in bytes) of the uploaded archive. Because a typical archive might be composed of several files, the archive size corresponds to the sum of the file sizes.

If the limit is exceeded, an archive that contains only the index file is created and uploaded by the Archive Manager. The index contains the following header line:

MaxArchiveSize: Exceeded

The default value is 1000000 (one million bytes), however, since IBM Endpoint Manager V8.0, the file system is 64-bit. This means that the actual maximum file size is  $2^{64} - 1$ , sufficient for any reasonably sized file.

#### **\_BESClient\_ArchiveManager\_IntervalSeconds**

When the OperatingMode is set to 1, this setting determines the interval at which the client triggers an archive.

The default value is 86400 seconds (24 hours).

## **Archive Manager internal variables**

These are the internal variables of the Archive Manager component:

#### **\_BESClient\_ArchiveManager\_LastArchive**

The Archive Manager updates this setting whenever it posts an archive. The value of the setting is the secure hash algorithm (sha1) of the file that was posted.

#### **\_BESClient\_ArchiveManager\_LastIntervalNumber**

The Endpoint Manager Client updates this setting whenever it posts an archive. It represents the interval number from 1970 to the time when the archive was last collected. If the interval is a day long (the default), then the setting indicates the number of days from 1970 to the day when it created the last archive. It is calculated such that when the interval number changes, it is time to create a new archive.

The value is also offset by a time corresponding to the computer id, to stagger the collecting of archives.

## **Archive Manager Index File Format**

During the building of the archive, the Archive Manager creates an index containing metadata about the archive. This is a sample index from an archive with a single file:

```
MIME-Version: 1.0
Content-Type: multipart/x-directory2; boundary="==="
Unique-ID: 1077307147
Archive-Size: 105
SendAll: 0
Date: Wed, 17 Mar 2004 02:23:01 +0000
FileSet-(LOG): c:\temp\log\newfile.log
```

--===

```
URL: file:///c:/temp/log/newfile.log
NAME: (LOG)newfile.log
SIZE: 105
TYPE: FILE
HASH: 3a2952e0db8b1e31683f801c6384943aae7fb273
MODIFIED: Sun, 14 Mar 2004 18:32:58 +0000
```

-----

---

## Upload Manager

The Upload Manager coordinates the sending of files in chunks to the Post File program. You can throttle the upload dataflow to conserve bandwidth. Since IBM Endpoint Manager version 8.0, the file system uses 64 bits, sufficient for file sizes of up to  $2^{64} - 1$  bytes in length.

### Upload Manager Settings

These are the settings of the Upload Manager component:

#### **\_\_BESClient\_UploadManager\_Progress**

This internal setting provides a value that tracks the progress of the upload. When an upload is underway, this setting takes on values of the form:

<sha1>: <position> of <size> bytes in <duration> seconds

For example:

51ee4cf2196c4cb73abc6c6698944cd321593007: 672 of 672 bytes in 5 seconds

The default value is "No Progress".

#### **\_\_BESClient\_UploadManager\_BufferDirectory**

The Archive Manager always sets the Upload Manager's input Buffer Directory to "\_\_BESData/\_\_Global/Upload". This directory is on the client computer, in the Endpoint Manager Client folder.

#### **\_\_BESRelay\_UploadManager\_BufferDirectory**

Like the Endpoint Manager Client, the Endpoint Manager Relay also has an Upload Manager, and it also has a buffer directory, whose path is specified by this setting. The Upload Manager uploads the files in the sha1 subdirectory of the specified directory. It sorts the files by modification time and then, just like the Endpoint Manager Client, it uploads them in chunks to smooth out the bandwidth requirements.

#### **\_\_BESRelay\_UploadManager\_BufferDirectoryMaxSize**

This setting denotes the maximum amount of space on disk that the server is allowed to take from the client using the Upload Manager. You can set the maximum file size to be as large as  $2^{64} - 1$  bytes. Its default is 1GB.

#### **\_BESRelay\_Uploadmanager\_BufferDirectoryMaxCount**

This setting denotes the number of files that the buffer directory is allowed to hold. Its default is 10,000.

#### **\_BESRelay\_UploadManager\_CompressedFileMaxSize**

This setting denotes the amount of space of the largest compressed file the Upload Manager will be allowed to handle. You can set the maximum file size to be as large as  $2^{64} - 1$  bytes. It applies only to the server and it is evaluated during the decompression of the uploaded archive.

#### **\_BESRelay\_UploadManager\_ChunkSize**

Uploads are done one chunk at a time. In case of a conflict between this computer and the upstream computer, the size of the chunk is set to the smaller of the two.

A value of 0 for the chunk size indicates that the upload should be done in a single chunk, and effectively disables restarts and throttling (this is NOT recommended). The local chunk size setting is specified in bytes.

The default value is 128K.

#### **\_BESRelay\_UploadManager\_ThrottleKBPS**

After each chunk has been uploaded, the Upload Manager calculates the amount of time to sleep to maintain the throttle speed in kilobytes per second (ThrottleKBPS). This allows you to compensate for network bottlenecks. For example, a Endpoint Manager relay connected over a slow VPN to the server might have a low upload throttle rate to minimize the bandwidth on that network segment.

In case of a conflict between this computer and the upstream server (or relay), the throttle KBPS is set to the smaller of the two.

The default value is 0, which disables throttling.

#### **\_BESRelay\_UploadManager\_ParentURL**

This setting specifies the location of the parent computer, which is either an Endpoint Manager relay or a server. The Upload Manager posts the file chunks to the PostFile program using a url such as:

**`http://host.domain.com:52311/cgi-bin/bfenterprise/PostFile.exe`**

This specifies an absolute address to the desired server. More typically, however, Upload Manager points to a folder on the current parent relay:

**`/cgi-bin/bfenterprise/PostFile.exe`**

This is the default setting.

#### **\_BESRelay\_UploadManager\_Progress**

The Upload Manager writes a status or error string into this setting. Like the Endpoint Manager Client progress setting, it takes on values of the form:

`<sha1>: <position> of <size> bytes in <duration> seconds`

The default value is "No Progress".

**Note:** There are two leading underscores on this setting, which prevent the Endpoint Manager Console Operator from affecting this internal value.

#### **\_BESRelay\_UploadManager\_CleanupHours**

Sometimes archived files accumulate but do not get uploaded. This could happen with a network outage, a downed server or other communication

problem. To avoid overloading the system, these old files are deleted or cleaned up. This setting determines how old a file can get before it is deleted.

The default value is 72 hours (3 days).

---

## PostFile

The PostFile program receives the chunks of files posted by the Upload Manager and appends them to its own copy of the file. The Upload Manager specifies the range of bytes being posted and the sha1 of the file, which is used as the filename. These parameters are appended to the URL as in the following example:

```
postfile.exe?sha1=51ee4cf2196c4cb73abc6c6698944cd321593007&range=1000,1999,20000
```

Here the sha1 value identifies the file, and the range in this case specifies the second 1,000 byte chunk of a 20,000 byte file.

When PostFile receives a chunk of the file it first checks to make sure it is the correct segment. If so, it appends the posted data to its local copy of the file. It returns the size of this file, as well as the current chunk size and throttle BPS settings.

PostFile has to handle several Endpoint Manager clients feeding into it at the same time. To balance that load, it adjusts the throttle rate. The effective throttling rate is determined by dividing the limiting PostFile rate by the number of concurrently uploading files.

For example, if PostFile has a throttle setting of 100 KBPS and 50 clients are simultaneously uploading files, the throttle value returned to each client would be adjusted to 2 KBPS. By setting custom throttle values to specific Endpoint Manager relays, you can efficiently deal with any bottlenecks in your network.

PostFile stores the partially uploaded files in the Upload Manager's buffer directory with an underscore in front of them (the Upload Manager does not upload files that begin with underscore). When PostFile receives the last chunk of the file, it calculates the sha1 of the file and checks that it matches the sha1 parameter in the URL. If so, it removes the leading underscore.

The Upload Manager can then upload the file to the next relay up the hierarchy (or any other server, if so specified).

PostFile determines whether or not the Upload Manager is running. If not, PostFile assumes that it has reached its root server destination. It renames the uploaded file, extracts the files from the archive, and deposits them in a subfolder of the Upload Manager's buffer directory.

The program calculates the subfolder path using a modulus of the computer ID. This has the effect of spreading out file directory accesses and preventing an overpopulation of any single directory.

For example, the path to file "log" from computer ID1076028615 is converted to the path "BufferDir/sha1/**15**/1076028615/log" where 15 is the remainder modulo 100 (the lower two digits) of the id.

If the uploaded file is a valid Endpoint Manager archive and is successfully extracted, then the original uploaded file is deleted.



## PostFile Settings

PostFile uses the `_BESRelay_PostFile_ChunkSize` and `_BESRelay_PostFile_ThrottleKBPS` settings for the chunk size and throttle values for incoming data. These values can be adjusted for varying connection speeds or other network anomalies.

When PostFile communicates with the upload manager, it passes along these values. As mentioned before, if there is a conflict between any two computers over these settings, it favors the smaller value.

The default values are 128K for ChunkSize and 0 for ThrottleKBPS (disable throttling).

---

## Resource Examples

### Example 1

In this example, we want to collect all the files in the `c:\log` folder and all the `.ini` files in the `c:\myapp` folder once an hour. Send up only the differences and don't send the archive if it exceeds 1,000,000 bytes in size. To set this up, create the following settings in the Endpoint Manager Console:

```
_BESClient_ArchiveManager_FileSet-(Log) = c:\log
_BESClient_ArchiveManager_FileSet-(Ini) = c:\myapp\*.ini
_BESClient_ArchiveManager_OperatingMode = 1
_BESClient_ArchiveManager_Interval_Seconds = 3600
_BESClient_ArchiveManager_SendAll = 0
_BESClient_ArchiveManager_MaxArchiveSize = 1000000
```

### Example 2

In this example, we want the same set of files as above, but we also want to collect some useful attributes (retrieved properties) from the client computer. A custom action can generate these attributes and trigger an archive when it completes. It uses the same settings as above, but sets the operating mode to 2 to enable the **archive now** action command:

```
_BESClient_ArchiveManager_OperatingMode = 2
```

You can then create a custom action, specifying the attributes you want to collect. For example, to append the operating system, computer name, and DNS name to the log file, create a custom action like this:

```
appendfile {"System:" & name of operating system}
appendfile {"Computer:" & computer name}
appendfile {"DNS name:" & dns name}
delete "c:\log\properties.log"
copy __appendfile "c:\log\properties.log"
archive now
```

The **appendfile** command creates a temporary text file named `__appendfile`. Each time you invoke the command, it appends the text you specify to the end of this temporary file.

The **delete** and **copy** commands clear out the old log file (if any) and copy the `__appendfile` to the log. This has the effect of creating a new `properties.log` file. The **archive now** command immediately creates an archive, as long as the `OperatingMode` is set to 2.

You can then target this action to any subset of Endpoint Manager Clients, using whatever scheduling you choose. Using variations on this scheme, you could perform a full archive once a week, in addition to nightly differences.

## Appendix B. Command-Line Interface

The Endpoint Manager Command-Line Interface (CLI) is a utility that facilitates programmatic control of an Endpoint Manager Server using the server RESTAPI. It is a lightweight wrapper for user authentication, session management, HTTP request and response generation, and parsing. The utility is packaged as `iem.exe` on Windows systems and `iem` on Linux Red Hat Enterprise V.5.0 (or later) systems and is installed with the server installer.

## Location

On a Linux server, the Endpoint Manager command line is deployed at the following path:

```
/opt/BESServer/bin/iem
```

On Windows server, the Endpoint Manager command line is deployed at the following path:

C:\Program Files (x86)\BigFix Enterprise\BES Server\iem.exe

## Conventions and usage

Conventions:

<> = required argument

[] = optional argument

\* = 0 or more instances supported

| = 0R

Usage:

```

    item <GET|DELETE> <Resource> [-q] [--param value]*

```

OR

```
iem <POST|PUT> [inputFile] <Resource> [-q] [--param value]*
```

OR

```
iem admin <COMMAND> [-q] <--pkey=KEYFILE>  
                        [--pkeypwd=PASS] [--param value]*\n
```

OR

```
iem LOGIN [-q] [--server=SERVER] [--user=USER]
[--password=PASS] [--masthead=PATH TO TRUSTED MASTHEAD]
```

`-q` : Quiet mode. Input prompts disabled.

## User Authentication and Session Management

To start the command line interface kog in to the server with the following command from a command prompt:

iem LOGIN

Three arguments are required, SERVER, USER, and PASSWORD. Provide these arguments in one of the following three ways::

### Environment variables

Use IEM\_SERVER, IEM\_USER, and IEM\_PASSWORD to specify the values of the arguments.

### Command line

Use --server, --user, and --password to specify the variables on the command line.

### Standard Input

If any arguments are not provided by either of the first two methods, the CLI utility prompts you to provide them.

If the server uses a self-signed certificate for HTTPS interactions, the utility prompts you to accept or decline the certificate. If you choose to trust it, the certificate is cached and used to validate all future interactions with the server.

The --masthead command line argument can be used to specify a local file to trust when communicating with the server, removing the need for this prompt. The masthead file is copied into the CLI cache directory and used for all future interactions with the server.

When login is successful, the utility receives a session token from the server, which it saves to a local config file and uses for future communication. This token is currently invalidated after 5 minutes of inactivity by the server. You can configure this time with the setting \_BESDataServer\_APIAuthenticationTimeoutMinutes.

---

## Local Data Directory

The CLI stores a config file and a directory tree of cached server certificates locally. By default, this is located in a .iem folder in the user profile directory /usr/{user} ) on Linux systems or in %LOCALAPPDATA%\BigFix on Windows systems. If a console is installed on the local Windows machine, any server certificates that have been trusted by the console are implicitly trusted by the CLI as well.

The directory used for local caching can be overridden with the environment variable IEM\_DATADIR.

---

## FIPS Deployments

The Endpoint Manager CLI tool is provided as a convenient wrapper for HTTP requests to the REST API on the root server. The CLI is currently **NOT** capable of using the Endpoint Manager FIPS-compliant cryptography library. To have this capability in a REST API HTTP environment, access REST API endpoints from another FIPS-capable client application.

---

## Making Requests

The CLI is a lightweight abstraction of HTTP requests to the Endpoint Manager Server RESTAPI. The basic syntax for constructing requests using the CLI is:

```
iem <METHOD> <RESOURCE>
```

where:

**<METHOD>**

Refers to the HTTP method of the request and can be: GET, POST, PUT, and DELETE

**<RESOURCE>**

Refers to the RESTAPI resource that is being requested. See RESTAPI.

## Query Parameters

If the request requires query parameters (such as, the RESTAPI resource `/api/query` requires the parameter `relevance=<expression>`), you can specify them by using the command line in the following format:

```
--param value
```

or

```
--param=value
```

Some examples:

```
iem GET query --relevance "names of bes computers"
iem GET query --relevance=now
```

## POST and PUT Input

POST and PUT requests require a body in their HTTP Requests. You can specify the body either as an input file on the command line, such as:

```
iem POST inputfile.xml operator/bigfix
```

By running this command you post the file `inputfile.xml` to the location `operator/bigfix` and update the operator `bigfix` with the information provided in the `inputfile.xml` file or, you can enter it manually when prompted (if no input file is specified on the command line, the utility prompts for input:

```
iem POST query
Input: relevance=now
```

The input must be of the format expected by the specified RESTAPI resource, the CLI does not do any pre-parsing or sanity checking.

## Portability

The Endpoint Manager executable can be run on any machine. To run it from a location other than the one in which it was installed, copy the executable and the `libBEScrypto_1_0_0_4` library into the same directory on the target machine. The Endpoint Manager tool runs only in non-FIPS mode so the `libBEScrypto_1_0_0_1` library is not required.

**Note:** On Linux systems, you must run the tool from the directory containing the `libBEScrypto_1_0_0_4` library, otherwise, the environment variable `BES_LIBPATH` must be set to a directory containing that executable.

---

## IEM CLI Examples

The following links contain relevant examples of the syntax used in the Endpoint Manager commands:

- [Login](#)
- [Operators](#)
- [Advanced Options](#)
- [System Options](#)
- [Export masthead](#)
- [Actions](#)
- [Fixlet](#)
- [LDAP](#)
- [Role](#)

### Login

To log in:

```
./iem login --server=ServerName:ServerPort --user=master --password=Mypassword
```

To perform an https login:

```
./iem login --server=https://TEMServer:52311 --user=master  
--password=Mypassword
```

### Operators

To display a list of operators (local and LDAP), run the following command:

```
./iem get operators
```

To get roles associated to an operator, run the following command:

```
./iem get operator/OperatorName/roles
```

To add an operator, use the XML syntax example from `./iem get operators`, remove the row `<LastLoginTime>`. For a local operator, add the row `<Password>`, and then run the following command:

```
./iem post MyOperator.xml operators
```

To modify an operator, use the XML syntax example from `./iem get operators`, and then run the following command:

```
./iem post /tmp/Operator.xml operator/MyOperatorName
```

To remove an operator (local and LDAP), run the following command:

```
./iem delete operator/OperatorName
```

### Advanced Options

To get the list of advanced options, run the following command:

```
./iem get admin/fields
```

The command returns the list of fields in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <AdminField Resource="https://nc926065:52311/api/admin
    /field/usePre70ClientCompatibleMIME">
    <Name>usePre70ClientCompatibleMIME</Name>
    <Value>false</Value>
  </AdminField>
```

To set the admin key `disableNmoSiteManagementDialog`, create an XML file (`besadmin.xml`) as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <AdminField Resource="https://nc926065:52311/api/admin
    /field/disableNmoSiteManagementDialog">
    <Name>disableNmoSiteManagementDialog</Name>
    <Value>1</Value>
  </AdminField>
</BESAPI>
```

Use the following command to set the appropriate attribute:

```
./iem post /TEM/besadmin.xml admin/fields
```

## System Options

To display `MinimumRefreshSeconds` (seconds), and `DefaultFixletVisibility` (Visible, Hidden) run the following command:

```
./iem get admin/options
```

The command returns the list of options in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001
  /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <SystemOptions Resource="https://nc926065:52311/api/admin/options">
    <MinimumRefreshSeconds>15</MinimumRefreshSeconds>
    <DefaultFixletVisibility>Visible</DefaultFixletVisibility>
  </SystemOptions>
</BESAPI>
```

To set the system option `MinimumRefreshSeconds` create an XML file (`SystemOptions.xml`) as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001
  /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <SystemOptions Resource="https://nc926065:52311/api/admin/options">
    <MinimumRefreshSeconds>20</MinimumRefreshSeconds>
    <DefaultFixletVisibility>Hidden</DefaultFixletVisibility>
  </SystemOptions>
</BESAPI>
```

Use the following command to set the appropriate attribute:

```
./iem post /TEM/SystemOptions.xml admin/options
```

## Export masthead

Use the following command to export the masthead to standard output:

```
./iem get admin/masthead
```



Use the following command to retrieve masthead parameters:

```
./iem get admin/masthead/parameters
```

The command returns the list of parameters in XML format as follows:

```
<BESAPI xmlns:xsi="http://www.w3.org/2001
/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <MastheadParameters Resource="https://nc926065:52311
/api/admin/masthead/parameters">
    <PortNumber>52311</PortNumber>
    <GatherInterval>Day</GatherInterval>
    <Controller>nobody</Controller>
    <InitialLockState>on</InitialLockState>
    <RequireFIPSCompliantCrypto>>false</RequireFIPSCompliantCrypto>
  </MastheadParameters>
</BESAPI>
```

## Actions

To submit the Fixlet ID 42 in the Master Action Site, on the computer nc926036.romelab.it.ibm.com, create an XML file as follows:

```
<BES xmlns:xsi="http://www.w3.org/2001
/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
  <SourcedFixletAction>
    <SourceFixlet>
      <SiteName>ActionSite</SiteName>
      <FixletID>42</FixletID>
      <Action>Action1</Action>
    </SourceFixlet>
    <Target>
      <ComputerName>nc926036.romelab.it.ibm.com</ComputerName>
    </Target>
  </SourcedFixletAction>
</BES>
```

Use the following command to post the action of submitting the Fixlet on a specific computer:

```
./iem post /TEM/take_action_site.xml actions
```

## Fixlet

To get the list of Fixlets in the custom site myfixes, use the following command:

```
./iem get fixlets/custom/myfixes
```

The command returns the list of Fixlets in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001
/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <Fixlet Resource="https://nc926065:52311/api/fixlet/custom/myfixes/34?"
    LastModified="Mon, 10 Dec 2012 14:33:36 +0000">
    <Name>myfixes Custom Fixlet</Name>
    <ID>34</ID>
  </Fixlet>
  <Fixlet Resource="https://nc926065:52311/api/fixlet/custom/myfixes/40?"
    LastModified="Mon, 10 Dec 2012 16:05:30 +0000">
    <Name>MyFixlet</Name>
    <ID>40</ID>
  </Fixlet>
</BESAPI>
```

## LDAP

To get the list of defined LDAPs, use the following command:

```
./iem get ldapdirectories
```

The command returns the list of LDAP in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <LDAPDirectory Resource="https://nc125058.romelab.it.ibm.com:52311
    /ldapdirectory/34">
    <ID>34</ID>
    <Name>AD</Name>
    <IsActiveDirectory>true</IsActiveDirectory>
    <IsGlobalCatalog>true</IsGlobalCatalog>
    <UseSSL>false</UseSSL>
    <BaseDN>DC=tem,DC=test,DC=com</BaseDN>
    <UIDAttribute>userPrincipalName</UIDAttribute>
    <UserFilter>(objectCategory=user)</UserFilter>
    <GroupFilter><![CDATA[(&(objectCategory=group)
      (groupType:1.2.840.113556.1.4.803:=2147483648))]]></GroupFilter>
    <User>TEM\Administrator</User>
    <Servers>
      <Server>
        <Host>10.43.5.20</Host>
        <Port>3268</Port>
        <Priority>0</Priority>
      </Server>
    </Servers>
  </LDAPDirectory>
</BESAPI>
```

To create a new LDAP, use the same XML syntax as `./iem get ldapdirectories` and add the following row after the User row in the XML file:

```
<Password>MyLDAP-Password</Password>
```

Then create the new LDAP with the following command:

```
./iem post MyLDAP.xml ldapdirectories
```

To get the configuration data of a specific LDAP having its ID (in the current example ID=34) run the following command:

```
./iem get ldapdirectory/34
```

The command returns the LDAP configuration in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="BESAPI.xsd">
  <LDAPDirectory Resource="https://nc125058.romelab.it.ibm.com:52311
    /ldapdirectory/34">
    <ID>34</ID>
    <Name>AD</Name>
    <IsActiveDirectory>true</IsActiveDirectory>
    <IsGlobalCatalog>true</IsGlobalCatalog>
    <UseSSL>false</UseSSL>
    <BaseDN>DC=tem,DC=test,DC=com</BaseDN>
    <UIDAttribute>userPrincipalName</UIDAttribute>
    <UserFilter>(objectCategory=user)</UserFilter>
    <GroupFilter><![CDATA[(&(objectCategory=group)
      (groupType:1.2.840.113556.1.4.803:=2147483648))]]></GroupFilter>
    <User>TEM\Administrator</User>
    <Servers>
      <Server>
        <Host>10.43.5.20</Host>
        <Port>3268</Port>
        <Priority>0</Priority>
      </Server>
    </Servers>
    <Password>MyLDAP-Password</Password>
  </LDAPDirectory>
</BESAPI>
```

```

        <Host>10.43.5.20</Host>
        <Port>3268</Port>
        <Priority>0</Priority>
    </Server>
</Servers>
</LDAPDirectory>

```

To remove a specific LDAP having its ID (in the current example ID=34) run the following command:

```
./iem delete ldapdirectory/34
```

To convert a local operator into an LDAP operator, run the following command:

```
BESAdmin.exe /convertToLDAP0perators [/mappingFile:<file>]
```

where <file> is the mapping file containing the matching between Windows local operators and LDAP operators. Each line of the file must contain the name of the user to convert, followed by a tab and the name of the user in LDAP or Active Directory. The LDAP name must have the same format used to log into the console, such as domain\user, user@domain, or user. If the file is not available, BESAdmin converts all local users assuming their name in LDAP or Active Directory is the same as their local user name.

## Role

To get the role configuration, run the following command:

```
./iem get roles
```

The command returns the role configuration in XML format.

To create a new role, run the following command:

```
./iem post Example.xml roles
```

Where Example.xml contains role configuration data in a XML format.

---

## Appendix C. 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 IBM Endpoint Manager.

**Client** Software installed on each networked computer to be managed under the IBM 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 IBM 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 IBM 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 IBM Endpoint Manager system.

### **Installation Computer**

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

### **Installation Generator**

An application that creates installers for the core IBM 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 IBM Endpoint Manager process, including URLs that point to where trusted Fixlet content is available. The IBM Endpoint Manager Client brings content into the enterprise based on subscribed mastheads.

**Mirror server**

A server required in the IBM 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 IBM 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 IBM 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 IBM 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 IBM 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 IBM 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 IBM Endpoint Manager Server, or simply Server.

**Signing password**

The password (specified when the IBM 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 person responsible for installing IBM Endpoint Manager and with the permission to create new Console operators.

**SQL server**

A full-scale database engine from Microsoft that can be acquired and installed into the IBM 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 IBM 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 IBM Endpoint Manager Server where the Server software and related files (including Console and Client installers) will be installed.

**IBM Endpoint Manager database**

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

**IBM 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-client computing in a wide-area network requiring more relays to aggregate downloads and reduce overhead.





---

## Appendix D. Support

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

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



---

## Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

## **Trademarks**

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

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

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

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

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

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

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

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

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

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

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









Printed in USA