IBM Endpoint Manager
Version 9.1

Installation Guide

IBM Endpoint Manager
Version 9.1

Installation Guide

****** MISSING FILE ******

This file was generated during the publishing process

****** MISSING FILE ******

This file was generated during the publishing process

Contents

Chapter 1. Introduction

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.

Fixlets 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 realtime. In addition, administrators can create or customize their own Fixlet solutions and tasks to suit their specific network needs.

is easy to install and has built-in public and private-key encryption technology to ensure the authenticity of Fixlets and actions. It grants you maximum power as the administrator, with a minimal impact on network traffic and computer resources. 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.

What is new in V9.1

V9.1 adds the following enhancements:

Enhanced Security

This enhancement includes the following functions:

- Ability to disable SHA-1 signatures in favor of SHA-256.
- Support for TLS 1.2 communication protocol.
- The root certificate key strength is increased from 1024 bits to 4096 bits.

Note: Enabling Enhanced Security results in loss of management of any agents or relays with versions earlier than 9.1, including proxy agents. For information about this enhancement, see Chapter 4, “Security Configuration Scenarios,” on page 23.

LDAP group support in Web Reports

For information about this enhancement, see Step 2: Assign a Web Reports role to LDAP users or groups.

Linux server processes are now 64-bit

The following services are now 64-bit:

- Root Server
- Web Reports
- FillDB
- GatherDB

Common Criteria security certification features

This enhancement includes the following functions:

- Configurable login banners for Console and Web Reports.

  To configure the login banner, set the option **loginWarningBanner** as described in “Advanced Options” on page 72 for Windows systems or in “Running the Administration Tool” on page 111 for Linux systems.
- Inactivity timeout for Console and Web Reports.

  To configure the inactivity timeout, specify the option **timeoutLockMinutes** as described in “Advanced Options” on page 72 for Windows systems or in “Running the Administration Tool” on page 111 for Linux systems.
- Increased server audit logging.

  To configure the server audit logging, specify the setting **_BESRootServer_Audit_Verbosity** as described in https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Endpoint Manager/page/Configuration Settings.

Dashboard API enhancements

This enhancement includes the following functions:

- Suppress warning for the StopAction API.
- Tag actions when importing.
- Asynchronous DownloadFile API.
- Asynchronous UploadFile API.

Enhanced screen reader support for the Client UI

This enhancement includes the following functions:

- Enabled screen reader for About dialog and Action History dialog.
- Support high contrast display mode in Client UI.

REST API enhancements

This enhancement includes the following functions:

- Ability to add a file that will to be gathered by agents to a site.
- Ability to delete a computer.
- Users that are created through the REST API are now logged in the server audit log.

The information about REST API is available at the following web page https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli Endpoint Manager/page/REST API.

New agent inspectors

This enhancement includes the following functions:

- Square root, for example, "sqrt of 4".

- Added comparison operators for type <time of day with time zone>.
- Group membership inspectors, for example, "manual groups of <client>".
- Ability to percent-encode and percent-decode strings.
- On Windows systems: ability to inspect whether Data Execution Prevention is enabled for a process.
- On Windows systems: registry inspectors support the **REG_QWORD** registry type.
- On Windows systems: get the process id (pid) of a service, for example, "pid of <service>".
- *nix: network socket inspectors.

The information about agent inspectors is available at the following web page http://support.bigfix.com/inspectors/Action%20Objects_Any.html.

For a list of fixes that are included in the V9.1, see http://support.bigfix.com/bes/changes/fullchangelist-91.txt.

For a list of known limitation that affects V9.1 (9.1.1065), see http://www-01.ibm.com/support/docview.wss?uid=swg21667537.

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 Endpoint Managementhttps://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 terms, but are used throughout the guide without being labeled every time with :

Agent means a computer where the client is installed

Console
means console

Client means client

Server means server

Relay means relay

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

Architectural components overview

The system has the following main components:

agents:

They are installed on every computer that you want to manage using . A computer on which the agent is installed, is also referred to as *client*. Clients access a collection of Fixlets that detects security exposures, incorrect configurations, and other vulnerabilities. The client can implement corrective actions received from the console through the server. The client runs undetected by users and uses a minimum of system resources.

The also allows the administrator to respond to screen prompts for those actions that require user input. clients can encrypt their upstream communications, protecting sensitive information. client software can run in Windows, Linux, Solaris, HP-UX, AIX, and Macintosh operating systems.

servers:

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

relays: Increase the efficiency of the system. Instead of forcing each networked computer to directly access the server, relays spread the load. Hundreds to thousands of clients can point to a single relay for downloads, which in turn makes only a single request to the server. relays can connect also to other relays, further increasing efficiency. An 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 agent installed. As soon as you install an relay, the clients in your network can automatically discover and connect to them.

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 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 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 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 might 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.

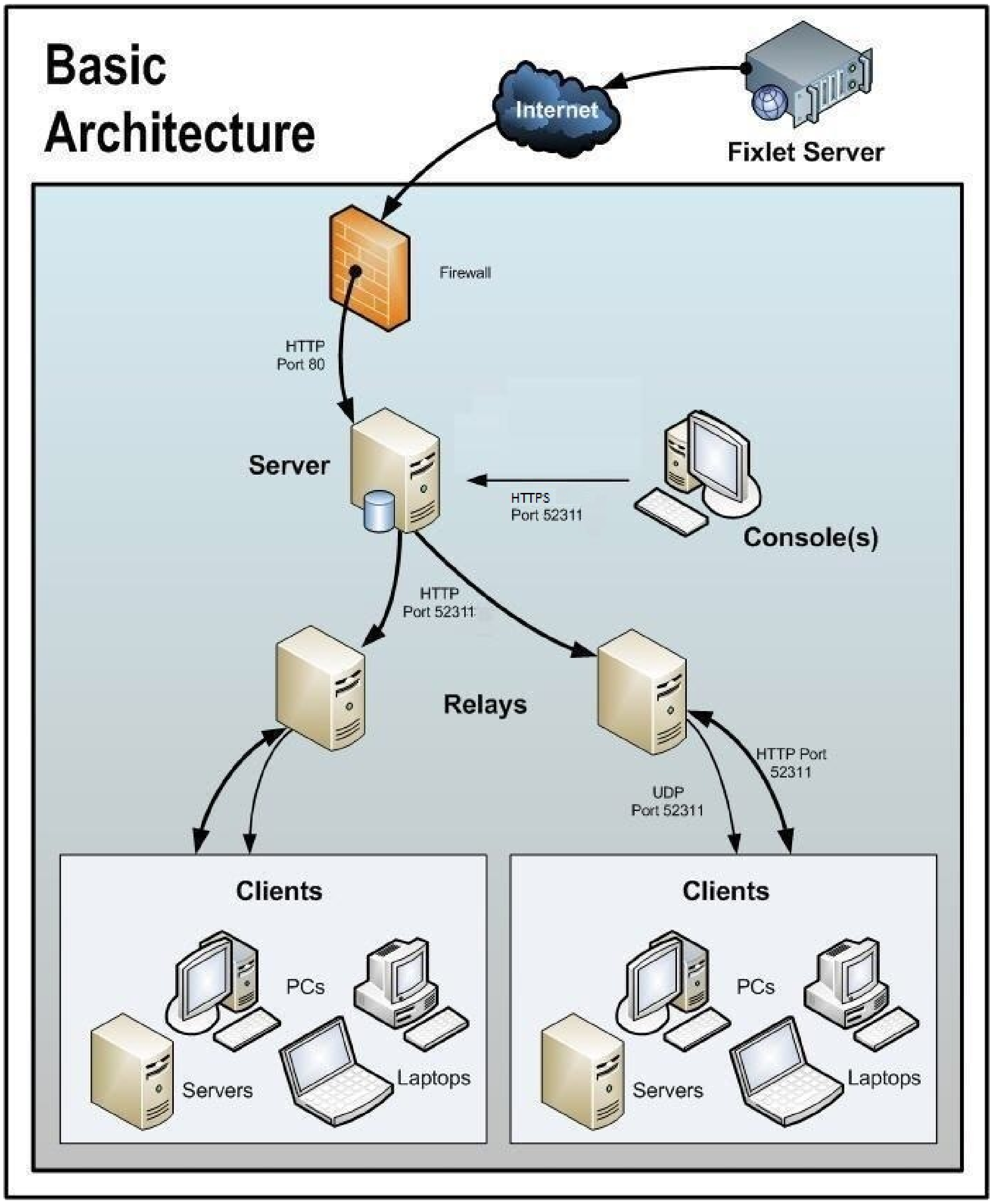
Pay careful attention to the relay distribution in each scenario. Relays provide a dramatic improvement in bandwidth and should be thoughtfully deployed, especially in those situations with low-speed communications. Relays are generally most efficient in fairly flat hierarchies. A top-level relay directly 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 failback and failover 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:

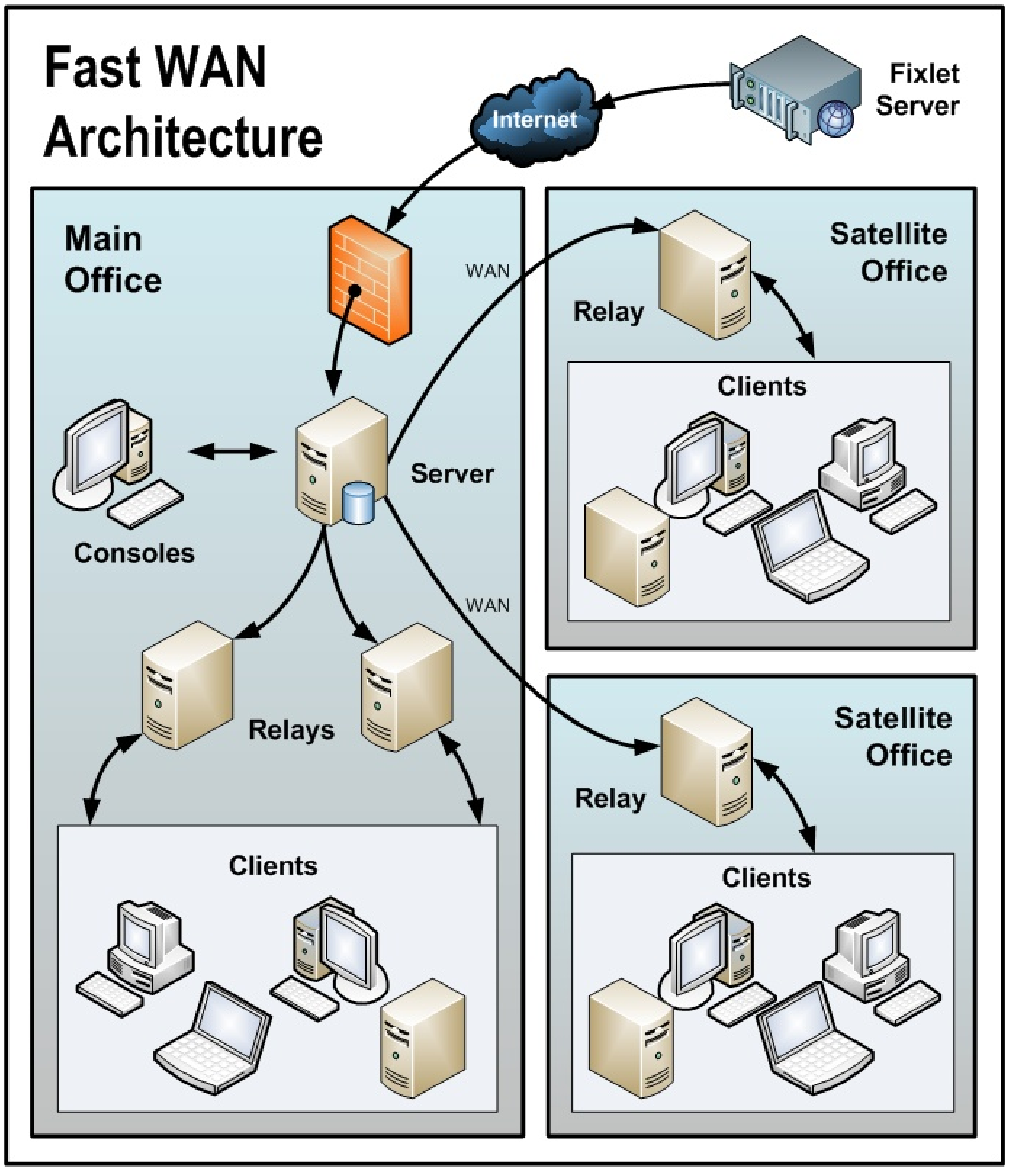
- Port 80 is used to collect Fixlet messages over the Internet from Fixlet providers such as IBM.
- A dedicated port (defaulting to 52311) is used for HTTP communications between servers, relays, and Clients.
- A dedicated port (defaulting to 52311) is used for HTTPS communications between servers and 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 relays can also take advantage of a UDP port to alert the Clients about updates, but this is not strictly necessary.
- The 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.

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.

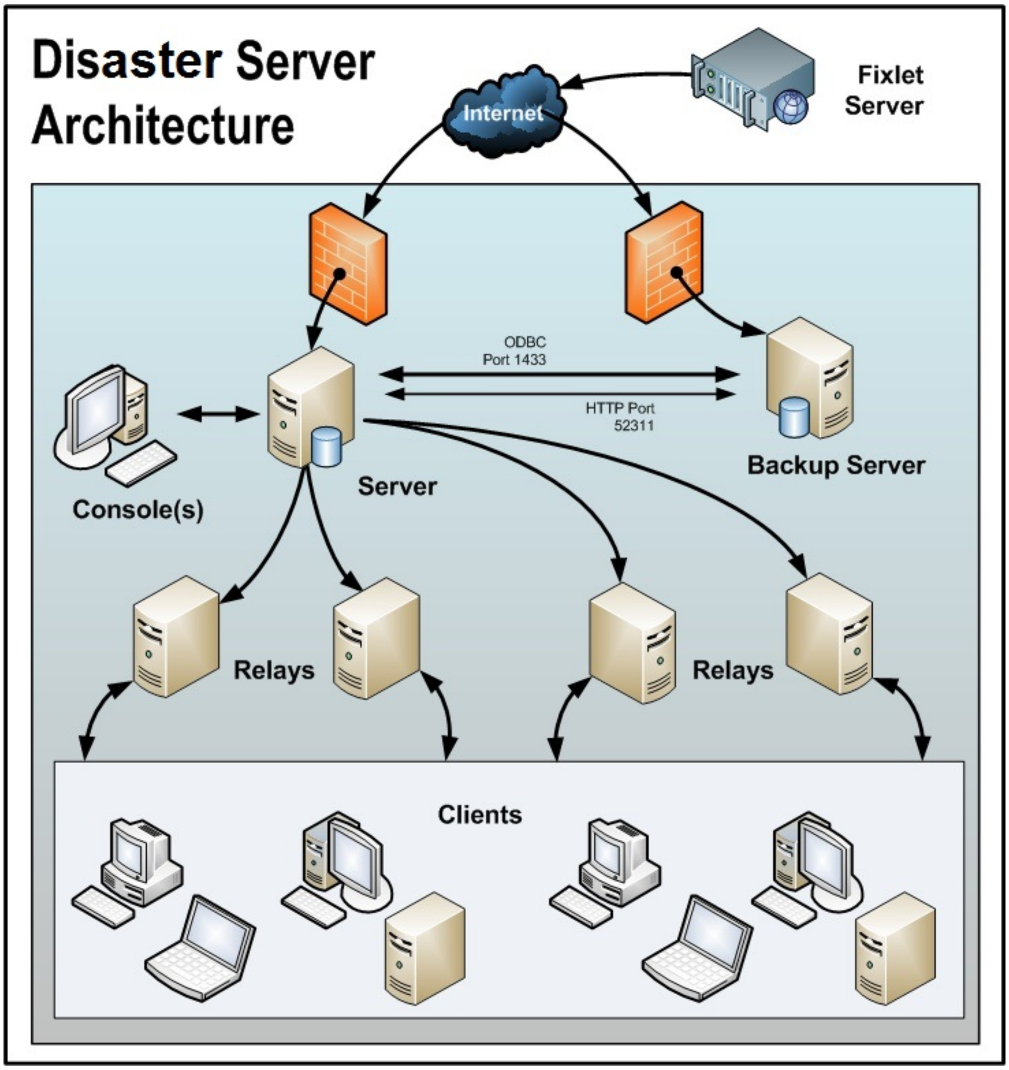


Note the following about the diagram:

- 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.

Disaster Server Architecture

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 case of a failover, the specific configured relays automatically find the backup server and reconnect the network. For more information about the relay configuration see Configuring relay failover.

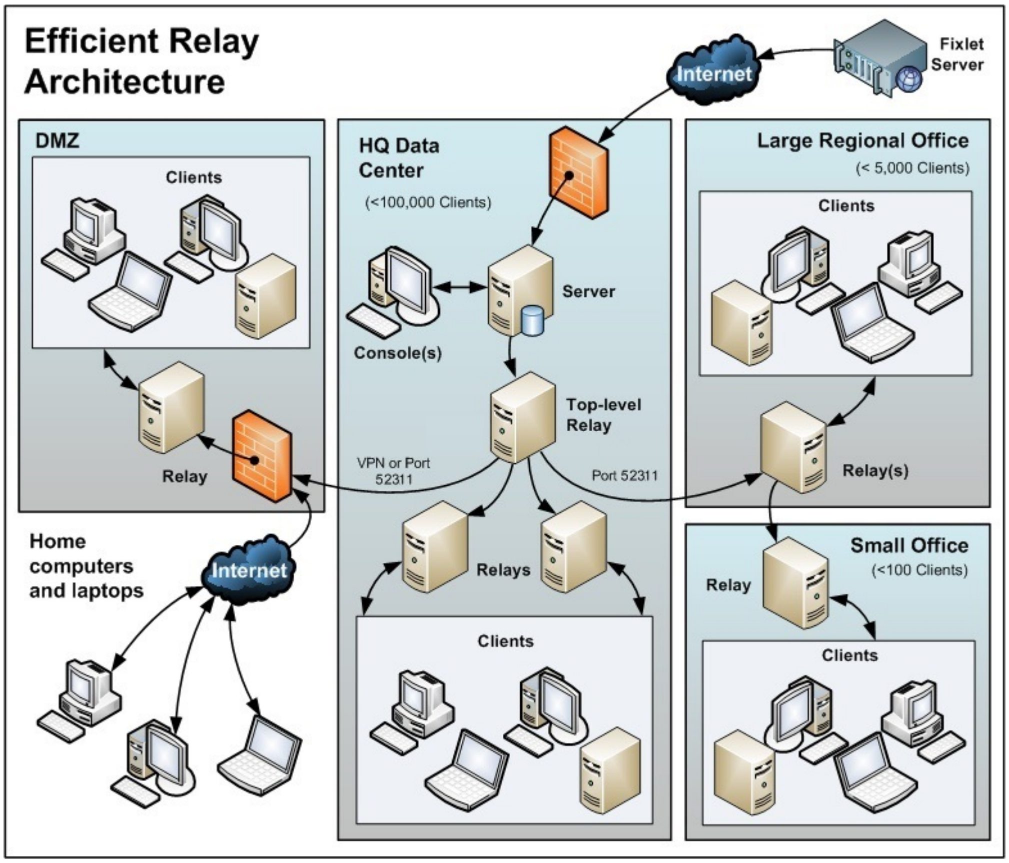
Note the following about the diagram:

- The 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 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 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 servers communicate on a regular schedule to replicate their data. You can review the current status and adjust the replication interval through 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.

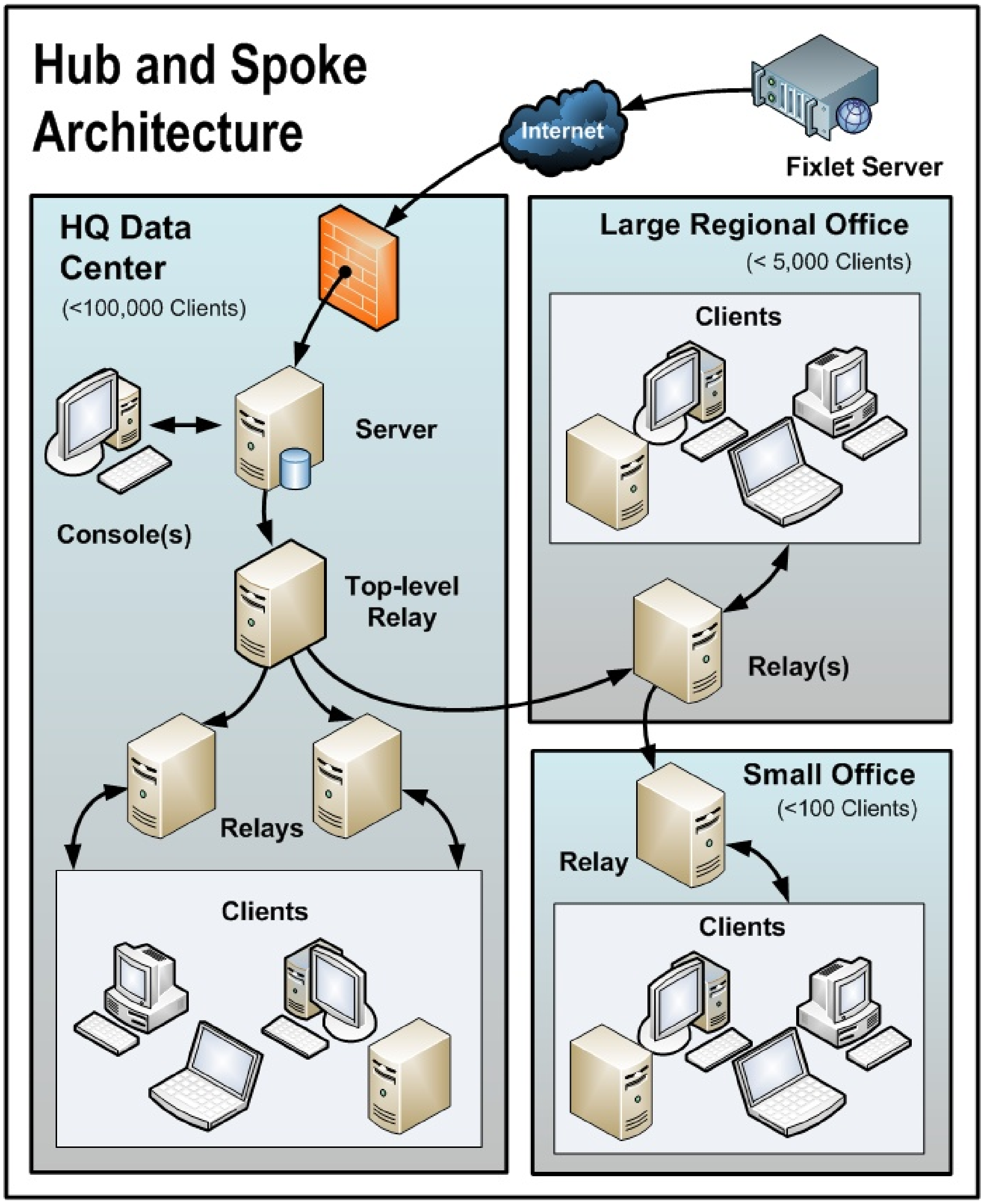


Note the following about the diagram:

- 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 . 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 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 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 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 data.
- Bandwidth throttling at the relay level is very helpful in this configuration. The 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 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.

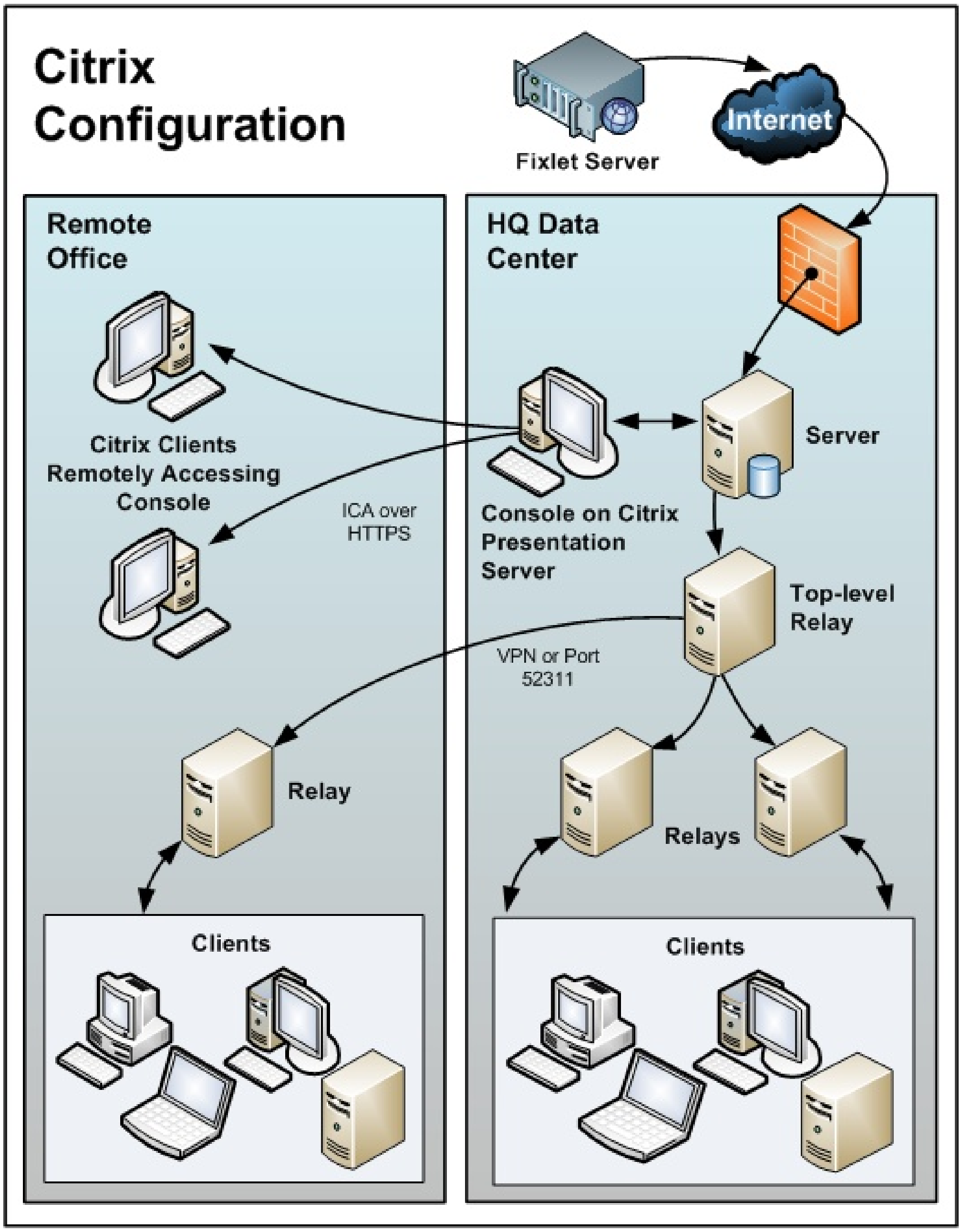
The relays are configured to manually create the optimal hierarchy. The hierarchy has three levels (from the top down):

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 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, Windows Terminal Server, 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

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 allows a single server to support hundreds of thousands of computers.

Assumptions

The process of getting the 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:

- servers can make connections to the Internet on port 80. The server can be set up to use a proxy, which is a common configuration. For more information see Chapter 12, "Setting up a proxy connection," on page 141.

  Alternatively, an air-gap can be used to physically separate the server from the Internet Fixlet server. For more information, see Downloading files in air-gapped environmentsthe *Configuration Guide*.
- Each 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 server.
- Each 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 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 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 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 for Lifecycle Management 9.1.

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 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 10.5. For information about how to install DB2 server on Red Hat Enterprise Linux Server 64-bit see "Installing and configuring DB2" on page 81 and Installation methods for IBM data server clients.
  - Red Hat packages required by Linux server and Web Reports components:

    `cyrus-sasl-lib.x86_64`

    `libstdc++.x86_64` and all their prerequisites

    `pam.x86_64`

    `krb5-libs.x86_64`

    `fontconfig.x86_64` (Web Reports only)

    `libXext.x86_64` (Web Reports only)

    `libXrender.x86_64` (Web Reports only)

    `zlib.x86_64` (Web Reports only)

  Note: Windows servers cannot be migrated to Linux servers.

  Minimum disk space requirements to install server and Web Reports on Linux:

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

  Web Reports: 250MB; DB2: 700MB

Console requirements

To find the latest information about console requirements, see IBM Endpoint Manager for Lifecycle Management 9.1.

The 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 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 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 Prerequisites of IBM Endpoint Manager for Lifecycle Management 9.1. .

Database requirements

The database stores all the data retrieved from the clients. Before installing the server, ensure that the database requirements are met.

- 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 server has the `sa` rights for the MSSQL Server to create the database and its tables.
- server on Red Hat Enterprise Linux systems supports the following configurations:
  - If the DB2 server is installed locally: DB2 10.5 Enterprise server Edition 64-bit or Workgroup Server Edition 64-bit.
  - If the DB2 server is installed remotely: IBM Data Server client 10.5.

  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.

For more information about the supported version of databases see Prerequisites of IBM Endpoint Manager for Lifecycle Management 9.1.

Security requirements

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

Before you can install , 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.

Fixlets are also digitally-signed. The Fixlet site author signs each message with a key that can be traced back to the 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 Fixlets you receive are from the original certified author.

There are a few other security-related issues to address before installing 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 -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: In your environment, if you reach the Internet through a proxy configure the connection as described in Chapter 12, "Setting up a proxy connection," on page 141. If you have firewall restrictions, see "Configuring a Local Firewall" on page 39.

To maintain a physical disconnect from the Internet see Downloading files in air-gapped environmentsthe *Configuration Guide*.

- 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 lock-down procedures might cause the servers to function incorrectly. Contact your IBM software support if you have any specific questions about lock-down 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 server should connect to the network at 100 mbps or higher.
- Consoles should have high speed connections to the server (100 mbps or higher)
- The Windows Firewall must be turned off on the server machine.
- The client must be installed on the 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 the Configuration Guide.. For information about larger installations, see Deployment Scenarios.

The 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 issues, see Performance Configurations.

Chapter 4. Security Configuration Scenarios

To improve the computer security, V9.1 provides the capability to follow the NIST security standards by configuring an enhanced security option. This setting enables SHA-256 as the hashing algorithm for digital signatures as well as content verification. It also enables the TLS 1.2 communication among the components.

You can set the enhanced security option only after the V9.1 installation or the upgrade of all components to V9.1. If you have a mixed environment, to keep the product compatibility with earlier versions of the components, do not set the enhanced security option or, before setting it, upgrade the components to V9.1.

Note: When you set this option you configure a very restricted security environment and the product performance might get worse. You can enable or disable this security setting at any time by editing the masthead file. For additional information see the Configuration Guide.

In addition to the enhanced security setting, you can now set a check for verifying the file download integrity using the SHA-256 algorithm. If you do not set this option, the file download integrity check is run using the SHA-1 algorithm. This new option does not break the compatibility with V9.0 components and can be set only if you set the enhanced security option.

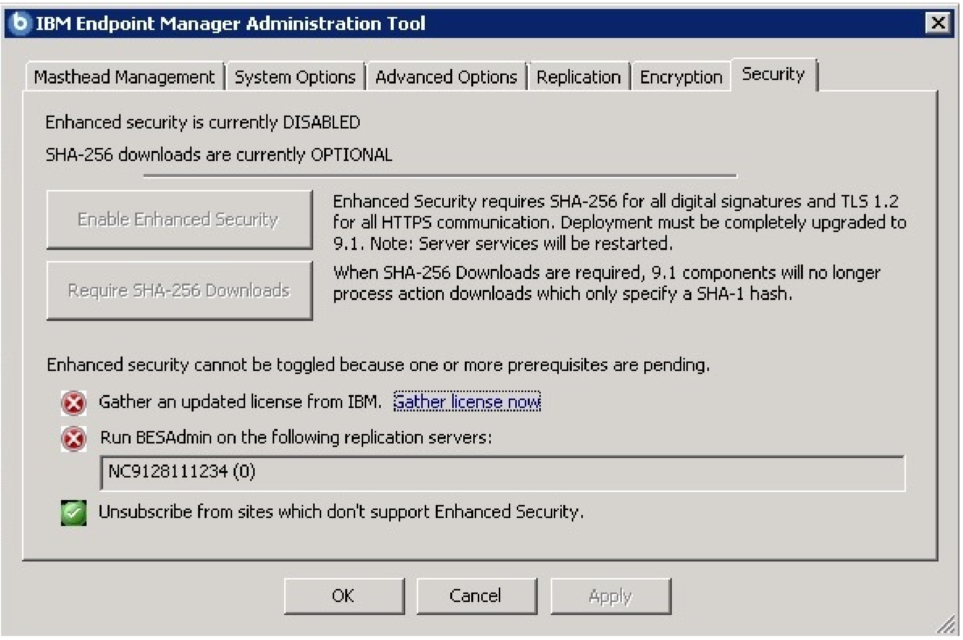
In a complex environment, you can enable the enhanced security option, only after all the DSA servers are upgraded to V9.1 and have got a new license.

Important: After you turn on the enhanced security option, you cannot roll back to a previous version of , even if you turn the option off. However, when needed, you can run a disaster recovery restore from V9.1 to V9.1 regardless of the enhanced security option setting. For additional information see Chapter 13, “Running backup and restore,” on page 153.

On Windows Systems

You can set the enhanced security option by performing the following steps:

1. Run the Administration Tool by clicking **Start > All Programs > > Administration Tool.** .
2. Browse to the location of your site license (`license.pvk`) and click **OK**.
3. Select the **Security** tab. The following window is displayed:



IBM Endpoint Manager Administration Tool

Enhanced security is currently DISABLED

SHA-256 downloads are currently OPTIONAL

Enhanced Security requires SHA-256 for all digital signatures and TLS 1.2 for all HTTPS communication. Deployment must be completely upgraded to 9.1. Note: Server services will be restarted.

When SHA-256 Downloads are required, 9.1 components will no longer process action downloads which only specify a SHA-1 hash.

Enhanced security cannot be toggled because one or more prerequisites are pending.

☒ Gather an updated license from IBM. Gather license now

☒ Run BESAdmin on the following replication servers:

NC9128111234 (0)

☑ Unsubscribe from sites which don't support Enhanced Security.

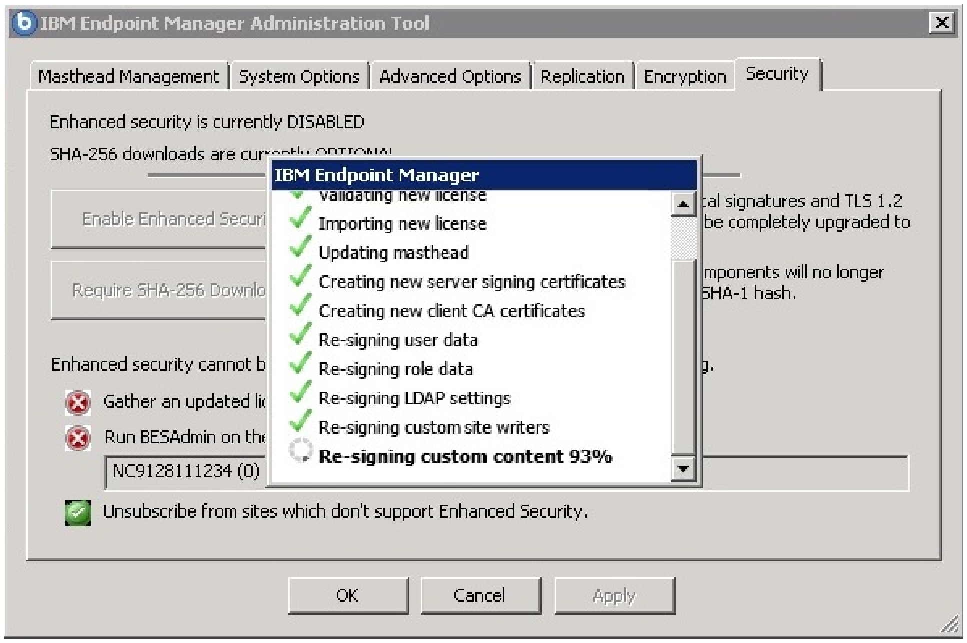
You can now enable the enhanced security options.

If you upgraded from an earlier version and the sites to which you were subscribed, supported the enhanced security option, the **Unsubscribe from sites which don't support Enhanced Security** is not selected.

The checkbox **Run BESAdmin on the following replication servers** is not checked until the product verifies that all servers involved in a Disaster Server Architecture (DSA) are version 9.1 and have the updated license.

4. Click **Gather license now** if you want to use the security enhancements provided with version 9.1. If you do not click you will use the security behavior provided by version 9.0.

   When you click **Gather license now** your updated license is gathered from the IBM site and is distributed to the clients. This step ensures that you use the updated license authorizations if you specified an existing licence file during the installation steps.



IBM Endpoint Manager Administration Tool

Enhanced security is currently DISABLED

SHA-256 downloads are currently OPTIONAL

IBM Endpoint Manager

- ✓ Validating new license
- ✓ Importing new license
- ✓ Updating masthead
- ✓ Creating new server signing certificates
- ✓ Creating new client CA certificates
- ✓ Re-signing user data
- ✓ Re-signing role data
- ✓ Re-signing LDAP settings
- ✓ Re-signing custom site writers
- **Re-signing custom content 93%**

…al signatures and TLS 1.2 … be completely upgraded to

…mponents will no longer … SHA-1 hash.

Enhanced security cannot b…

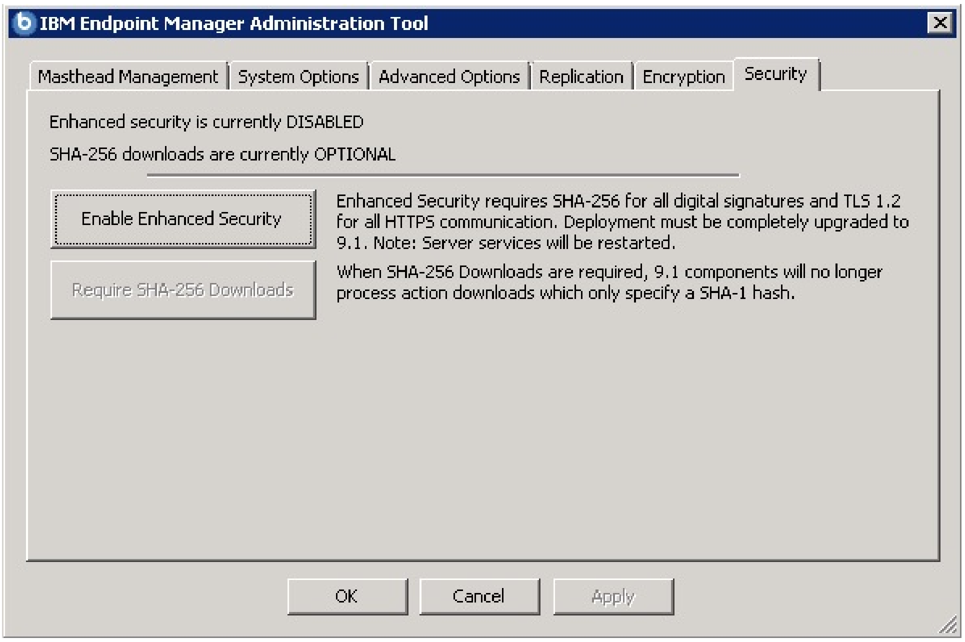
☒ Gather an updated li…

☒ Run BESAdmin on the…

NC9128111234 (0)

✓ Unsubscribe from sites which don't support Enhanced Security.

5. When the three check marks are green, you can set the enhanced security by clicking **Enable Enhanced Security**:



IBM Endpoint Manager Administration Tool

Enhanced security is currently DISABLED

SHA-256 downloads are currently OPTIONAL

Enhanced Security requires SHA-256 for all digital signatures and TLS 1.2 for all HTTPS communication. Deployment must be completely upgraded to 9.1. Note: Server services will be restarted.

When SHA-256 Downloads are required, 9.1 components will no longer process action downloads which only specify a SHA-1 hash.

6. To ensure that data has not changed after you download it using the SHA-256 algorithm click **Enable Enhanced Security**. If you do not select this option, the integrity check of the downloaded files is run using the SHA-1 algorithm.

   Note: You can enable the **Require SHA-256 Downloads** option only after you enable the **Enable Enhanced Security** option.

For additional information about how to create or edit the masthead, see “Step 2 - Requesting a license certificate and creating the masthead” on page 42 or the Configuration Guide..

On Linux Systems

You can set the security options after you install V9.1 or upgrade it to V9.1, by running the following command as super user:

```
./BESAdmin.sh -securitysettings -sitePvkLocation=<path+license.pvk>
             -enableEnhancedSecurity -requireSHA256Downloads
```

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

The full syntax of the `./BESAdmin.sh -securitysettings` is the following:

```
./BESAdmin.sh -securitysettings -sitePvkLocation=<path+license.pvk>
   [-sitePvkPassword=<password>]
   { -status | {-enableEnhancedSecurity|-disableEnhancedSecurity}
   | {-requireSHA256Downloads|-allowSHA1Downloads} }
```

where:

status Shows the status of the security settings in your environment.

Example:

```
BESAdmin.sh -securitysettings -sitePvkLocation=/root/backup/license.pvk
-sitePvkPassword=mypassw0rd -status

Enhanced security is currently ENABLED
SHA-256 downloads are currently OPTIONAL
```

enableEnhancedSecurity | disableEnhancedSecurity
Enables or disables the enhanced security that adopts the SHA-256 cryptographic digest algorithm for all digital signatures as well as content verification and the TLS 1.2 protocol for communications among the Endpoint Manager components.

Note: If you use this setting you break backward compatibility because version 9.0 or earlier components cannot communicate with the version 9.1 server or relays.

requireSHA256Downloads
Ensures that data has not changed after you download it using the SHA-256 algorithm.

Note: You can set **requireSHA256Downloads** only if you also set **enableEnhancedSecurity**.

allowSHA1Downloads
Ensures that the file download integrity check is run using the SHA-1 algorithm.

Chapter 5. 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 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 license authorization file, you are ready to create a personalized **action site masthead** that, in turn, allows you to install and use .

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 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. 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 console and Web Reports.

Note: The evaluation installation does not support the enhanced security option. For more information about this feature see Chapter 4, “Security Configuration Scenarios,” on page 23.

Production installation

To install a production copy of , 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 license authorization file. You must use this file the first time you run a production installation. If you have not yet purchased a license, visit the 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 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 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.

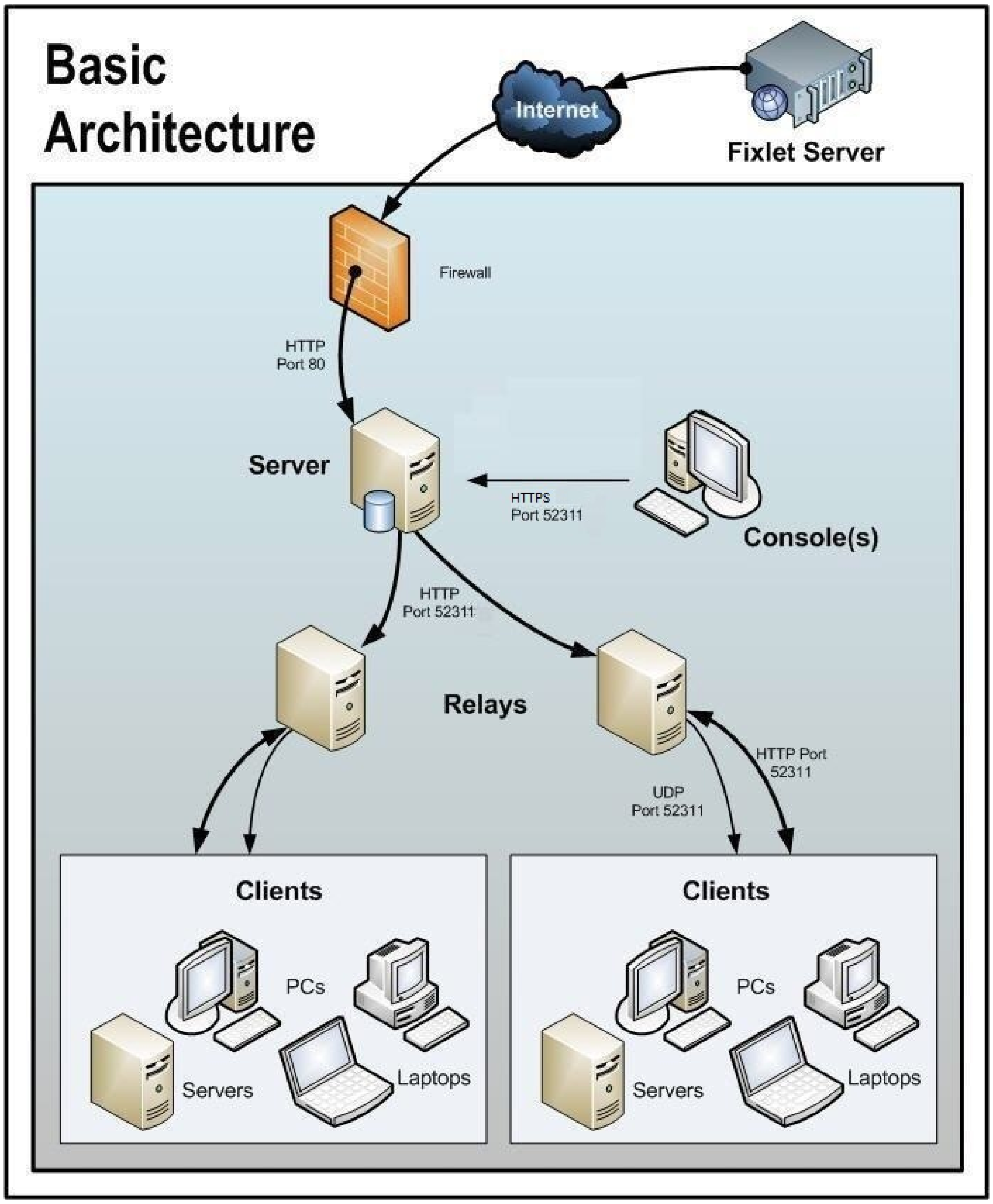
Production license
Use this option if you have already the production license `license.crt` and the private key file on the machine on which you are installing the server, but did not complete the server installation.

An existing masthead
Use this type of installation to reinstall the 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 server IP address or server name, port number, and locking behavior. It contains information necessary for the digital signature security scheme that uses (the masthead contains the public key information), and the licensing information that allows users to run with a specified number of users for a specified length of time. The 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 Console and WebReports

A basic installation

A simplified deployment is shown in the following diagram. There is at least one server that gathers Fixlets 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 Fixlets back to the relay, which compresses the data and passes it back up to the servers.



This window displays a basic installation. A simplified deployment is shown in the following diagram. There is at least one server that gathers Fixlets 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 Fixlets back to the relay, which compresses the data and passes it back up to the servers.

The 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 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 realtime 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 , 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 Fixlets into your network. Clients gather Fixlets 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 to work correctly. View the article about network traffic at the 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 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

includes the important ability to add multiple, fully redundant servers – a feature called Distributed Server Architecture (DSA). Each server maintains a replica of the 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 reestablished, the servers automatically reconnect and sync up. The relays and clients are also capable of successfully recovering from such a disconnect. DSA provides the following capabilities:

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

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

For more information about using server redundancy, see the Configuration Guide..

Chapter 6. Managing licenses

You must obtain a license key before you can install and use . 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	You must purchase a license in the following situations: • You want to purchase . • Your trialware license expired. • Your paid license expired. • Your license is over-deployed and an updated license.crt is required for the increased license count purchase. • Your upgrade license expired. 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.
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.
Generate your license files during installation: • Create the private key file • Request and get the license certificate • Generate the masthead file	During the installation of the Server, after you specify the license authorization file, you generate the `license.pvk` file, which is your private key file. You also request and get the `license.crt` file, which is your public key file. These two files together complete your license. See Requesting the license files on Windows and Step 2 - Installing the Server.

Back up your license files	Store your license.crt (public key) file with your existing license.pvk (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. In particular the license.pvk file is the part of your key files that needs to stay private. The license.crt 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.
Check license status and distribute the new license and masthead files	You can see the notifications about expired license and other license issues for the license that you imported into the console. See "Distributing the Updated License and Masthead" on page 34.

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

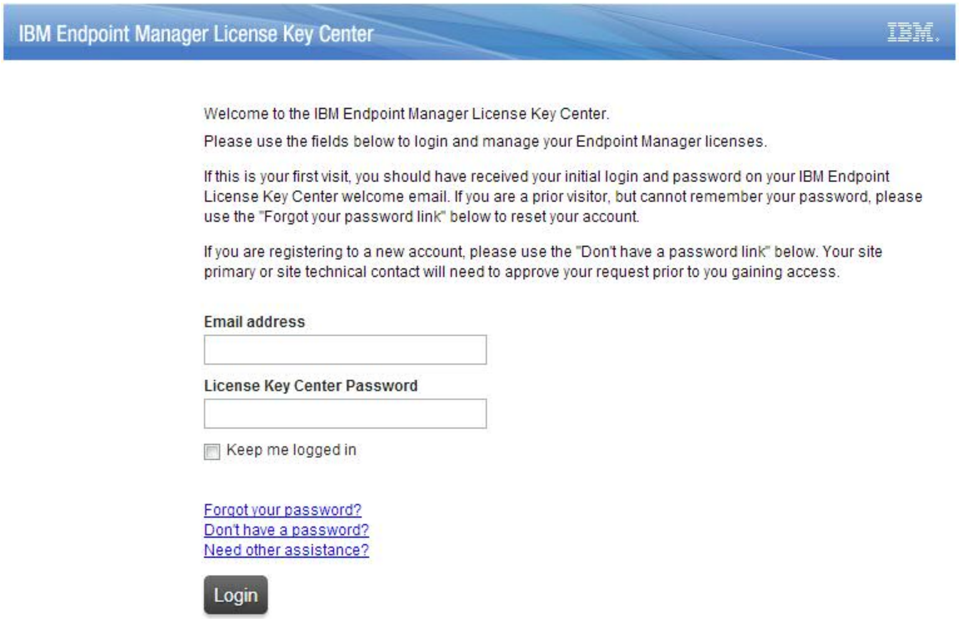
1. Purchase a license.
2. Get an authorization file from the IBM Endpoint Manager License Key Center site.
3. Start the installation and enter the authorization file when requested to get the `license.crt` file. At the end of the process both the public key and private key license files are generated 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.



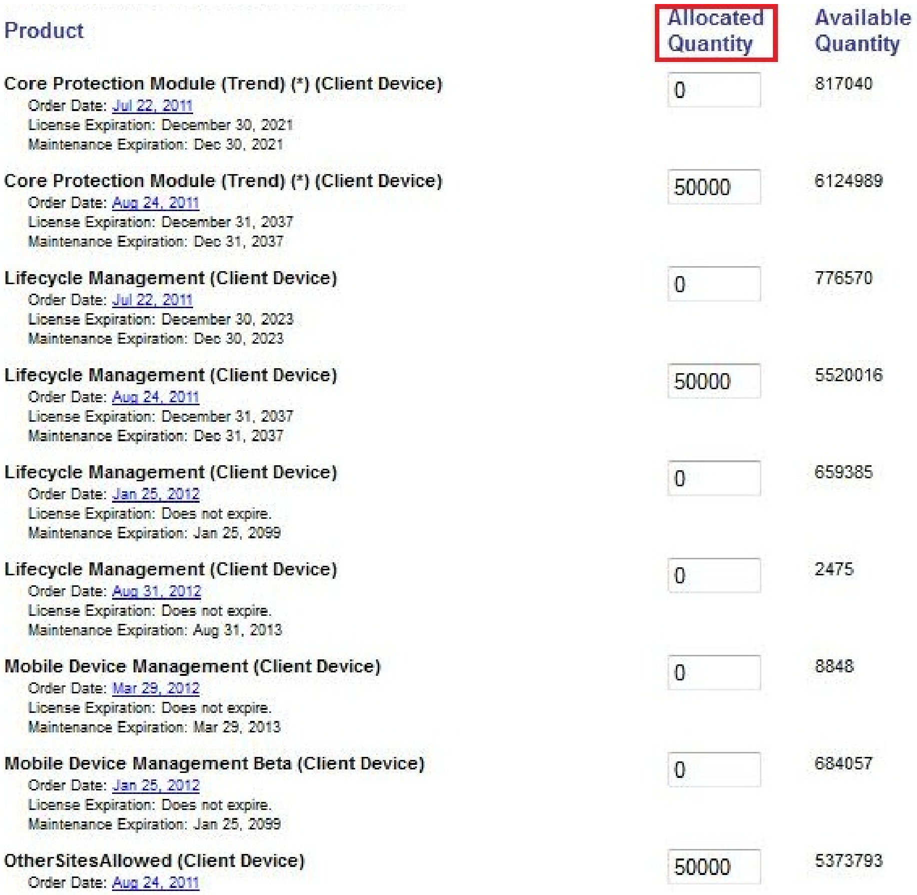
Welcome to the IBM Endpoint Manager License Key Center.

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.

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



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

Licensing Assistance

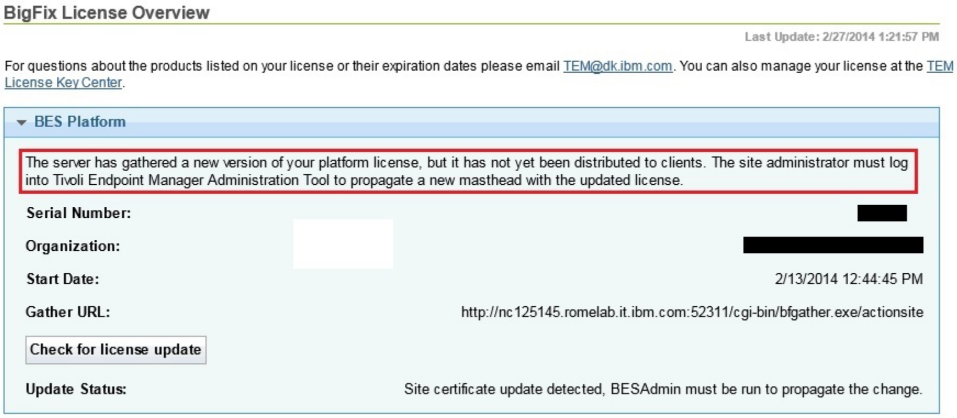
For specific problems with your license such as license expiration date, entitlement counts, or lost authorization files, contact the IBM Endpoint Manager licensing team at TEM@dk.ibm.com. Support questions not related to licensing, such as general installation problems, setup configuration, deployment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

Distributing the Updated License and Masthead

When you upgrade to V9.1, all existing license certificates are updated to contain both SHA-1 and SHA-256 signatures. If you are connected to Internet, the message of a new license ready to be distributed to the clients together with the masthead is displayed in the **License Overview** dashboard after an automatic periodic gather or a manual check.

To force your server to check immediately run the following steps:

1. Open the console.
2. go to the **BigFix Management** domain.
3. click the **License Overview** node
4. Click **Check for license update**. You might receive a notification that deployment has gathered an update to your license (a new `license.crt` file):



BigFix License Overview

Last Update: 2/27/2014 1:21:57 PM

For questions about the products listed on your license or their expiration dates please email TEM@dk.ibm.com. You can also manage your license at the TEM License Key Center.

BES Platform

The server has gathered a new version of your platform license, but it has not yet been distributed to clients. The site administrator must log into Tivoli Endpoint Manager Administration Tool to propagate a new masthead with the updated license.

Serial Number: [redacted]

Organization: [redacted]

Start Date: 2/13/2014 12:44:45 PM

Gather URL: http://nc125145.romelab.it.ibm.com:52311/cgi-bin/bfgather.exe/actionsite

Update Status: Site certificate update detected, BESAdmin must be run to propagate the change.

Note: This message might appear either because IBM needs to update the license or because you requested an update of your license. If you requested an update of your license, you receive a new `license.crt` file, that you must save on your server computer.

To distribute the updated license, resign the masthead and the objects in the database with both SHA-1 and SHA-256 signatures, run the Administration Tool (`./BESAdmin.sh` on Linux as super user).

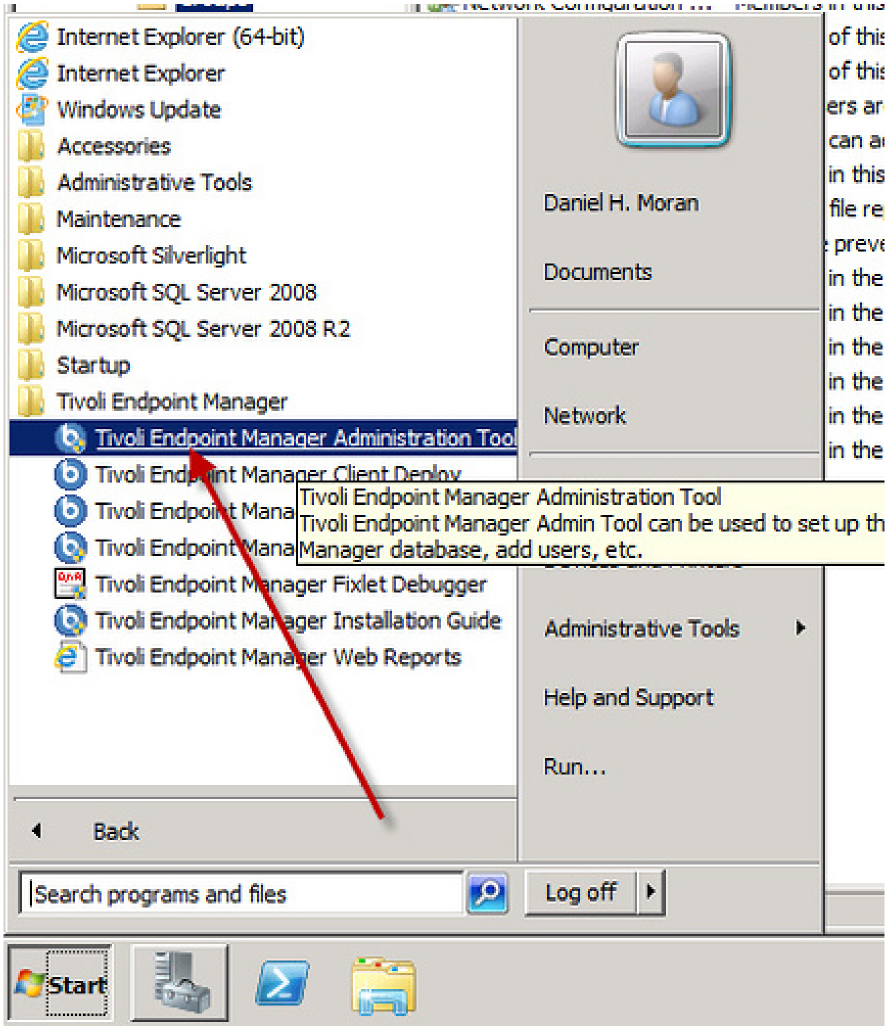
If you are in an air-gapped environment the update of the license is not processed automatically. You can retrieve the license from the IBM site by using the AirgapTool utility. After importing it, you are notified from the License dashboard that a license update is ready to be distributed. You must run the Administration tool (`./BESAdmin.sh` on Linux) to distribute the updated license, and to resign the masthead and the database objects.

For more information about how to distribute the masthead on the clients see "Distributing the masthead from the Windows server to clients" and "Distributing the masthead from the Linux server to the clients" on page 37.

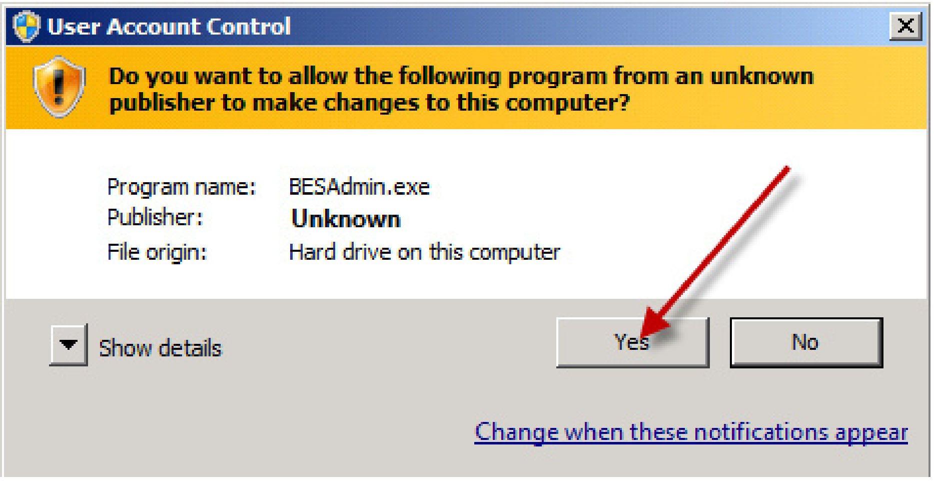
Distributing the masthead from the Windows server to clients

From an Windows server, you can distribute a new masthead file with an updated license certificate, that extends your license, seat count, or entitlements to the clients, as follows:

1. Open the Administration Tool by selecting **Start** > **All Programs** > > **Administration Tool**. After you log in, the installation Admin account distributes the masthead to the clients.


Internet Explorer (64-bit)
Internet Explorer
Windows Update
Accessories
Administrative Tools
Maintenance
Microsoft Silverlight
Microsoft SQL Server 2008
Microsoft SQL Server 2008 R2
Startup
Tivoli Endpoint Manager
Tivoli Endpoint Manager Administration Tool
Tivoli Endpoint Manager Client Deploy
Tivoli Endpoint Mana
Tivoli Endpoint Mana
Tivoli Endpoint Manager Fixlet Debugger
Tivoli Endpoint Manager Installation Guide
Tivoli Endpoint Manager Web Reports
Back
Search programs and files
Daniel H. Moran
Documents
Computer
Network
Administrative Tools
Help and Support
Run...
Log off
Start

Tivoli Endpoint Manager Administration Tool
Tivoli Endpoint Manager Admin Tool can be used to set up th
Manager database, add users, etc.

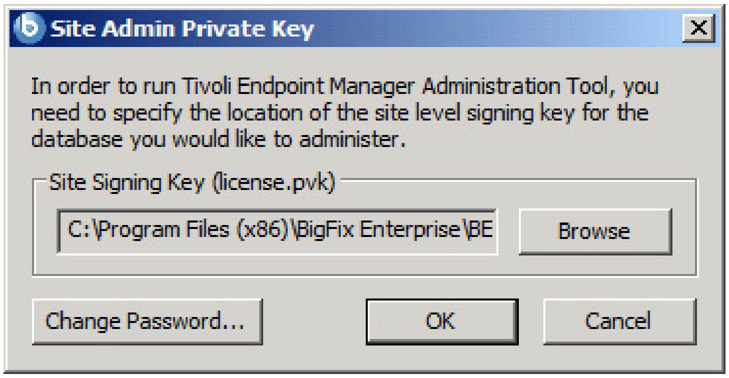


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name: BESAdmin.exe
Publisher: **Unknown**
File origin: Hard drive on this computer

2. Choose your `license.pvk` file.

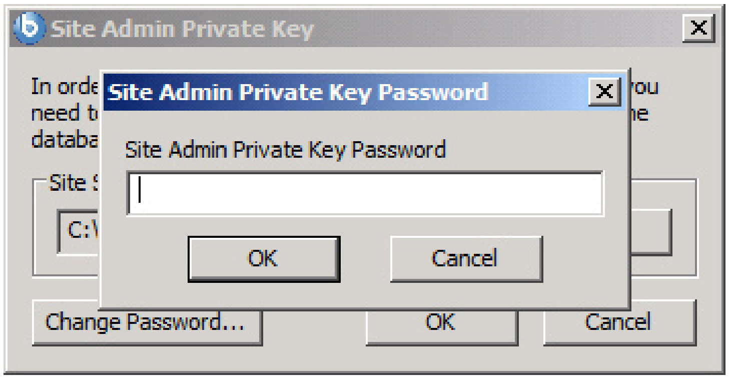


Site Admin Private Key

In order to run Tivoli Endpoint Manager Administration Tool, you need to specify the location of the site level signing key for the database you would like to administer.

Site Signing Key (license.pvk): C:\Program Files (x86)\BigFix Enterprise\BE

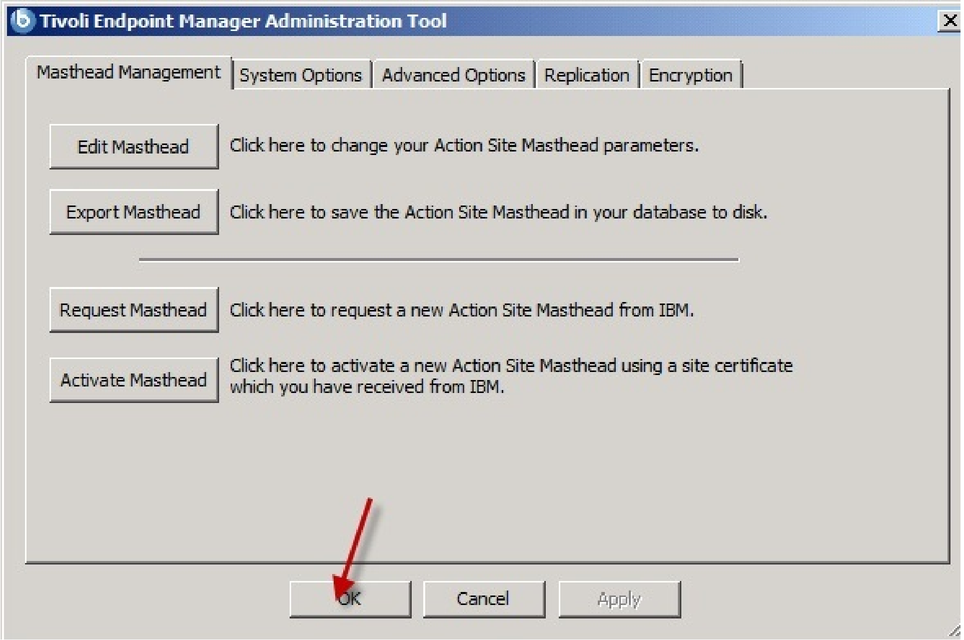
3. Enter your master (site level) password



Site Admin Private Key Password

Site Admin Private Key Password:

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



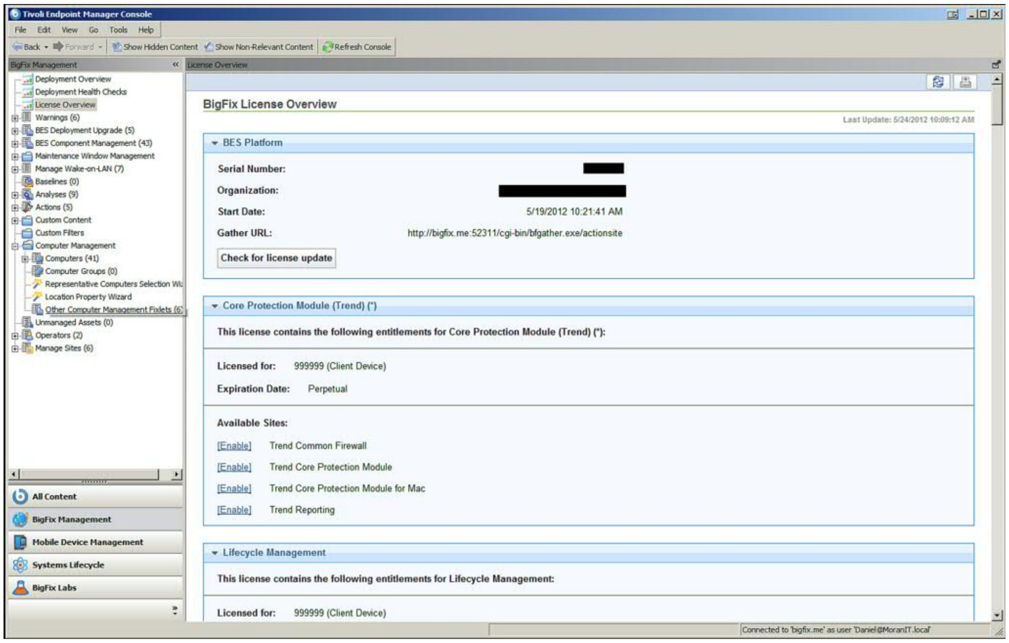
Click here to change your Action Site Masthead parameters.

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

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

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

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



BigFix License Overview

Last Update: 5/24/2012 10:09:12 AM

BES Platform

Serial Number: [redacted]

Organization: [redacted]

Start Date: 5/19/2012 10:21:41 AM

Gather URL: http://bigfix.me:52311/cgi-bin/bfgather.exe/actionsite

Core Protection Module (Trend) (*)

This license contains the following entitlements for Core Protection Module (Trend) (*):

Licensed for: 999999 (Client Device)

Expiration Date: Perpetual

Available Sites:

[Enable] Trend Common Firewall

[Enable] Trend Core Protection Module

[Enable] Trend Core Protection Module for Mac

[Enable] Trend Reporting

Lifecycle Management

This license contains the following entitlements for Lifecycle Management:

Licensed for: 999999 (Client Device)

Distributing the masthead from the Linux server to the clients

From an Linux server, you can distribute the updated license, resign the masthead and the database objects to the clients, by running the following command as super user:

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

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

Chapter 7. Before installing

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

Configuring a Local Firewall

If you have defined an active firewall on the computer where you are installing the server, you can decide to configure this firewall during the server installation in one of the following ways:

- During an interactive installation, the installation programs detects if a local firewall is active and you can specify if you want to configure it for the server.
- During a silent installation, you can set `CONF_FIREWALL=YES` in the response file to require the firewall configuration. For more information, see "Silent installation" on page 89.

When you specify to configure the firewall, the following two ports are opened:

- Port `52311` for UDP and TCP/IP
- Port `80` for Web Reports and TCP/IP

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 8. 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 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 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 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 **Installer**, which you can download from IBM.

Installation Steps

To install the product, perform the following steps:

1. Download .
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 installation.

Step 1 - Downloading IBM Endpoint Manager

Download from the IBM Passport Advantage portal.

You can download 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. Software required for installing Server

Software Name	Part Number	Image
IBM Endpoint Manager Platform Install V9.1 for Multiplatforms	CITM5ML	`IBM Endpoint Manager 9.1.1082.0.zip`

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

1. Copy the Server zip file `IBM Endpoint Manager 9.1.1082.0.zip` to your Windows Server.
2. Expand the zip file using the following command:

   ```
   unzip "IBM Endpoint Manager 9.1.1082.0.zip"
   ```

   You can find the `setup.exe` file to install the Windows Server in the `IBM Endpoint Manager 9.1.1082.0` folder.

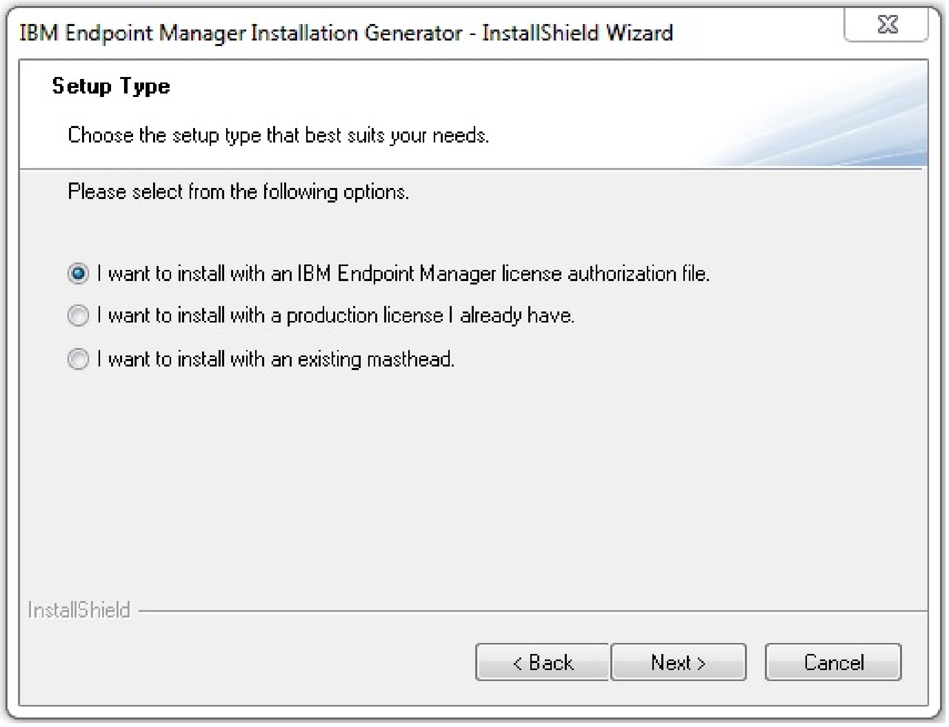
Step 2 - Requesting a license certificate and creating the masthead

Before you perform the steps below, you must have purchased a license and obtained an 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 . 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 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**.

   Note: If you choose the **Evaluation** installation, consider that this type of installation does not support the enhanced security option. For more information about this feature, see Chapter 4, "Security Configuration Scenarios," on page 23.
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.



IBM Endpoint Manager Installation Generator - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

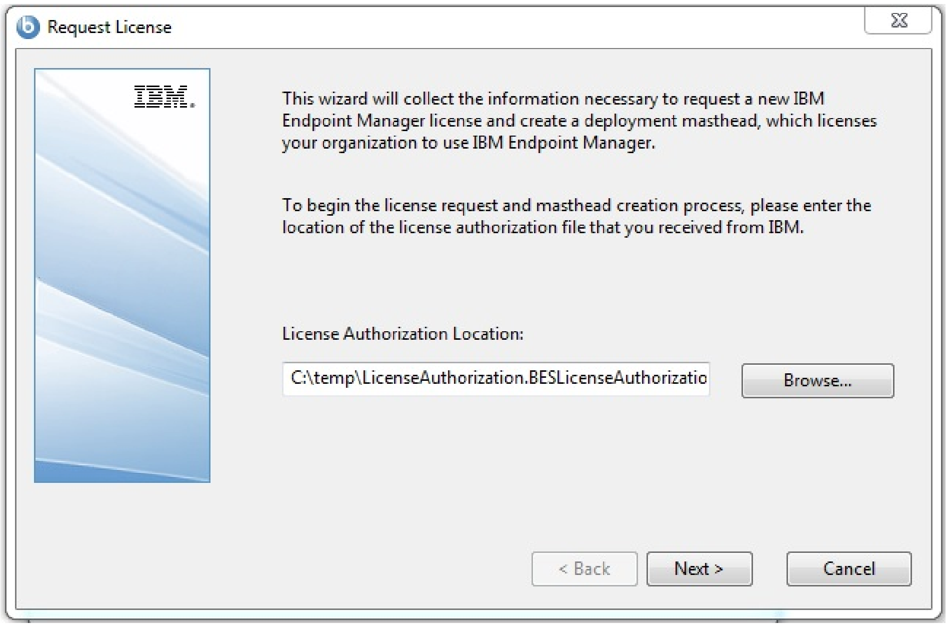
Please select from the following options.

● I want to install with an IBM Endpoint Manager license authorization file.

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

○ I want to install with an existing masthead.

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



Request License

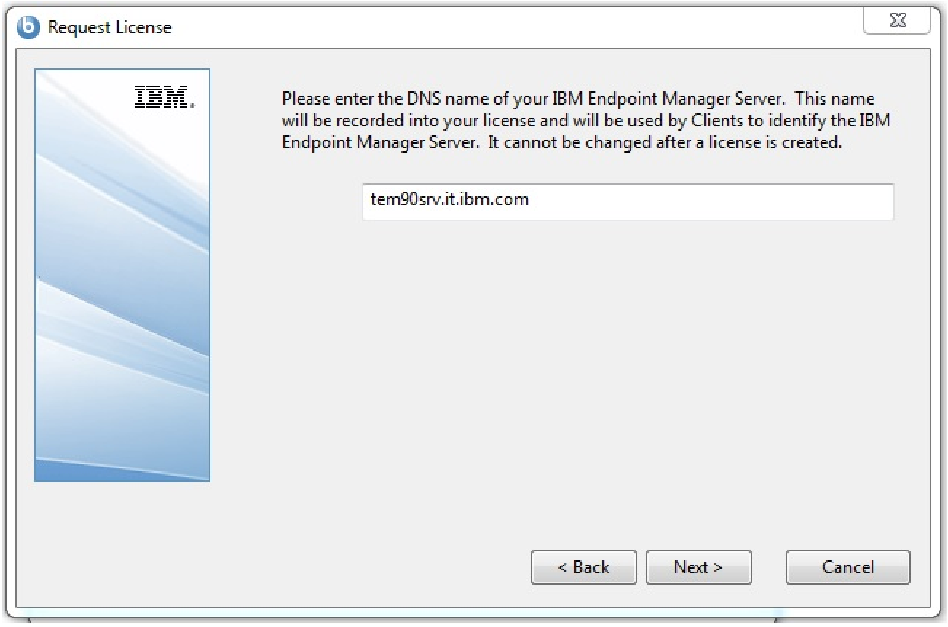
This wizard will collect the information necessary to request a new IBM Endpoint Manager license and create a deployment masthead, which licenses your organization to use IBM Endpoint Manager.

To begin the license request and masthead creation process, please enter the location of the license authorization file that you received from IBM.

License Authorization Location:

C:\temp\LicenseAuthorization.BESLicenseAuthorizatio

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



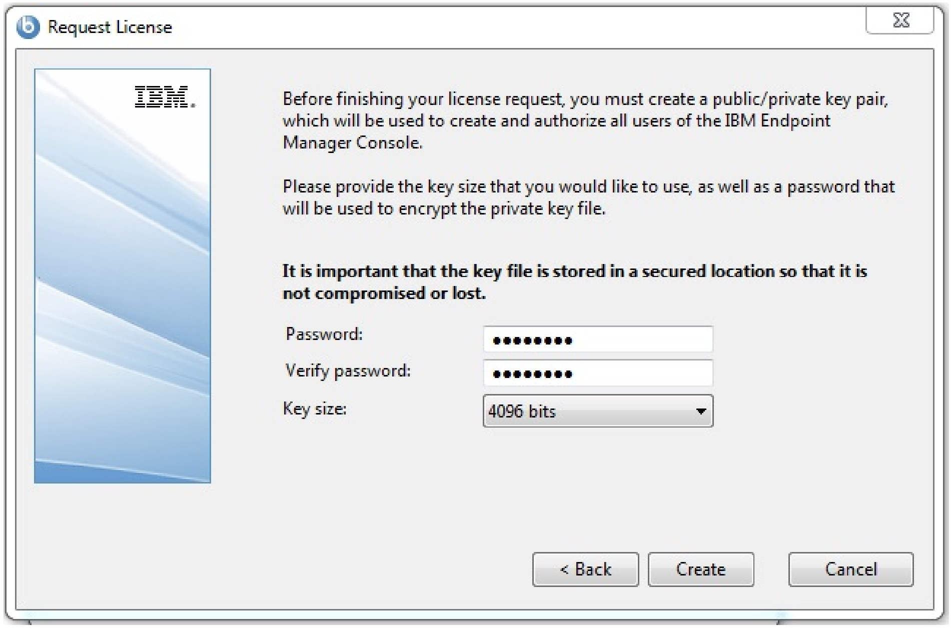
Request License

Please enter the DNS name of your IBM Endpoint Manager Server. This name will be recorded into your license and will be used by Clients to identify the IBM Endpoint Manager Server. It cannot be changed after a license is created.

tem90srv.it.ibm.com

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 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**.



Request License

Before finishing your license request, you must create a public/private key pair, which will be used to create and authorize all users of the IBM Endpoint Manager Console.

Please provide the key size that you would like to use, as well as a password that will be used to encrypt the private key file.

It is important that the key file is stored in a secured location so that it is not compromised or lost.

Password: ••••••••

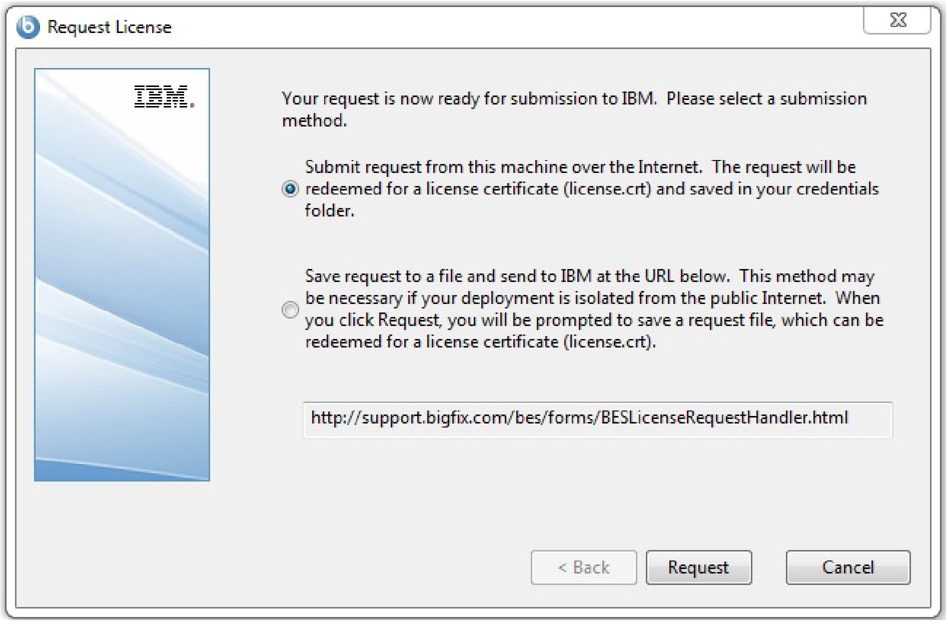
Verify password: ••••••••

Key size: 4096 bits

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

   Your request is now ready for submission to IBM. Please select a submission method.

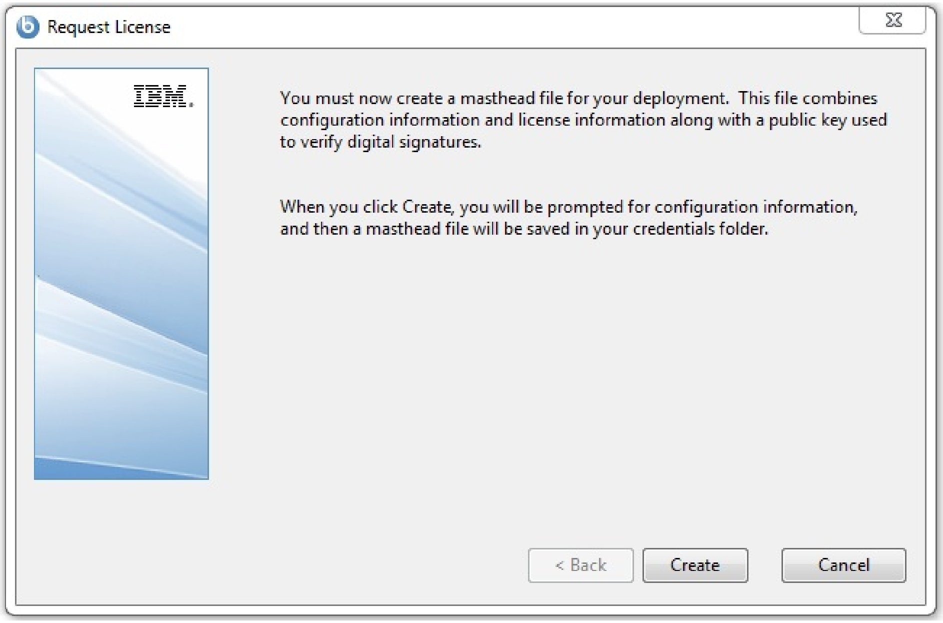
   ● Submit request from this machine over the Internet. The request will be redeemed for a license certificate (license.crt) and saved in your credentials folder.

   ○ Save request to a file and send to IBM at the URL below. This method may be necessary if your deployment is isolated from the public Internet. When you click Request, you will be prompted to save a request file, which can be redeemed for a license certificate (license.crt).

   http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html

   You are prompted for a location to save the resulting license certificate file (`license.crt`), and a request file is sent to 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 DNS name and your public key, all packaged into a single file.
8. Click **Request**. The Wizard retrieves your license certificate (`license.crt`) from the License server.

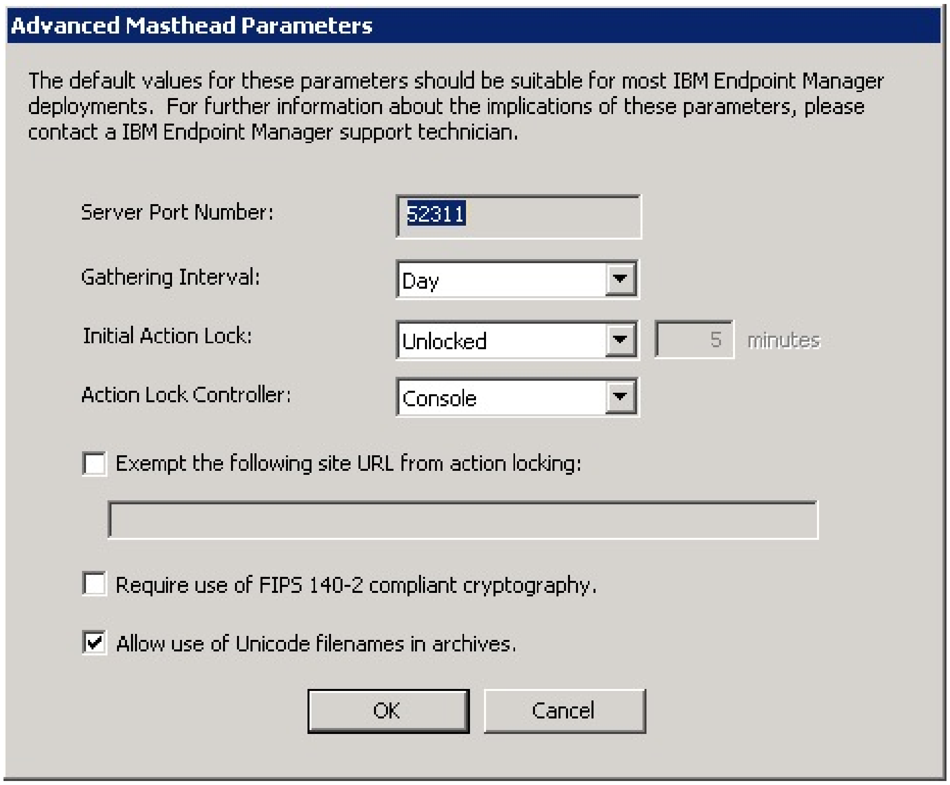
   Alternatively, if you are on an airgap without internet connectivity, choose the option to save the request as a file named `request.BESLicenseRequest`. Copy the file to a machine with internet connectivity and submit your request to the URL of the website shown in the installer. The page provides you 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



You must now create a masthead file for your deployment. This file combines configuration information and license information along with a public key used to verify digital signatures.

When you click Create, you will be prompted for configuration information, and then a masthead file will be saved in your credentials folder.

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.



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: 52311

Gathering Interval: Day

Initial Action Lock: Unlocked 5 minutes

Action Lock Controller: Console

□ Exempt the following site URL from action locking:

□ Require use of FIPS 140-2 compliant cryptography.

☑ Allow use of Unicode filenames in archives.

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, 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 components because it is reserved for proxy agents.

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).

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://`.

Require use of FIPS 140-2 compliant cryptography
Check this box to be compliant with the Federal Information Processing Standard in your network. This changes the masthead so that every 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.

Allow use of Unicode filenames in archives:
This setting specifies the codepage used to write filenames in the IBM Endpoint Manager archives. Check this box to write filenames UTF-8 codepage.

Do not check this box to write filenames using the local deployment codepage, for example Windows-1252 or Shift JIS. If you run a fresh install of IBM Endpoint Manager V9.1, by default, the filenames are written in UTF-8.

Note: If you upgraded your IBM Endpoint Manager environment to V9.1, by default, the filenames are written in the local deployment codepage.

Click **OK** when you are finished.

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

    Note: This step creates the installers for the client, console, and 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 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 **Installation Guide**.

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

1. If it is not already running, launch the Installation Guide (**Start > Programs > > 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 components. You can also Browse Install Folders. The component installers includes:
   - Install Server
   - Install Console
   - Install Clients
3. The 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

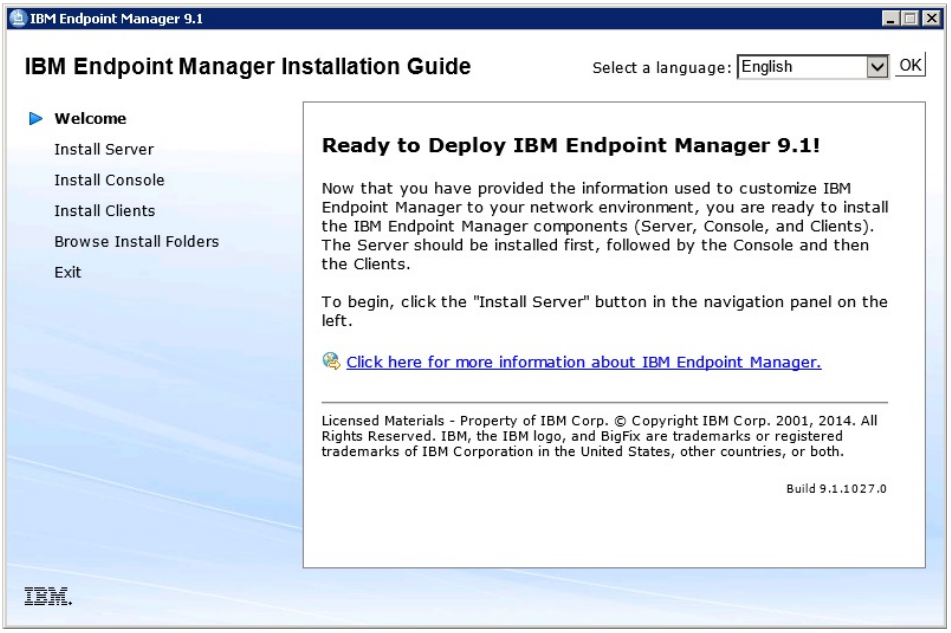
The server is the heart of the system. It runs on a server-class computer on your network, which must have direct Internet access as well as direct access to all the client computers in your network. Make sure your server meets the requirements outlined in IBM Endpoint Manager for Lifecycle Management 9.1.

Important: Ensure that the user that logs in to install the server has the `sa` rights for the MSSQL Server to create the database and its tables.
The default installation paths for the 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 > > Installation Guide**). A new panel opens.



IBM Endpoint Manager Installation Guide

Select a language: English OK

Ready to Deploy IBM Endpoint Manager 9.1!

Now that you have provided the information used to customize IBM Endpoint Manager to your network environment, you are ready to install the IBM Endpoint Manager components (Server, Console, and Clients). The Server should be installed first, followed by the Console and then the Clients.

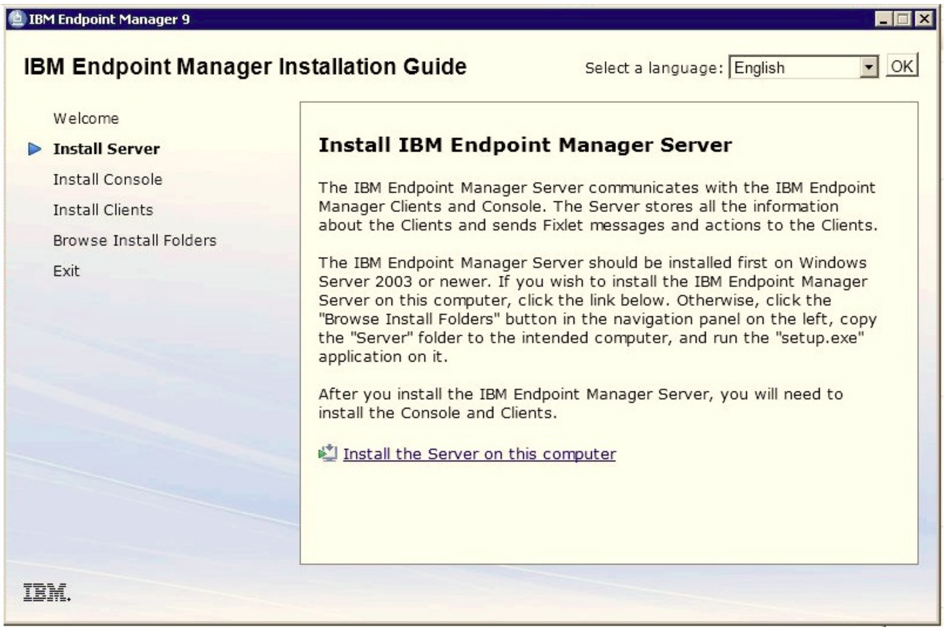
To begin, click the "Install Server" button in the navigation panel on the left.

Click here for more information about IBM Endpoint Manager.

Licensed Materials - Property of IBM Corp. © Copyright IBM Corp. 2001, 2014. All Rights Reserved. IBM, the IBM logo, and BigFix are trademarks or registered trademarks of IBM Corporation in the United States, other countries, or both.

Build 9.1.1027.0

2. Click **Install Server**:



IBM Endpoint Manager Installation Guide

Select a language: English OK

Install IBM Endpoint Manager Server

The IBM Endpoint Manager Server communicates with the IBM Endpoint Manager Clients and Console. The Server stores all the information about the Clients and sends Fixlet messages and actions to the Clients.

The IBM Endpoint Manager Server should be installed first on Windows Server 2003 or newer. If you wish to install the IBM Endpoint Manager Server on this computer, click the link below. Otherwise, click the "Browse Install Folders" button in the navigation panel on the left, copy the "Server" folder to the intended computer, and run the "setup.exe" application on it.

After you install the IBM Endpoint Manager Server, you will need to install the Console and Clients.

Install the Server on this computer

The 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 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. A dialog displays a list of the Server components about to be installed. In general, accept the default components and click **Next**.
5. A dialog prompts you to choose a **Single or Master Database** or a **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 first button. Click **Next**.

6. A dialog prompts you to choose if you want to **Use Local Database** or **Use Remote Database**. If you want to use another computer to host the Database, it must have a SQL Server already installed. The most common choice is to use the local database. If you are installing with a remote database, see "Server installation with remote database" on page 51.
7. If you select **Use Local Database**, you are prompted for a destination for the database server component. The default location is `C:\Program Files (x86)\Microsoft SQL Server`.
8. The installer prompts you for a destination for the Server components. The default location is `C:\Program Files (x86)\BigFix Enterprise\BES Server`, but you can specify a different location by clicking the **Browse** button. When you have chosen the destination, click **Next**.
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 port or errors will occur. Do not use port number 52314 for the network communication between the components because it is reserved for proxy agents.
10. The Web Reports Properties dialog prompts you to enter a location for the Web Reports web root folder (if different from the default) and the port number to use. The default and port number are also available for editing, if you want to change them.

    Note: If IIS is installed, the it chooses port 52312 instead.
11. The Server installer opens a window displaying the selected installation parameters of the components to be installed. 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. After the database has been initialized you are prompted to 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.
14. The Server installation is now complete. Ensure that the box labeled Run the IBM Endpoint Manager Diagnostic Tool is unchecked and then click **Finish** to exit the wizard.

    Note: If you select to run the diagnostic tools at this stage, some steps are likely to fail (for example, you haven't installed a client yet). However, the services and web reports should be running correctly.
15. Follow the instruction listed in "Installing the client manually" on page 65 to install the IBM Endpoint Manager Client locally on the same Windows system where you installed the Server.
16. If you configured a proxy to access the Internet, follow the steps described in Chapter 12, "Setting up a proxy connection," on page 141 to configure the proxy in your IBM Endpoint Manager environment.

    Note: You might need to wait until the proxy configuration is updated to start using the communication through the proxy.

17. On the Windows desktop select **Start > Run the Diagnostic Tool**. The Diagnostic Tool tabs show the results of the verification run in your environment. For more information about this tool, see **Running the Diagnostics Tool**.

Server installation with remote database:

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

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

Creating a new database user:

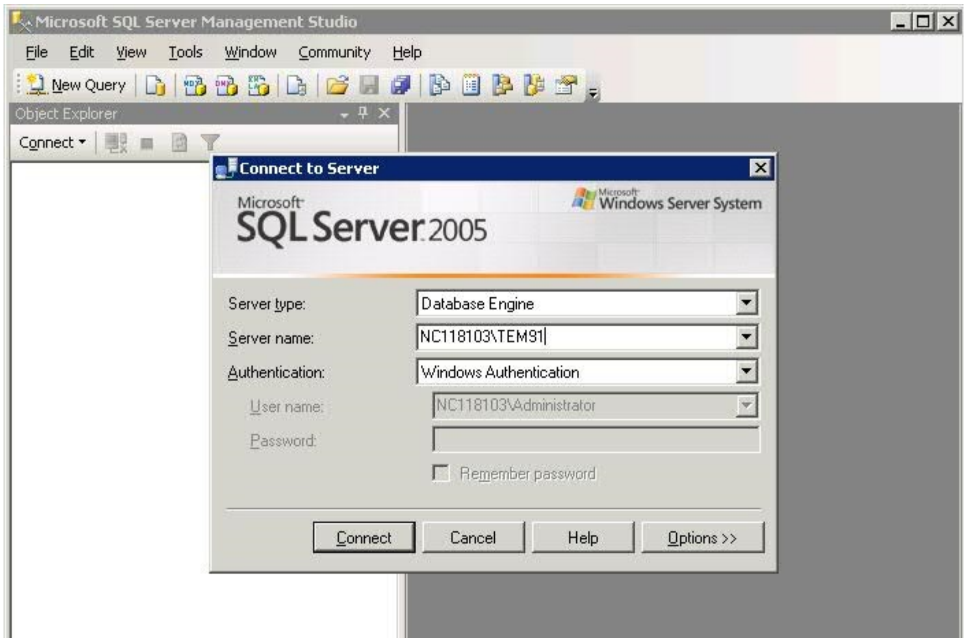
After creating a database instance on the machine where the Microsoft SQL Server is installed, if you do not want to use the SA user for the database connection, you must create a new user with SA Privileges.

To create a new user for a specific database instance, for example `TEM91`, 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 `TEM91` the server name is: `NC118103\TEM91`.



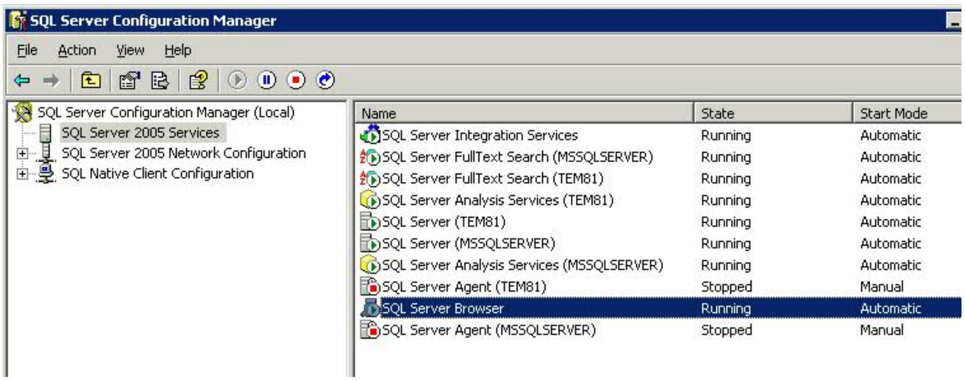
Server type: Database Engine
Server name: NC118103\TEM91
Authentication: Windows Authentication
User name: NC118103\Administrator
Password:

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:

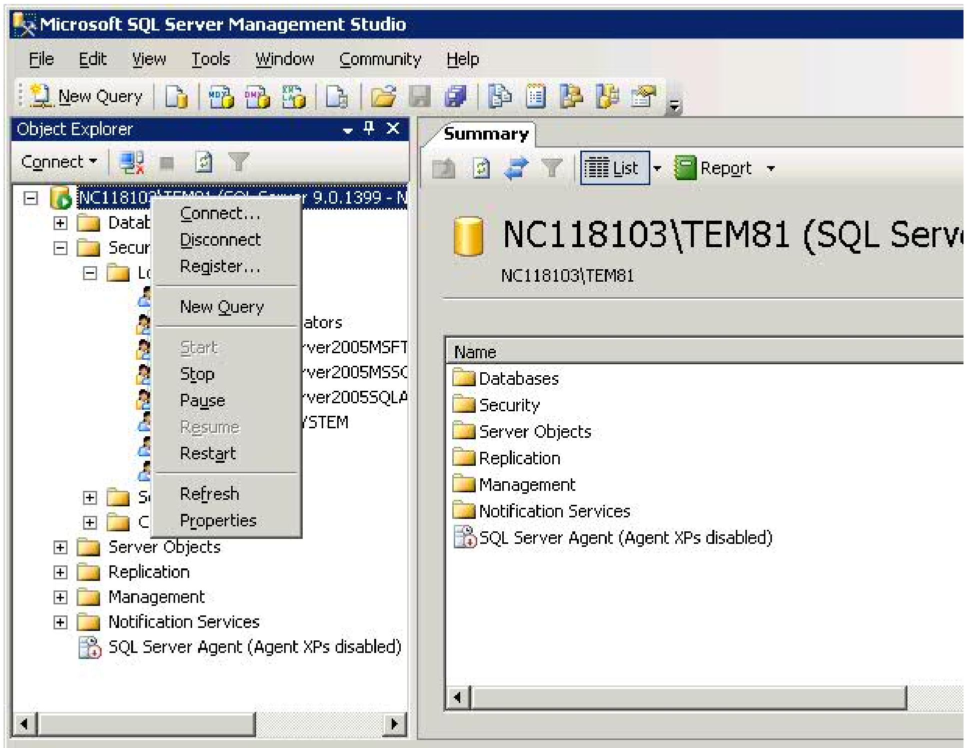

SQL Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
SQL Native Client Configuration

Name	State	Start Mode
SQL Server Integration Services	Running	Automatic
SQL Server FullText Search (MSSQLSERVER)	Running	Automatic
SQL Server FullText Search (TEM81)	Running	Automatic
SQL Server Analysis Services (TEM81)	Running	Automatic
SQL Server (TEM81)	Running	Automatic
SQL Server (MSSQLSERVER)	Running	Automatic
SQL Server Analysis Services (MSSQLSERVER)	Running	Automatic
SQL Server Agent (TEM81)	Stopped	Manual
SQL Server Browser	Running	Automatic
SQL Server Agent (MSSQLSERVER)	Stopped	Manual

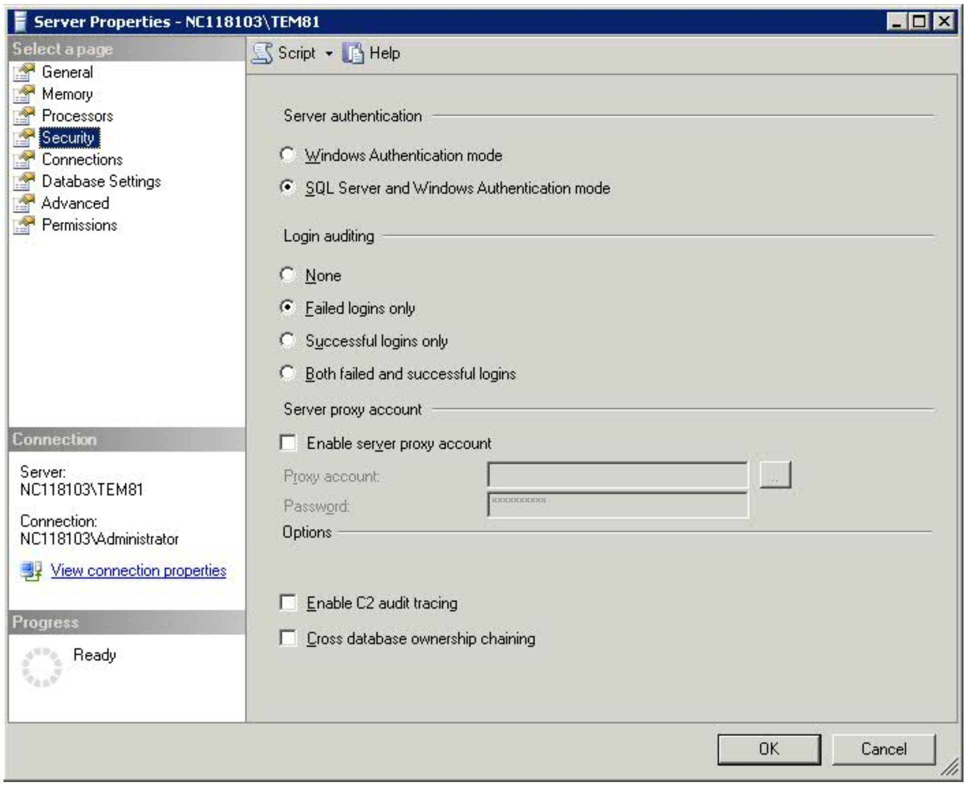
Enabling the SQL Server Authentication Mode:

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.



Server authentication

○ Windows Authentication mode

● SQL Server and Windows Authentication mode

Login auditing

○ None

● Failed logins only

○ Successful logins only

○ Both failed and successful logins

Server proxy account

□ Enable server proxy account

Proxy account:

Password: xxxxxxxxxx

Options

□ Enable C2 audit tracing

□ Cross database ownership chaining

Connection

Server:
NC118103\TEM81

Connection:
NC118103\Administrator

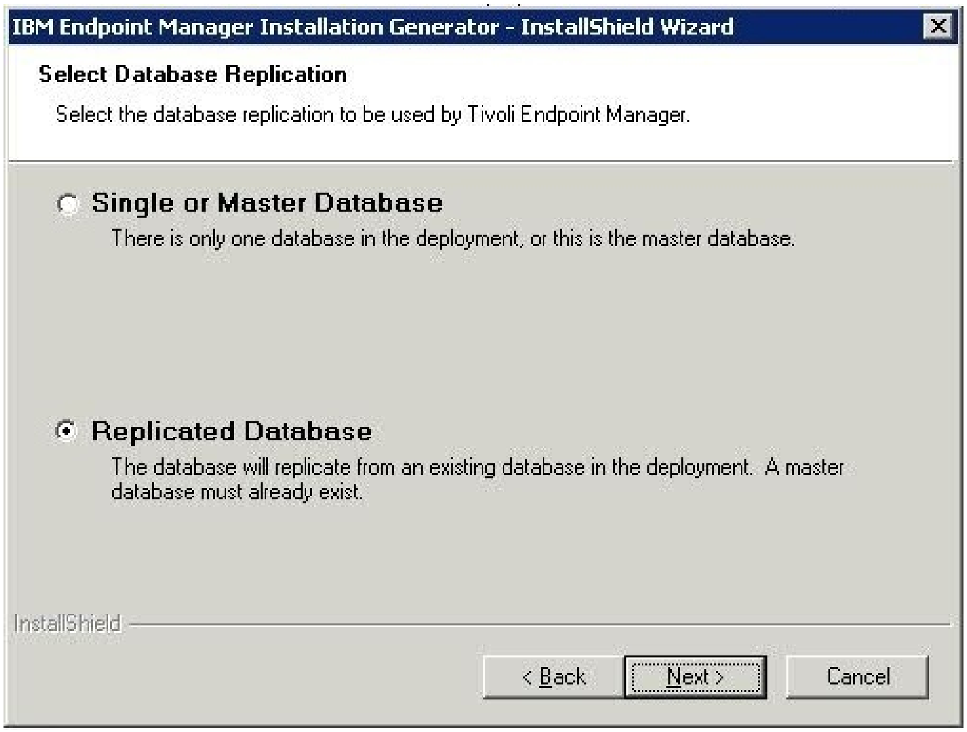
Progress

Ready

Installing a server with remote database SQL authentication:

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

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



IBM Endpoint Manager Installation Generator - InstallShield Wizard

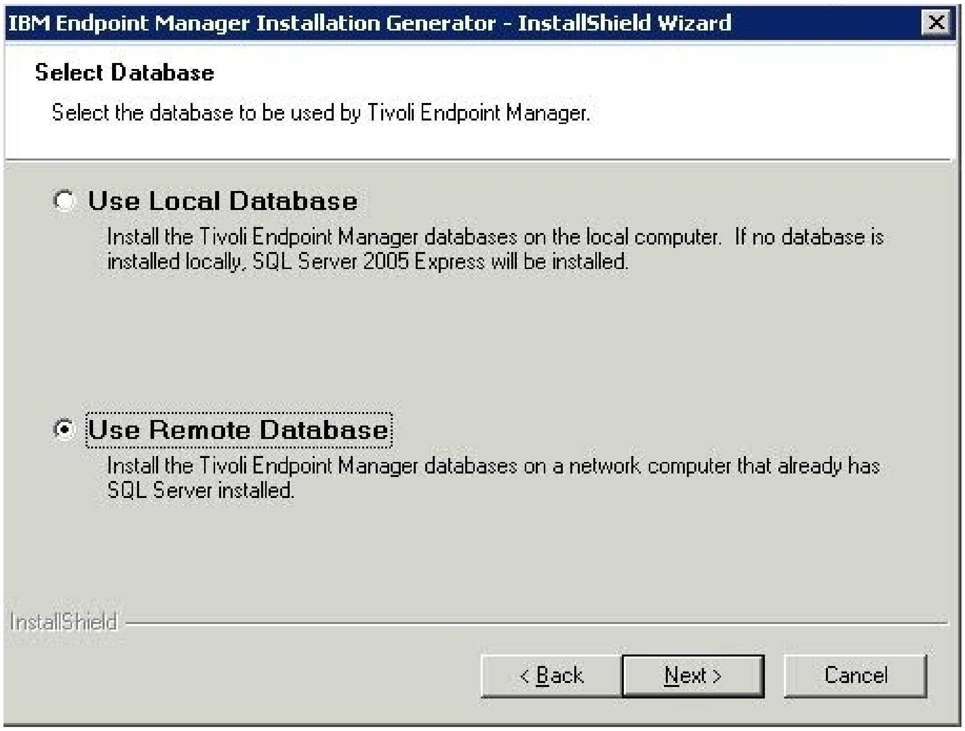
Select Database Replication

Select the database replication to be used by Tivoli Endpoint Manager.

○ **Single or Master Database**
There is only one database in the deployment, or this is the master database.

● **Replicated Database**
The database will replicate from an existing database in the deployment. A master database must already exist.

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



IBM Endpoint Manager Installation Generator - InstallShield Wizard

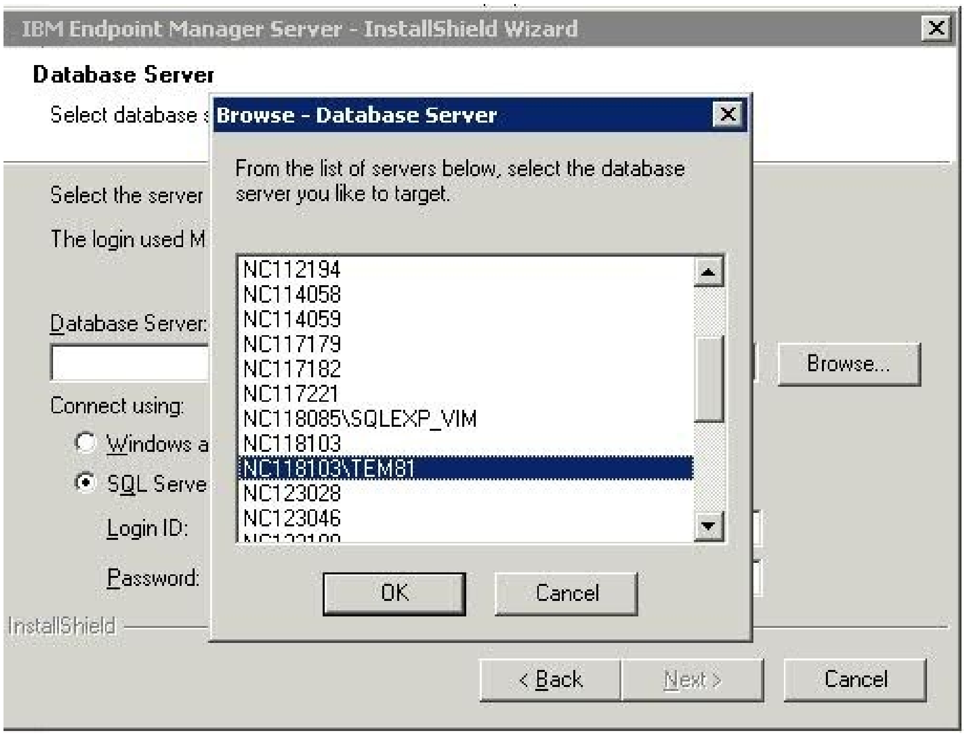
Select Database

Select the database to be used by Tivoli Endpoint Manager.

○ **Use Local Database**
Install the Tivoli Endpoint Manager databases on the local computer. If no database is installed locally, SQL Server 2005 Express will be installed.

● **Use Remote Database**
Install the Tivoli Endpoint Manager databases on a network computer that already has SQL Server installed.

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



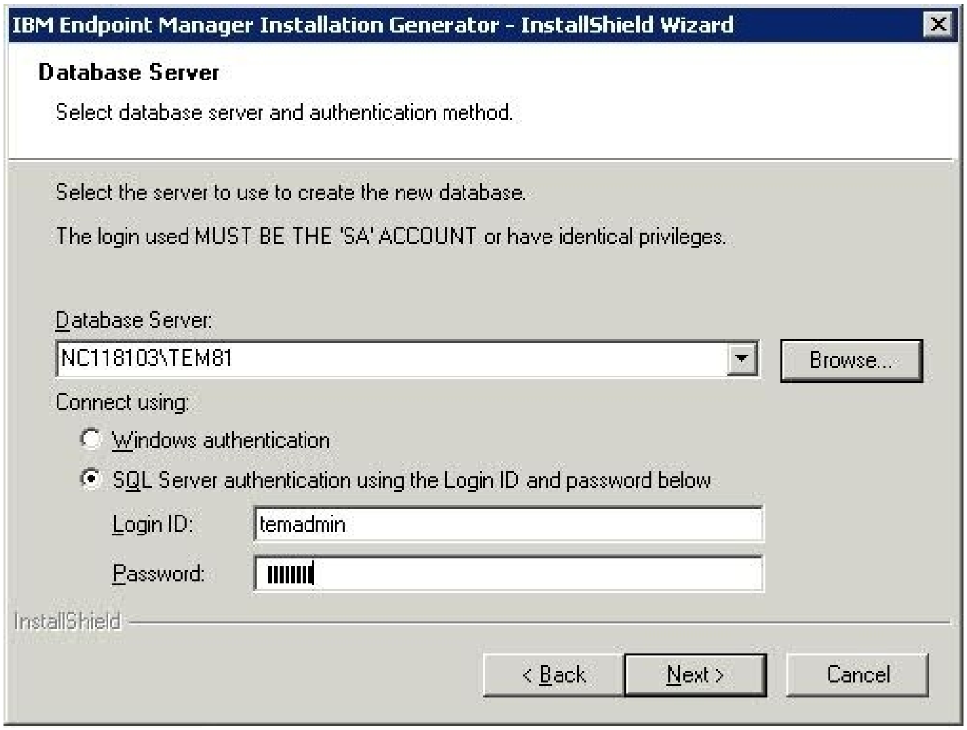
Browse - Database Server

From the list of servers below, select the database server you like to target.

NC112194
NC114058
NC114059
NC117179
NC117182
NC117221
NC118085\SQLEXP_VIM
NC118103
NC118103\TEM81
NC123028
NC123046

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.



IBM Endpoint Manager Installation Generator - InstallShield Wizard

Database Server

Select database server and authentication method.

Select the server to use to create the new database.

The login used MUST BE THE 'SA' ACCOUNT or have identical privileges.

Database Server: NC118103\TEM81

Connect using:

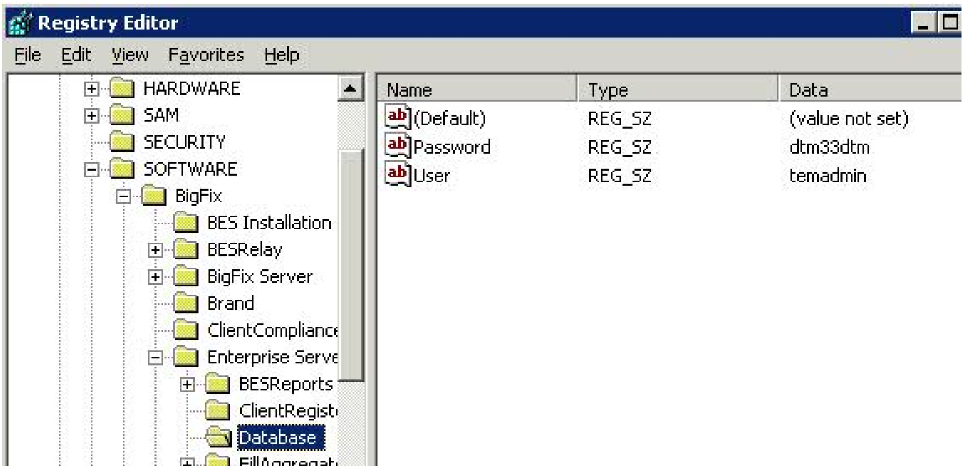
○ Windows authentication

● SQL Server authentication using the Login ID and password below

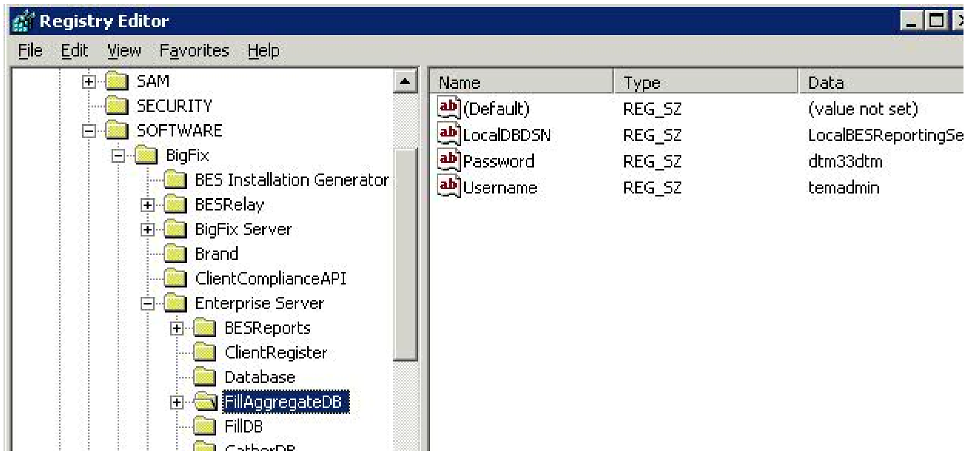
Login ID: temadmin

Password: ||||||||

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
Password	REG_SZ	dtm33dtm
User	REG_SZ	temadmin



Name	Type	Data
(Default)	REG_SZ	(value not set)
LocalDBDSN	REG_SZ	LocalBESReportingSe
Password	REG_SZ	dtm33dtm
Username	REG_SZ	temadmin

Authenticating Additional Servers

Multiple servers can provide a higher level of service for your 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, BES Root, and Web Reports services to the domain user or member of the user group created in step 2, and restart the services.

Note: After you complete the installation of the server and begin to use Product sites, you might install additional components such as the **BES Server Plugin Service** and **BES NMAP Unmanaged Asset Importer**. Both these services have their **LogOn** settings set for the NT user for Remote Database access.

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. The password for this account typed in clear text is obfuscated under the `HKLM` branch of the registry on each server, after the restart of the FillDB service.

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 `HKLM\Software\BigFix\Enterprise Server\FillDB` key on Window 32-bit systems and `HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB` key on Window 64-bit systems:

   ```
   ReplicationUser = <login name>
   ReplicationPassword = <password>
   ReplicationPort = <SQL_port>
   ```
4. Restart the `FillDB` service.

Note:

This choice must be made on a deployment-wide basis; you cannot mix domain-authenticated servers with SQL-authenticated servers.

`ReplicationUser`, `ReplicationPassword`, and `ReplicationPort` must be uniquely defined in all the server registries of your DSA environment.

All 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" on page 56.

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).

   Note: You can also select a remote database hosted on a different server. In this case ensure that the server you are installing can resolve the hostname of the remote server where the database resides. For additional information see "Server installation with remote database" on page 51.
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 **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.

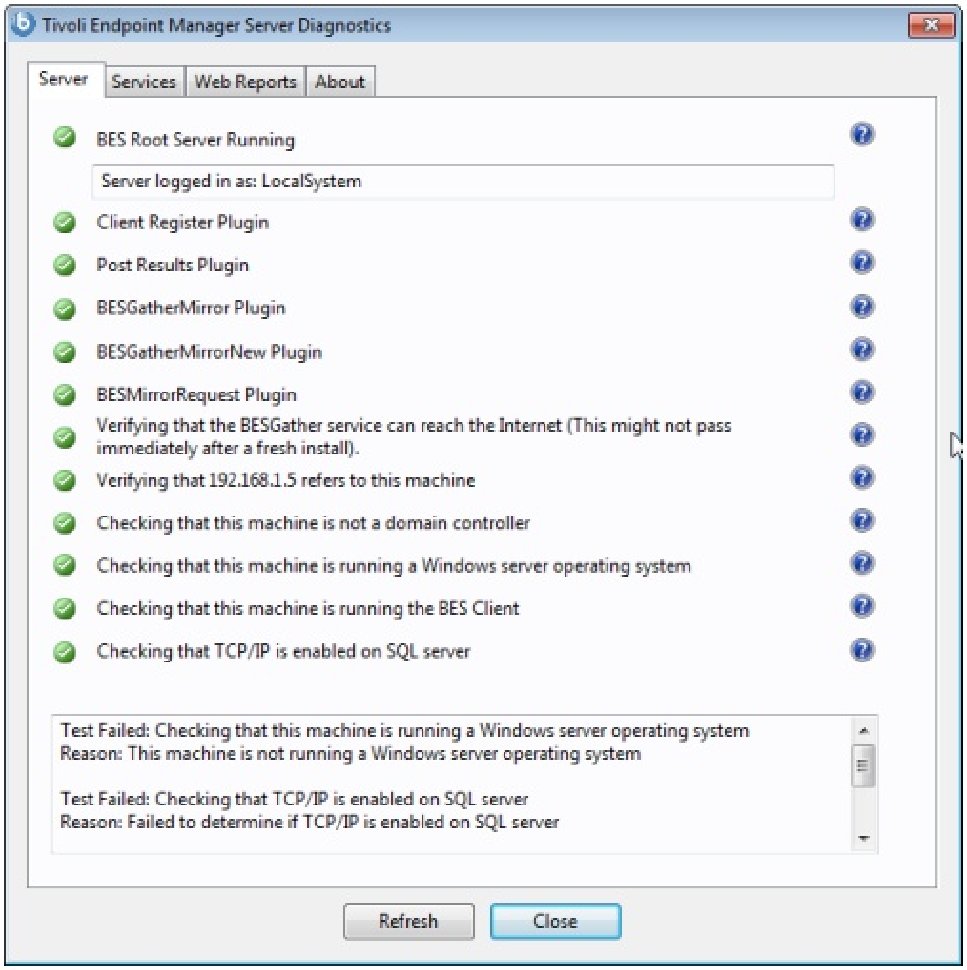
    Note: The initial replication can take several hours depending on the size of your database. Wait for the replication to complete before taking any actions from a console connected to the replica Server.
11. You can see a graph of the servers and their connections by clicking the **Edit Replication Graph**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

Running the Diagnostics tool

The 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 > > Diagnostics Tool.The program analyzes the server components and creates a report.
2. For more in-depth information, click the **Full Interface** . The Diagnostic control panel is displayed. This window has tabs corresponding to the categories of server diagnostics, including **Services** and **Web Reports.**



✓ BES Root Server Running

Server logged in as: LocalSystem

✓ Client Register Plugin

✓ Post Results Plugin

✓ BESGatherMirror Plugin

✓ BESGatherMirrorNew Plugin

✓ BESMirrorRequest Plugin

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

✓ Verifying that 192.168.1.5 refers to this machine

✓ Checking that this machine is not a domain controller

✓ Checking that this machine is running a Windows server operating system

✓ Checking that this machine is running the BES Client

✓ Checking that TCP/IP is enabled on SQL server

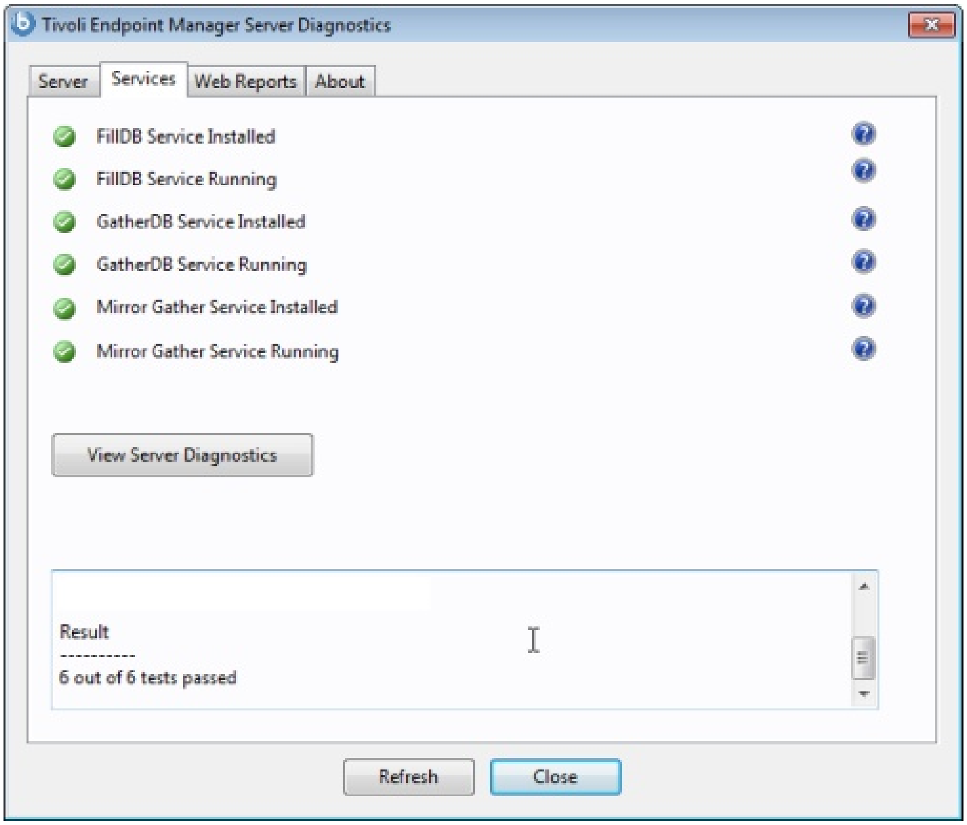
```
Test Failed: Checking that this machine is running a Windows server operating system
Reason: This machine is not running a Windows server operating system

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

Note: 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 Chapter 12, “Setting up a proxy connection,” on page 141.

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.



FillDB Service Installed

FillDB Service Running

GatherDB Service Installed

GatherDB Service Running

Mirror Gather Service Installed

Mirror Gather Service Running

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

If a red light is glowing next to an item, it indicates a failure of that component. You must address the stated problem before you can be sure that the Server is functioning correctly. Similarly, there is a tab to diagnose the **Web Reports** server.

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

Installing the console

The 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 > > Installation Guide**). Click **Install 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 *Console Users Guide*.

Installing the clients

Install the Client on every computer in your network that you want to administer, including the computer that is running the console. This allows that computer to receive important Fixlet messages such as security patches, configuration files, or upgrades.

If you are running the console, select **Install 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 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 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 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 Client Deploy Tool is created by the Installation Generator. You can launch the tool from the Installation Guide. Click the **Install Components > Install Clients > Install Remotely** button or launch it directly from **Start > Programs > > Client Deploy**.
2. The resulting dialog offers three ways to deploy the Clients:

   Find computers using Active Directory
   The 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 . 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 support site.

Installing the client manually:

You can install the 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 > > Installation Guide**) and click the button marked **Browse Install Folders** to open the **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 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 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 of the Windows server and in the `/ServerInstaller_9.1.`*`xxx.x`*`-rhe6.x86_64/repos/ClientMSI` folder of the Linux server.

To install the Windows client perform the following steps:

1. Copy the `BESClientMSI.msi` program on the `c:\BESInstallers\ClientMSI` folder of a Windows system.
2. If you do not run the `BESClientMSI.msi` program located in the `BESInstallers\ClientMSI` folder of the Windows server, you must copy the `actionsite.afxm` masthead located in the server, to the client installation directory that can be the default installation directory, `%PROGRAM FILES%\BigFix Enterprise\BES Client`, or a specific installation directory, `INSTALLDIR="c:\myclient"`.
3. Run the `BESClientMSI.msi` program in one of the following ways:
   - `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 specified directory (`INSTALLDIR="c:\myclient"`).

   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. Transform file list

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 Command-Line Options. To create a Group Policy Object (GPO) for BESClientMSI deployments, see the Microsoft knowledge base article: http://support.microsoft.com/kb/887405.

4. Start the BES client service.

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 using 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. 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 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 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 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 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.

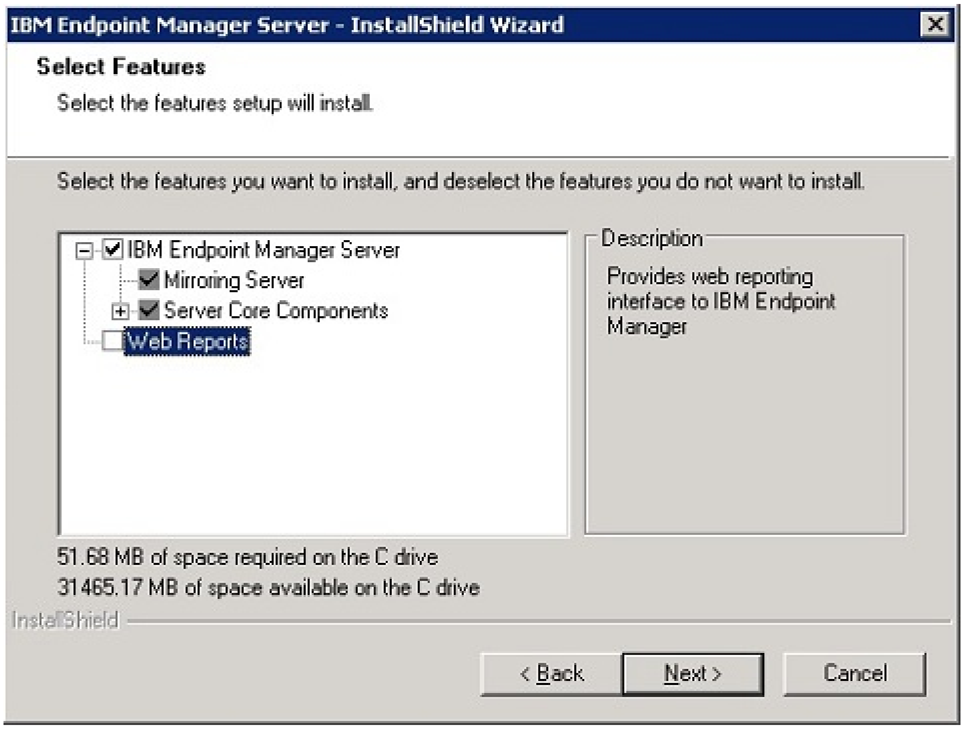
none No encryption is done, even if an encryption certificate is present. This allows you to turn off encryption after you enable it.

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.

For additional information about encryption, see “Encryption” on page 73.

Installing the Web Reports

By default, the Web Reports component is installed together with the server. However, you can choose to not install this component by removing the check in the following installation panel:



IBM Endpoint Manager Server - InstallShield Wizard

Select Features

Select the features setup will install.

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

- ☑ IBM Endpoint Manager Server
  - ☑ Mirroring Server
  - ☑ Server Core Components
- □ Web Reports

Description

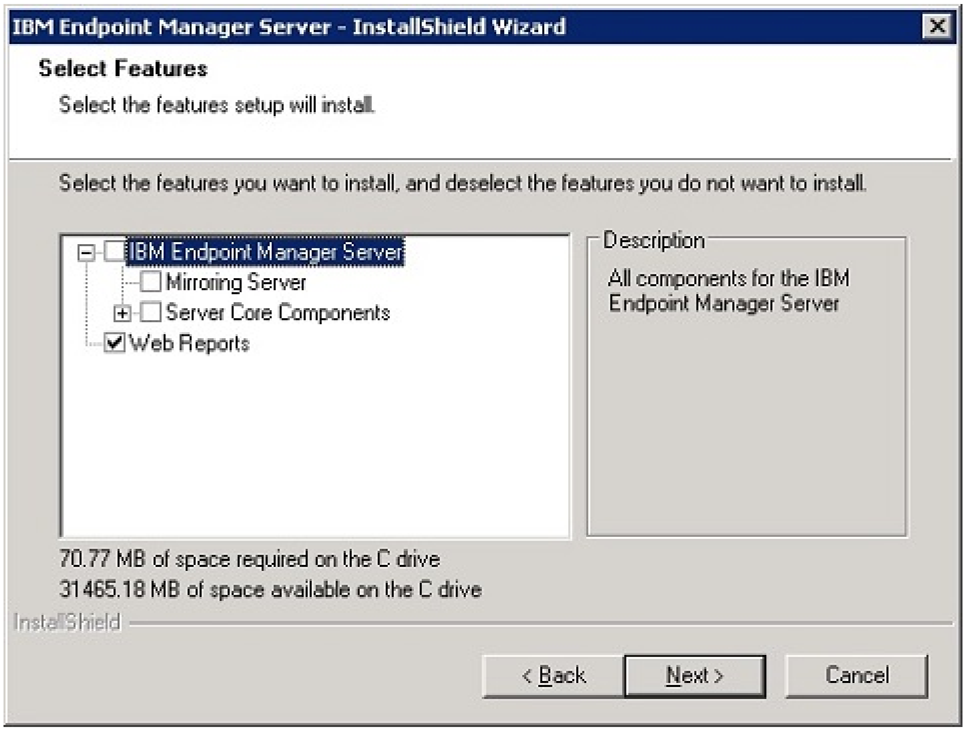
Provides web reporting interface to IBM Endpoint Manager

51.68 MB of space required on the C drive

31465.17 MB of space available on the C drive

You can install it later either on the same system as the server or stand-alone on a different system by running the following steps:

1. Run the Installation Guide (**Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Installation Guide**).
2. Select **Install Server**.
3. Choose to use the masthead generated at the server installation time.
4. Select to install only the Web Reports component in this panel:


IBM Endpoint Manager Server - InstallShield Wizard

Select Features

Select the features setup will install.

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

- □ IBM Endpoint Manager Server
  - □ Mirroring Server
  - □ Server Core Components
- ☑ Web Reports

Description

All components for the IBM Endpoint Manager Server

70.77 MB of space required on the C drive

31465.18 MB of space available on the C drive

5. Complete by choosing the database options that applies to your configuration.
6. Review the installation parameter and click **Next** to trigger the installation.

Running the Administration Tool

The Installer automatically creates the 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 > > Administration Tool.** To run the program, you must first browse to the private key (license.pvk).

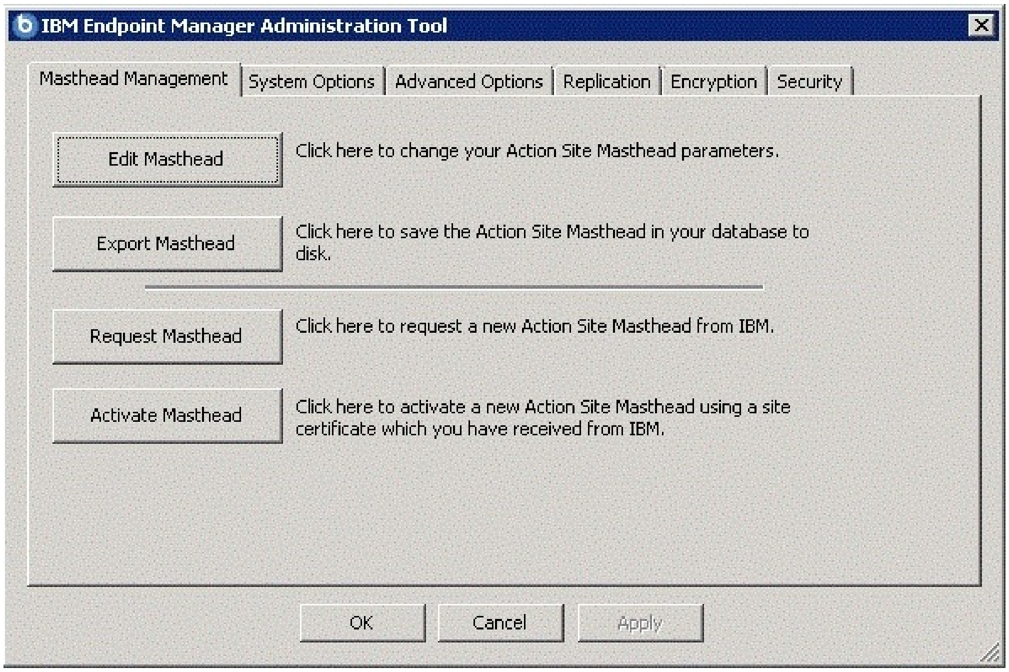
You can also change your administrative password through this interface. After you have selected the private key file, click **OK** to continue. You must supply your private key password to proceed.

Note: When you change the private key password you change only the password of the local file; the other DSA servers are not updated. They continue to use their own license file and password unless it is replaced from the changed license file.

Use the console to perform the user management tasks.

Masthead Management:

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



Click here to change your Action Site Masthead parameters.

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

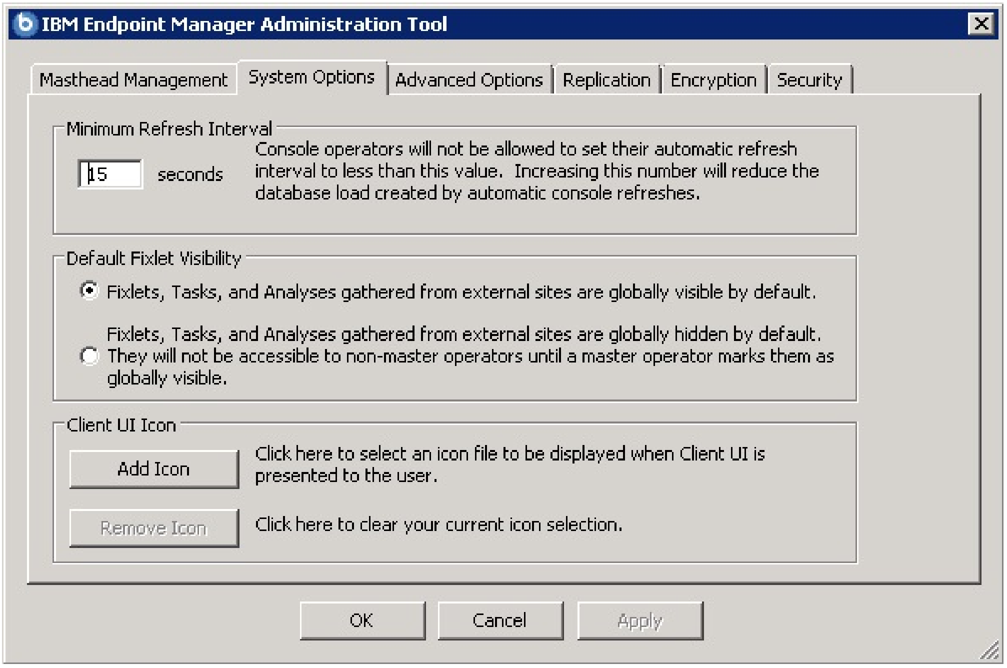
Click here to request a new Action Site Masthead from IBM.

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

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

System Options:

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



Minimum Refresh Interval

15 seconds

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

Default Fixlet Visibility

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

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

Client UI Icon

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

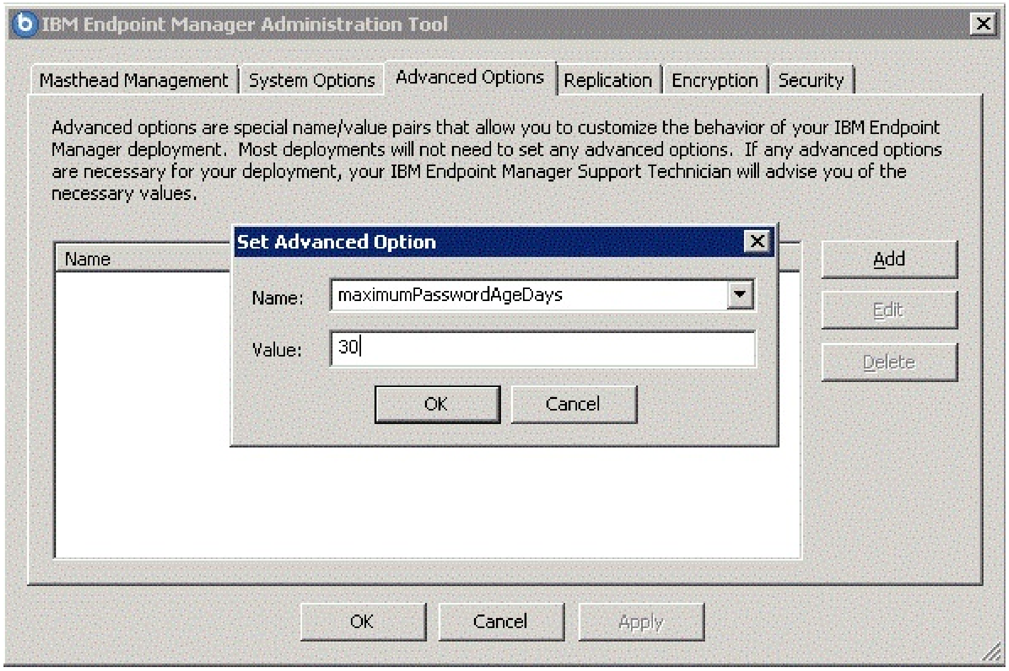
Click here to clear your current icon selection.

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



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

Name: maximumPasswordAgeDays

Value: 30

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. These are some of the advanced options that you can specify:

Table 3. Advanced Settings Names

Name	Value
loginWarningBanner	If set with text, any user who logs into the Console or Web Reports will be shown the text after they log in. The user will have to click **OK** to continue.
timeoutLockMinutes	The amount of idle time in minutes before the console requires to authenticate again. This is different from **loginTimeoutSeconds** in that timeout lock will hide the entire console to prevent any other user to see or use it. Idle time refers to the lack of any type of input to the session including key buttons, mouse clicks, and mouse movements.

Note: Non efficient mime advanced option is no longer is supported by the 9.1 server. Existing actions continue to run on clients but the server is no longer able to generate non efficient mime actions.

Replication:

The fourth tab opens the **Replication** dialog. Use this dialog to visualize your replication servers. For more information, see the Configuration Guide..

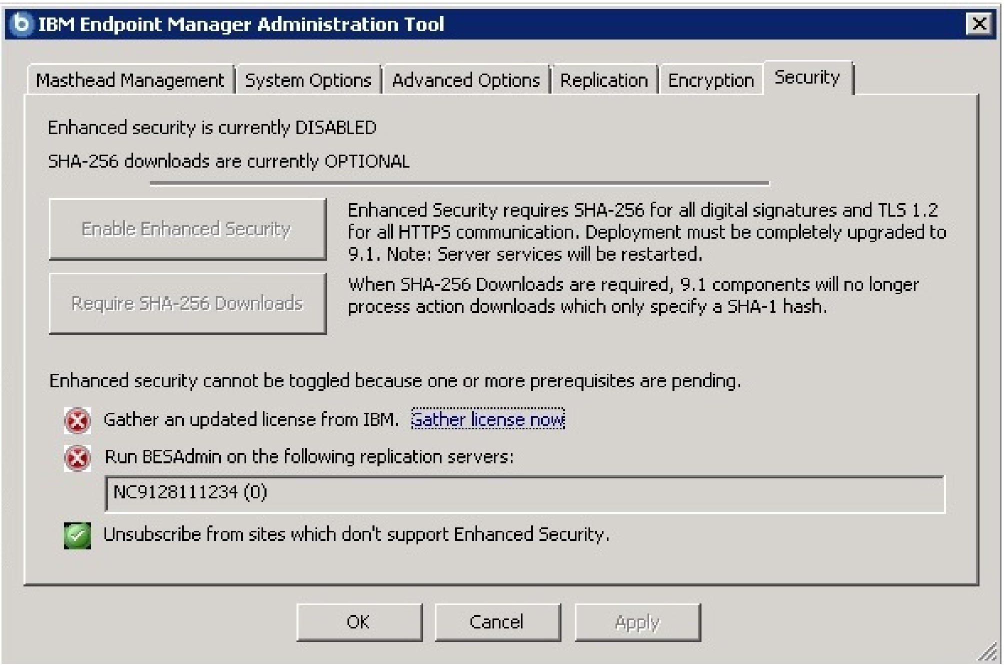
Encryption:

The fifth tab opens the **Encryption** dialog. Use this dialog to generate a new encryption key or to disable encryption altogether. For more information, the Configuration Guide..

Security:

Click the sixth tab to open the **Security** dialog.

The first time that you access the Security tab after installing the server, you see the following information:



Enhanced security is currently DISABLED

SHA-256 downloads are currently OPTIONAL

Enhanced Security requires SHA-256 for all digital signatures and TLS 1.2 for all HTTPS communication. Deployment must be completely upgraded to 9.1. Note: Server services will be restarted.

When SHA-256 Downloads are required, 9.1 components will no longer process action downloads which only specify a SHA-1 hash.

Enhanced security cannot be toggled because one or more prerequisites are pending.

☒ Gather an updated license from IBM. Gather license now

☒ Run BESAdmin on the following replication servers:

NC9128111234 (0)

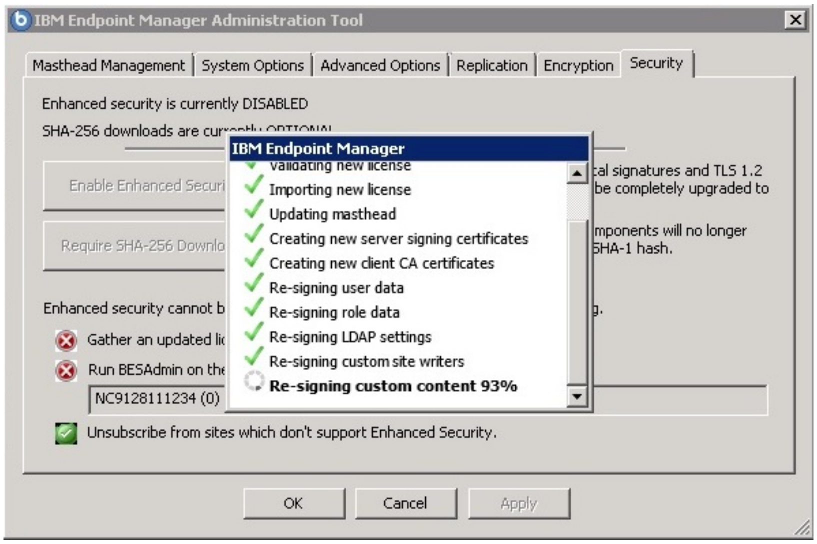
✓ Unsubscribe from sites which don't support Enhanced Security.

The following check marks are automatically updated by the product:

Gather an updated license from IBM
This check mark is:

Green If the updated license was downloaded from the IBM site and distributed to all the clients.

Red If the license stored on the server is not synchronized with the license stored on the IBM site. Click **Gather license now** to update the license on the server. When you click **Gather license now** your updated license is automatically gathered from the IBM site and distributed to the clients.



Enhanced security is currently DISABLED

SHA-256 downloads are currently OPTIONAL

tal signatures and TLS 1.2
be completely upgraded to

mponents will no longer
SHA-1 hash.

Enhanced security cannot b

☒ Gather an updated lic

☒ Run BESAdmin on the

NC9128111234 (0)

☑ Unsubscribe from sites which don't support Enhanced Security.

IBM Endpoint Manager

✓ Validating new license
✓ Importing new license
✓ Updating masthead
✓ Creating new server signing certificates
✓ Creating new client CA certificates
✓ Re-signing user data
✓ Re-signing role data
✓ Re-signing LDAP settings
✓ Re-signing custom site writers
Re-signing custom content 93%

The status of the check mark is automatically updated when the license processing completes.

Run BESAdmin on the following replication servers

If you defined replication servers, this check mark is:

Green If all replication servers have version 9.1 installed and they have the updated license.

Red If at least one server in the DSA configuration does not satisfy the conditions specified above. To fix this situation:

1. Ensure that the **Gather an updated license from IBM** check mark is green.
2. Ensure that the replication servers listed below the check mark have version 9.1 installed.
3. By default replication occurs every 5 minutes, you can specify a different interval in the **Replication** tab of the **IBM Endpoint Manager Administration Tool**. After the replication runs and distributes the updated license on all servers, run **BESAdmin** on those replication servers to update their license.
4. Restart **IBM Endpoint Manager Administration Tool** to update the check mark status in the **Security** tab.

Unsubscribe from sites which don’t support Enhanced Security

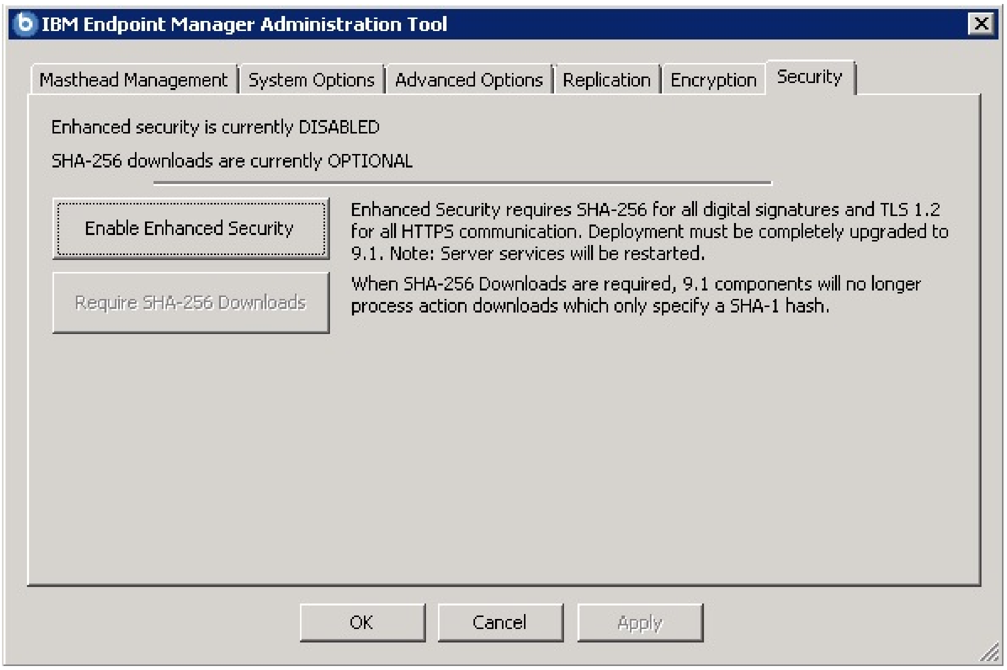
This check mark is:

Green If all sites that you subscribed to, support the Enhanced Security feature, which means that they support the SHA-256 cryptographic digest algorithm for all digital signatures as well as for content verification.

Red If at least one site that you are subscribed to does not support the Enhanced Security feature. To fix this situation, unsubscribe from the sites that are listed below the check mark. Then access the Administration tool again to refresh the status of the check mark.

If any of the three check marks is red the product will use the security behavior provided by version 9.0.

When the three prerequisites are satisfied, the **Enable Enhanced Security** button is enabled in the **Security** tab and you can choose to use the **Enable Enhanced Security** feature in your environment.



Enhanced security is currently DISABLED

SHA-256 downloads are currently OPTIONAL

Enhanced Security requires SHA-256 for all digital signatures and TLS 1.2 for all HTTPS communication. Deployment must be completely upgraded to 9.1. Note: Server services will be restarted.

When SHA-256 Downloads are required, 9.1 components will no longer process action downloads which only specify a SHA-1 hash.

Click the **Enable Enhanced Security** button to adopt the SHA-256 cryptographic digest algorithm for all digital signatures as well as for content verification and to use the TLS 1.2 protocol for communications among the Endpoint Manager components.

Note: If you use this setting you break backward compatibility because version 9.0 or earlier components cannot communicate with version 9.1 server or relays.

Note: When you disable the enhanced security mode, the `BESRootServer` service fails to auto-restart. To solve the problem, restart the service manually.

The **Require SHA-256 Downloads** button is disabled until you click the **Enable Enhanced Security** button. Click the **Require SHA-256 Downloads** button to change all download verification to use only the SHA-256 algorithm. Existing custom actions might need to be edited to conform to the **prefetch** action script syntax updated for V9.1. If you do not select this option, the file download integrity check is run using the SHA-1 algorithm.

For more information about the Enhanced Security feature and the supported security configuration, see Chapter 4, "Security Configuration Scenarios," on page 23.

Additional administration commands

The installation automatically downloads the Administration Tool program `BESAdmin.exe`, in the `C:\Program Files (x86)\BigFix Enterprise\BES Server` directory.

You can run the script `BESAdmin.exe` to perform additional operations. To run this script from the command prompt, use the following command:

```
.\BESAdmin.exe /service { arguments }
```

where *service* can be one of the following:

```
converttoldapoperators
createuser
deleteuser
edituser
findinvalidsignatures
minimumSupportedClient
resignsecuritydata
rotateserversigningkey
setproxy
```

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

Each service has the following *`arguments`* :

`converttoldapoperators`

You can convert local operators to LDAP operators, so that they can log in with their LDAP credentials. Optionally you can use the `-mappingFile` argument to specify a file, the mapping file, where each line has the name of the user to convert, followed by a tab, followed by the name of the user in LDAP/AD. Specify the name using the same format that the user will use to log into the console, *domain\user*, *user@domain*, or *user*. If you do not specify a mapping file, all users are converted assuming their name in LDAP/AD is the same as their local user name.

The syntax to run this service is:

```
.\BESAdmin.exe /convertToLDAPOperators [/mappingFile:<file>]
```

`createuser`

You can create accounts for operators that access the Console. For security purposes, a password-protected public/private key is also generated so the new operator can properly create and sign actions.

The syntax to run this service is:

```
.\BESAdmin.exe /createUser:<UserName>
/userPassword:<UserPassword>
/masterOp:<yes|no>
/customContent:<yes|no>
/showotherusersactions:<yes|no>
/unmanagedAssetPrivilege:<all|none|scanpoint>
```

Optionally you can specify the following parameters:

masterOp

Specifies whether the user is a master operator. The default value is **yes**.

customContent

Specifies whether the user can create custom content. The default value is **yes**.

showotherusersactions

Specifies whether the user can see other user's actions that affect the computers they manage. The default value is **yes**.

unmanagedAssetPrivilege

Defines what unmanaged assets the user can see. The default value is **scanpoint**.

deleteuser

You can mark as deleted a non-master operator. When you run this command the operator instance is removed from the database but the content that the operator created is not removed.

The syntax to run this service is:

```
.\BESAdmin.exe /deleteUser <UserName>
```

editUser

The syntax to run this service is:

```
.\BESAdmin.exe /editUser <UserName>
/loginPermission:<always|never|role>
/customContent:<yes|no>
/showOtherUsersActions:<yes|no>
/unmanagedAssetPrivilege:<all|none|scanpoint>
```

Optionally you can specify the same parameters supported for `createUser` with the exception of `masterOp` that is supported only by `createUser`, and `loginPermission` that is supported only by `editUser` and has the following behavior:

loginPermission

Specifies when the user is allowed to log in. The default value is **always** which means that the user is always allowed to log in. The value **never** means that the user is not allowed to log in at all. The value **role** means that the user can log in if he is a member of a role. This parameter is used to disable operators login, or to assign a role to an LDAP group and allow anyone in that LDAP group to log in.

findinvalidsignatures

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

-resignInvalidSignatures (optional)

Attempts to resign any invalid signatures that `BESAdmin` finds.

-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.exe /findinvalidsignatures
[ /resignInvalidSignatures | /deleteInvalidlySignedContent ]
```

minimumSupportedClient

This service defines the minimum version of the Agents used in your environment.

Note: Based on this setting, the components can decide when it is safe to assume the existence of newer functions across all the component in the deployment. Individual agent interactions might be rejected if the interaction does not comply with the limitations imposed by this setting.

The currently available values are:

- **8.2** which means that no activity issued by Agents V8.2, such as registration to server, archive files and reports uploads, are prevented from running or limited. This behavior applies also if the `minimumSupportedClient` service is not set.

- **9.0** which means that:
  - Initial or regular registrations of V8.2 Clients to a Relay or to the Server succeed.
  - Reports sent by V8.2 Clients are discarded by FillDB.
  - The upload of an archive file generated on a V8.2 Client, by an **archive now** command for example, fails.

If you ran a fresh installation of V9.1.11 the `minimumSupportedClient` is not set and so all the agents, regardless of their version, can join your environment.

The syntax to run this service is:

```
.\BESAdmin.exe [/sitePvkFile=<path+license.pvk>] [/sitePassword=<password>]
/minimumSupportedClient=<version>.<release>
```

If you omit `[/sitePvkFile=<path+license.pvk>] [/sitePassword=<password>]`, you will be requested to enter the site key and password in a pop-up window.

For example, if you want to state that agents V8.2 are not supported in your environment, you can run the following command:

```
./BESAdmin.exe /minimumSupportedClient=9.0
```

resignsecuritydata

You can resign all of the users content in the database to enable user login to the Console. The command resigns security data using the existing key file. You can specify the following parameter:

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

The complete syntax to run this service is:

```
.\BESAdmin.exe /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 command creates a new server signing key, resigns all existing content using the new key, and revokes the old key.

The syntax to run this service is:

```
.\BESAdmin.exe /rotateserversigningkey /sitePvkLocation=<path+license.pvk>
[ /sitePvkPassword=<password> ]
```

setproxy

If your enterprise uses a proxy to access the Internet, you must set a proxy connection to enable the server to gather content from sites as well as to do component-to-component communication or to download files.

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:<proxy_host> /user:<proxy_username>
/pass:<proxy_password> [/exceptionlist:<proxy_exceptionlist>]
```

For information about how to run the command and about the values to use for each argument, see “Setting up a proxy connection on the server” on page 143.

Removing the Primary Server on Windows systems

To uninstall the Server, you must remove the Server, the Client, and Web Reports components, and the related databases.

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

1. Download the **BESRemove.exe** utility from TEM Remove Utility.
2. Double-click on **BESRemove.exe** to run the utility.

   Note: The **BESRemove.exe** utility does not remove the Microsoft SQL Server 2005 instance that was installed with V9.1.

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 support site.

Chapter 9. Installing on Linux systems

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

Because 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 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 server or at the same time:

- **DB2 V10.5 Enterprise Server Edition**: if you want to install the Enterprise Server Edition you must install this version of DB2 before installing the server. Install it on the local workstation where you want to install the 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 server ensure that the DB2 V10.5 Enterprise Server Edition has been installed and started as follows:
  - If the DB2 V10.5 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 V10.5 Enterprise Server Edition is installed remotely:
    1. Install a DB2 10.5 client locally and connect it to the DB2 10.5 server installed on the remote workstation. No additional DB2 configurations (such as the catalog of the remote database) are required. To install the DB2 client you can run the installation wizard or the silent installation with a response file. For additional details see Installation methods for IBM data server clients.

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 V10.5 Workgroup Server Edition**: this is the DB2 version included in the installation package. Depending on the installation package you download, you can install this version of DB2 either before installing the server by following the previous steps or together with the server installation after downloading it. You download it to the local workstation where you want to install the server. During the 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 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 `/opt/ibm/db2/V10.1/bin/db2ilist`;
   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 *Installation requirements for DB2 database products* and “Database requirements” on page 19.

Installation Steps

To install the Server perform the following steps:

1. Download .
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 from IBM Passport Advantage portal.

You can download 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 4. Parts required for installing Server

Software Name	Part Number	Image
IBM Endpoint Manager Platform Install V9.1 for Multiplatforms	CITM5ML	`IBM Endpoint Manager 9.1.1082.0.zip`
IBM Endpoint Manager Platform Install V9.1 for Linux and DB2	CITM6ML	`IEM-9.1.1082-Linux-DB2.tgz`

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

1. Copy the Server compressed zip file `IBM Endpoint Manager 9.1.1082.0.zip` on your Linux Server.
2. Expand the compressed zip file using the following command:
   ```
   unzip "IBM Endpoint Manager 9.1.1082.0.zip"
   ```
3. From the *`linux_server`* folder, expand the `ServerInstaller_9.1.1082.0-rhe6.x86_64.tgz` file on your Red Hat Enterprise Linux Server by using the following command:
   ```
   tar -zxvf ServerInstaller_9.1.1082.0-rhe6.x86_64.tgz
   ```

   You can find the `install.sh` file to install the Linux Server in the `ServerInstaller_9.1.1082.0-rhe6.x86_64` folder.

To extract the Linux Server installation files together with DB2, perform the following steps:

1. Copy the tar file `IEM-9.1.1082-Linux-DB2.tgz` on your Linux Server.
2. Expand the compressed file using the following command:
   ```
   tar -zxvf IEM-9.1.1082-Linux-DB2.tgz
   ```
3. When you expand the `IEM-9.1.1082-Linux-DB2.tgz` image, you have the DB2 image, `v10.5fp2_linuxx64_server_r.tar.gz` in the `IEM-9.1.1082-Linux-DB2` folder, on your computer. To install the Linux server, run the `install.sh` command from the `ServerInstaller_9.1.1082.0-rhe6.x86_64` folder.

   Note: Do not expand the `v10.5fp2_linuxx64_server_r.tar.gz` file, because the `install.sh` command searches for the DB2 archive `*.gz`.

Step 2 - Installing the Server

Before running the installation, to ensure you have all the 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 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`*`-rhe6.x86_64` 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
   ```

   Note: If you enter 1 to run the evaluation installation, consider that this type of installation does not support the enhanced security option. For more information about this feature see Chapter 4, “Security Configuration Scenarios,” on page 23.
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. The installation program checks if a DB2 instance is already installed. If it is already installed, skip to step 7.

   If the database is not detected, enter 1 to specify the DB2 download package and install it:

   ```
   ####################
   DB2 Installation Check
   The installer does not detect DB2 as installed on the system. Determine which
   of the options corresponds to your installation:
   [1]  DB2 is not installed, install it
   [2]  DB2 is installed, use the installed instance
   [3]  Exit from the installation
   Choose one of the options above or press  <Enter> to accept the default: [1]

   If the user chooses the option1 then the user will be prompted with the
   following question with details of the settings that will be used.
   ```

6. Enter 1 to accept the DB2 default settings:

   ```
   ####################
   DB2 Installation
   DB2 will be installed using the following settings:
           DB2 Instance owner: db2inst1
           DB2 Fenced user: db2fenc1
           DB2 Administration Server user: dasusr1
           DB2 communication port: 50000
           DB2 Installation directory: /opt/ibm/db2/V10.5
   If you need to use settings different from those proposed above, you can
   specify them in the installation response file. Refer to the product
   documentation for further details.
   [1]  Proceed installing also DB2
   [2]  Exit from the installation
   Choose one of the options above or press  <Enter> to accept the default: [1]
   ```

7. Enter 1 to create a Master database for later replication or single database if you need only one 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 the *Configuration Guide*.

8. 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 server is `BFENT`. The local database name of Web Reports is `BESREPOR`.

   Note: To use an external database for , 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 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.

9. 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
   ```

10. 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
    ```

11. 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.

12. Enter the user name for the local DB2 Administrative user. The default is `db2inst1`.
13. Enter the DB2 Local Administrative user password.
14. Enter the DB2 instance configuration.
15. Enter the user ID and the password to define the initial administrative user. The user name default is: `IEMAdmin`.
16. If the local firewall is running the installation program asks to enter the `Local firewall configuration`.
17. 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 a first installation, or part of it, you can specify option 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.

18. If selected option 1 in the previous step, specify where the generated license authorization file is located:

    ```
    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
    ```

19. 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 server. It cannot be changed after a license is created.
20. Specify the related Site Admin Private Key Password.
21. 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: [2]
    ```

22. 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
    ```

23. 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 with option 2:

    ```
    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
```

24. If there is a proxy that requires a username and password every time an internet request is made, set a proxy connection to enable the server or relay to connect to the internet as described in Chapter 12, "Setting up a proxy connection," on page 141.
25. 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 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).

If you selected 1 in the previous step, you have now created the license files (`license.pvk` and `license.crt` files). After this step, the `masthead.afxm` file is created with the specified parameters.

26. Enter the port number for the DB2 connection to create the DB2 instance:

```
####################
DB2 Connection:
Specify the DB2 Port Number or press <Enter>  to accept the default: 50000
```

The 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.

Note: If you configured a proxy to access the Internet, follow the steps described in Chapter 12, "Setting up a proxy connection," on page 141 to configure the proxy in your IBM Endpoint Manager environment.

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  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 from `/etc/init.d`:

```
./besserver status
./besfilldb status
./besgatherdb status
./besclient status
./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 diretory
```

   Check that the following databases are created:

   - Server component: `BFENT`
   - WebReports component: `BESREPOR`

4. Launch the 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. If during the disaster recovery the installation program finds BFENT or BESREPOR databases, it uses them.

Silent installation

To run a silent installation enter the following command:

```
./install.sh -f response_file -opt keyword=value
```

where:

response_file
Is the file containing the keywords to install the product.

keyword=value
Is the keyword and the value of the response file you want to override.

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

Note: In the response file you can specify a subset of keywords, such as the keywords common to different systems. The missing or invalid keywords are requested by the installation program. The silent installation runs in unattended way only if all the required keywords are specified in the response file.

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
```

This is an example of response file for a production server installation:

```
##IEM GENERATED RESPONSE FILE
LA_ACCEPT="true"
IS_EVALUATION="false"
COMPONENT_SRV="true"
COMPONENT_WR="true"
SINGLE_DATABASE="true"
LOCAL_DATABASE="true"
BES_WWW_FOLDER="/var/opt/BESServer"
WR_WWW_FOLDER="/var/opt/BESWebReportsServer"
WR_WWW_PORT="80"
INSTALL_DB2="yes"
DB2_INSTANCE_NAME="db2inst1"
DB2_DAS_USERNAME="dasusr1"
DB2_FENCED_USERNAME="db2fenc1"
DB2_INSTALL_DIR="/opt/ibm/db2/V10.5"
DB2_PORT="50000"
DB2_SETUP_FILE="../server_r/db2setup"
DB2_USERS_PWD="Bigfix11"
TEM_USER_NAME="IEMAdmin"
TEM_USER_PWD="Bigfix11"
CONF_FIREWALL="no"
BES_SETUP_TYPE="authfile"
BES_AUTH_FILE="/opt/iemlic/LicenseAuthorization.BESLicenseAuthorization"
SRV_DNS_NAME="NC9128110090.romelab.it.ibm.com"
BES_LICENSE_PVK_PWD="Bigfix11"
PVK_KEY_SIZE="max"
BES_LIC_FOLDER="/opt/iemlic"
SUBMIT_LIC_REQUEST="yes"
USE_PROXY="true"
PROXY_USER="proxyuser"
PROXY_PWD="Bigfix11"
PROXY_HOST="nc114087.romelab.it.ibm.com"
PROXY_PORT="3128"
ADV_MASTHEAD_DEFAULT="true"
```

This is an example of response file for an evaluation server installation:

```
##IEM GENERATED RESPONSE FILE
LA_ACCEPT="true"
IS_EVALUATION="true"
CREDENTIAL_USER="John Smith"
CREDENTIAL_EMAIL="john.smith@us.ibm.com"
CREDENTIAL_ORG="IBM US"
SRV_DNS_NAME="NC9128110090.romelab.it.ibm.com"
BES_SERVER_PORT="52311"
WR_WWW_PORT="80"
CONF_FIREWALL="no"
DB2_ADMIN_USER="db2inst1"
DB2_ADMIN_PWD="Bigfix11"
DB2_PORT="50000"
BES_LIC_FOLDER="/opt/iemlic"
USE_PROXY="true"
PROXY_USER="none"
PROXY_HOST="nc114087.romelab.it.ibm.com"
PROXY_PORT="3128"
```

where:

Table 5. Response file keywords

Keyword	Values
LA_ACCEPT	Accepts the License Agreement: `true` to accept and continue `false` to exit the installation

Table 5. Response file keywords (continued)

Keyword	Values
IS_EVALUATION	Specifies the type of installation: `true` to run an evaluation installation `false` to run a production installation **Note:** The evaluation installation does not support the enhanced security option. For more information about this feature see Chapter 4, "Security Configuration Scenarios," on page 23.
CREDENTIAL_USER	Specifies the user name. An example is: `John Smith`. **Note:** Valid in the evaluation installation only
CREDENTIAL_EMAIL	Specifies the user email address. An example is: `john.smith@us.ibm.com`. **Note:** Valid in the evaluation installation only
CREDENTIAL_ORG	Specifies the user's organization. An example is: `IBM US`. **Note:** Valid in the evaluation installation only
COMPONENT_SRV	Specifies to install the server component: `true` to install the server and client `false` to not install the server and the client
COMPONENT_WR	Specifies to install the Web Reports component: `true` to install Web Reports `false` to not install Web Reports
SINGLE_DATABASE	Creates a master database for later replication or if you only need a single database in your deployment. `true` to create a single database `false` to create a replicated database
LOCAL_DATABASE	Uses a local or remote database: `true` to use a local database `false` to use a remote database through a DB2 client
DB2_ADMIN_USER	Specifies the user name of the local DB2 Administrative user. Only if DB2 is already installed.
DB2_ADMIN_PWD	Specifies the password of the local DB2 Administrative user. Only if DB2 is already installed.
DB2INST_CONFIGURE	Configures the database during the installation: `yes` to configure the DB2 `no` to not configure the DB2 Only if DB2 is already installed.
BES_WWW_FOLDER	Specifies the installation folder of server. The default value is `/var/opt/BESServer`.
WR_WWW_FOLDER	Specifies the installation folder of Web Reports. The default value is `/var/opt/BESWebReportsServer`.
WR_WWW_PORT	Specifies the Web Reports port number. The default value is `80`.
INSTALL_DB2	Installs DB2 together with the server: `yes` to install DB2 `no` to not install DB2
DB2_INSTANCE_NAME	Specifies the name of the database instance. The default value is `db2inst1`.

Table 5. Response file keywords (continued)

Keyword	Values
DB2_DAS_USERNAME	Specifies the username of the account under which the DB2 administration server (DAS) runs. The default value is `dasusr1`.
DB2_FENCED_USERNAME	Specifies the user name of the account used to run user defined functions (UDFs) and stored procedures outside of the address space used by the DB2 database. The default user is `db2fenc1`.
DB2_INSTALL_DIR	Specifies the directory where to install DB2. For example: `/opt/ibm/db2/V10.5`.
DB2_PORT	Specifies the DB2 port. The default value is `50000`.
DB2_SETUP_FILE	Specifies the setup file to install DB2. For example: `../server_r/db2setup`.
DB2_USERS_PWD	Specifies the DB2 user password.
TEM_USER_NAME	Specifies the user ID to define the initial administrative user. The default value is `IEMAdmin`.
TEM_USER_PWD	Specifies the password to define the initial administrative user.
CONF_FIREWALL	Configures the firewall to enable the server or relay to connect to the Internet: `yes` to set the firewall configuration `no` not to set the firewall configuration
BES_SETUP_TYPE	Specifies the type of setup to run: `authfile` to install with a BES license authorization file `prodlic` to install with a Production license that is already available `masthead` to install with an existing masthead
BES_AUTH_FILE	Specifies the path of the authorization file. An example of path is: `/opt/iemlic/LicenseAuthorization.BESLicenseAuthorization`.
SRV_DNS_NAME	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 server. It cannot be changed after a license is created.
BES_LICENSE_PVK_PWD	Specifies the password of the `license.pvk` file.
PVK_KEY_SIZE	Specifies the size in bits of the public key (`license.crt`): **`min`** Corresponds to 2048 bits. **`max`** Corresponds to 4096 bits. This is the default value.
BES_LIC_FOLDER	Specifies the License folder where the installation generates and saves `license.crt`, `license.pvk` and `masthead.afxm`. An example of License folder is `/tmp/ServerInstaller_9.1-rhel/offlic`.
SUBMIT_LIC_REQUEST	Submits the request to IBM for getting the license certificate: `yes` to submit a request from this machine over the Internet for a license certificate (`license.crt`) and saved in your credential folder. `no` to save the request to a file and manually submit it to IBM (http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html). This method might be necessary if your deployment is isolated from the public Internet.
USE_PROXY	Specifies a proxy connection to enable the server to connect to the Internet during the installation: `true` to set the proxy. `false` to not set the proxy.

Table 5. Response file keywords (continued)

Keyword	Values
PROXY_USER	Specifies the user of the proxy. If the proxy does not require authentication, you must set `PROXY_USER` to `NONE`.
PROXY_PWD	Specifies the password of the proxy user.
PROXY_HOST	Specifies the hostname of the computer where the proxy is running.
PROXY_PORT	Specifies the port of the computer where the proxy is running.
ADV_MASTHEAD_DEFAULT	Accepts the default masthead values: `true` to use the default values `false` to use custom values.
IS_SILENT	Forces the installation to end with a message if a required parameter is missing: `true` to force the installation to end if a required parameter is missing. `false` to prompt the user for the missing parameter. If a parameter is missing the installation variable associated with the missing parameter is reported in the error message.

Installation Folder Structure

After the 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)
```

Note: If you want to move the content of your /var/opt/BESClient directory to a new location, you can use the UNIX symbolic link feature to point to the new directory.

Install Log Files:

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

Note: Be aware that if one of the following folders does not exist, the installation procedure fails:

```
/opt
/etc
/var
```

Configuration and Masthead Files

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

Table 6. Configuration Files

Component	File
Server	- Configuration file: /var/opt/BESServer/besserver.config - Masthead file: /etc/opt/BESServer/actionsite.afxm
Web Report	- Configuration file: /var/opt/BESWebReportsServer/beswebreports.config - Masthead file: /etc/opt/BESWebReportsServer/actionsite.afxm
Client	- Configuration file: /var/opt/BESClient/besclient.config - Masthead file: /etc/opt/BESClient/actionsite.afxm

Table 6. Configuration Files (continued)

Component	File
Relay	• Configuration file: /var/opt/BESRelay/besrelay.config

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 BESWebReports service searches for the configuration parameters first in besclient.config and then in beswebreports.config.

Managing the Services

You can start, stop, restart, or query the status of Linux 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 server, you can change the database password and set it in the configuration files by performing the following steps:

1. Stop the berserver and the beswebreports services:

   ```
   service besserver stop
   service beswebreports stop
   ```

2. Change DB2 Administrative user password:

   ```
   #passwd db2inst1
   ```

   You are asked to set the new password for the specified user account.

3. Open the configuration file: /var/opt/BESServer/besserver.config
4. Go to [Software\BigFix\EnterpriseClient\Settings\Client_BESServer_Database_Password] and set:

   ```
   value = "db2newpassword"
   ```

5. Open the configuration file: /var/opt/BESWebReportsServer/beswebreports.config
6. Go to [Software\BigFix\Enterprise Server\FillAggregateDB] and set:

   ```
   value = "db2newpassword"
   ```

7. Start the besserver and beswebreports services:

   ```
   #service besserver start
   #service beswebreports start
   ```

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

Changing the DB2 port

After you install the DB2 database of the Endpoint Manager server, you can change the DB2 instance connection port and set it in the configuration files as follows:

1. Stop all the services and all applications connected to the DB2 instance.
2. Change the DB2 connection port:
   ```
   #su – db2inst1
   $db2 update dbm cfg using SVCENAME <new_port_number>
   $db2stop; db2start
   ```
3. Open the configuration file: `/var/opt/BESServer/besserver.config`
4. Go to `[Software\BigFix\EnterpriseClient\Settings\Client\_BESServer_Database_Port]` and set the new port number as follows:
   ```
   value  = "<new_port_number>"
   ```
5. Open the configuration file: `/var/opt/BESWebReportsServer/beswebreports.config`
6. Go to `[Software\BigFix\Enterprise Server\FillAggregateDB]` and set the new port number as follows:
   ```
   Port  = "<new_port_number>"
   ```
7. Start all the services.

Authenticating Additional Servers (DSA)

Multiple servers can provide a higher level of service for your installation. If you choose to add Disaster 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. The password for this account typed in clear text is obfuscated in the configuration file on each server, after the restart of the FillDB service. 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>
   ReplicationPort = <DB2_port>
   ```
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.

ReplicationUser, ReplicationPassword, and ReplicationPort must be uniquely defined in all the server configuration files of your DSA environment.

All 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 56.

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 in order to have the 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).

   Note: You can also select a remote database hosted on a different server. In this case ensure that the server you are installing can resolve the hostname of the remote server where the database resides.
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 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 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 traffic.

Installing the Console

You can install the 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 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 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 *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 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 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 Client on every computer in your network that you want to administer, including the computer that is running the console. This allows that computer to receive important Fixlet messages such as security patches, configuration files, or upgrades.

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

Note: Some agent components, such as UploadManager, use the `/tmp` directory as a location for temporary files. To avoid any installation issues, be sure to give execute rights to this directory.

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

Find computers using Active Directory
The 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 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 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 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 . 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 support site.

Installing the Client Manually

The 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.

SUSE (32-bit) Installation Instructions

1. Download the corresponding client RPM file to the SUSE computer.
2. Install the RPM by running the command

   ```
   rpm -ivh client_RPM_path
   ```
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
4. Start the Endpoint Manager client by running the command

   ```
   /etc/init.d/besclient start
   ```

SUSE (32-bit) Fixlet Content:

To get the Fixlet content for the SUSE agent, subscribe your server to the appropriate Fixlet site. To subscribe to a new Fixlet site, perform the following steps:

1. Go to a computer with the console installed.
2. Download the appropriate masthead
3. When prompted to open or save the file, click **Open** to opens the console.
4. Log into the console with your username and password.
5. After you logged in, the Endpoint Manager Console asks if you wish to subscribe to the Patches for SUSE Linux Enterprise Fixlet site, click **OK**.
6. Type in your private key password and click **OK**.

   After the console subscribes to the site, it automatically starts gathering new Fixlet messages from the site.

For further information about SUSE (32-bit) Content see http://support.bigfix.com/bes/sites/susepatches.html.

SUSE Linux Enterprise (64-bit) Installation Instructions

Before installing the client on SUSE Linux Enterprise, ensure you have disabled the SELinux process.

1. Download the corresponding client RPM file to the SUSE computer.
2. Install the RPM by running the command

   ```
   rpm -ivh client_RPM_path
   ```
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
1. Start the client by running the command

   ```
   /etc/init.d/besclient start
   ```

Red Hat Installation Instructions

Before installing the client on Red Hat Enterprise Linux 6 or later, ensure you have:

- Disabled the SELinux process.
- Installed the Athena library (libXaw package) that is used by the user interface component of the client.

To install the client perform the following steps:

1. Download the corresponding client RPM file to the Red Hat computer.
2. Install the RPM by running the command

   ```
   rpm -ivh client_RPM_path
   ```
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each Endpoint Manager Server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
4. Start the client by running the command:

   ```
   /etc/init.d/besclient start
   ```

Red Hat Fixlet Content:

To get the Fixlet content for the Red Hat agent, you need to subscribe your server to the appropriate Fixlet site. To subscribe to a new Fixlet site, perform the following steps:

1. Go to a computer with the console installed.
2. Download the appropriate masthead:
3. When prompted to open or save the file, click **Open** to open the console.
4. Log into the console with your username and password.
5. After logged in, the console asks if you wish to subscribe to the Patches for RedHat Linux Fixlet site, click **OK**.
6. Type in your private key password and click **OK**.

   After the console subscribes to the site, it starts gathering new Fixlet messages from the site.

For further information about Redhat Enterprise Linux, see http://support.bigfix.com/bes/sites/rhelpatches.html.

Solaris Installation Instructions

To install the client perform the following steps:

1. Download the corresponding Endpoint Manager Client package file to the Solaris computer.
2. Install the PKG by running the command

   ```
   pkgadd -d package_client_path
   ```
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
4. Start the client by running the command

   ```
   /etc/init.d/besclient start
   ```

Note: To install the client in the local zone, after you have copied the masthead into the `/etc/opt/BESClient/` local zone folder, ensure that the `svcs BESClient` service is online in the local zone by completing the following steps:

1. Check the status of the `BESClient` service:

   ```
   svcs -x BESClient
   ```

   If it is online, no additional action is needed.
2. If the service is in maintenance, stop the `BESClient`:

   ```
   /etc/init.d/besclient stop
   ```
3. Enable the `BESClient` svc service:

```
svcadm clear BESClient
```

4. Check if the service is online and that the client is started:

```
scvs -x BESClient
svcs -p BESClient
```

Note: All Solaris agents must have package SUNWlibC installed.

Solaris Fixlet Content:

1. To get the Fixlet content for the Solaris BES Agent, you will need to subscribe your Endpoint Manager Server to the appropriate Fixlet site. To subscribe to a new Fixlet site, go to a computer with the Endpoint Manager console installed.
2. Download the Solaris Evaluation masthead.
3. When prompted to open or save the file, click "Open" and this will automatically open the Endpoint Manager console.
4. Log into the Endpoint Manager console with your username/password.
5. Once logged in, the Endpoint Manager console asks if you wish to subscribe to the Patches for Solaris Fixlet site, click **OK**.
6. Type in your private key password and click **OK**.
7. After the Endpoint Manager console subscribes to the site, it should automatically start gathering new Fixlet messages from the site.

HP-UX PA-RISC Installation Instructions

To install the client perform the following steps:

1. Download and copy the corresponding client package file to the HP-UX computer (the computer must be PA-RISC system). The file name is in the format: `BESAgent-9.1.`*`xxx`*`.`*`x`*`.pa_risc_hpux`*`xxxx`*`.depot` with variations, depending on the particular version of the agent downloaded.

   Note: Internet Explorer might label the downloaded file as a `.tar` file. Mozilla and other browsers download the file with the extension `.depot`.

2. Run the following command:

   ```
   /usr/sbin/swinstall -s HOSTNAME:/path/BESAgent_filename BESAgent
   ```

   where:

   HOSTNAME
   Is the name of the system on which the agent is being installed.

   /path/ Is the path to the agent installation source.

   BESAgent_filename
   Is the name of the file you downloaded.

   For example:

   ```
   /usr/sbin/swinstall
      -s hpsystemb:/tmp/BESAgent-9.1.xxx.x.pa_risc_hpuxxxxx.depot BESAgent
   ```

3. Copy your actionsite masthead to the HP-UX client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\BES Installers`). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   The masthead file for each server is downloadable at http://servername:port/masthead/masthead.afxm

Note: The directory /etc/opt/BESClient/ is not automatically created by the installer. If it does not exist, create it manually.
The masthead file for each Endpoint Manager Server is downloadable at http://*servername*:*port*/masthead/masthead.afxm (example: http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm).

4. Start the client by running the command:

   ```
   /sbin/init.d/besclient start
   ```

HP-UX Fixlet Content:

1. To get the Fixlet content for the HP-UX BES Agent, you will need to subscribe your Endpoint Manager Server to the appropriate Fixlet site. To subscribe to a new Fixlet site, go to a computer with the Endpoint Manager console installed.
2. Download the HP-UX Evaluation masthead.
3. When prompted to open or save the file, click "Open" and this will automatically open the Endpoint Manager console.
4. Log into the Endpoint Manager console with your username/password.
5. Once logged in, the Endpoint Manager console asks if you wish to subscribe to the Patches for HP-UX Fixlet site, click **OK**.
6. Type in your private key password and click **OK**.
7. After the Endpoint Manager console subscribes to the site, it should automatically start gathering new Fixlet messages from the site.

HP-UX Itanium Installation Instructions

To install the client perform the following steps:

1. Download and copy the corresponding client package file (BESAgent-9.1.*xxxx*.*x*.pa_risc_hpux*xxxxx*.depot) to the HP-UX Itanium computer.
2. Run the following command:

   ```
   /usr/sbin/swinstall -x "allow_incompatible=true"
     -s HOSTNAME:/path/BESAgent-9.1.xxxx.x.pa_risc_hpuxxxxx.depot
      BESAgent
   ```

   where *HOSTNAME* is the name of the system which the Agent is being installed, and */path/* is the path to the Agent installation source
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (actionsite.afxm) can be found in your BES Installation folders (by default they are placed under C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client on Windows and /var/opt/BESInstallers/Client/ on Linux). If the masthead is not named actionsite.afxm, rename it to actionsite.afxm and place it on the computer at the following location: /etc/opt/BESClient/actionsite.afxm.

   Note: The directory /etc/opt/BESClient/ is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at http://*servername*:*port*/masthead/masthead.afxm (example: http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm).
4. Start the client by running the command

   ```
   /sbin/init.d/besclient start
   ```

Mac Installation Instructions

The distribution includes one DMG (mountable Disk Image file) that contains utilities and a separate PKG download for the install or upgrade package. The files are identified as 10.6 versions in the file names. To install the Mac client perform the following steps:

1. Download the corresponding Endpoint Manager client package file to the Mac computer.
2. Copy the PKG file to any directory and copy the masthead file for your deployment into the same directory. Ensure that the masthead file is named `actionsite.afxm`.
3. You might include a pre-defined settings file (`clientsettings.cfg`) in the install directory to create custom settings for the Mac client at installation time.
4. Launch the PKG installer by double-clicking the PKG file (such as `BESAgent-9.1.`*`xxx.x`*`-BigFix_MacOSX`*`xx.x`*`.pkg`) and run through the installer. The agent starts up after the installation completes as long as the masthead file is included in the installation directory.

OSX Installation Instructions:

The distribution includes one DMG (mountable Disk Image file) that contains utilities and a separate PKG download for the install or upgrade package.

1. Download the corresponding Endpoint Manager client package file to the Mac computer.
2. Copy the PKG file to any directory and copy the masthead file for your deployment into the same directory. Ensure the masthead file is named `actionsite.afxm`.
3. You might optionally include a pre-defined settings file (`clientsettings.cfg`) in the install directory to create custom settings for the Mac client at installation time.
4. Launch the PKG installer by double-clicking the PKG file (such as `BESAgent-9.1.`*`xxx.x`*`-Endpoint Manager_MacOSX`*`xx.x`*`.pkg`) and run through the installer. The agent starts up after the installation completes as long as the masthead file is included in the install directory.

Mac Fixlet Content:

To get the Fixlet content for the Mac agent, subscribe your server to the appropriate Fixlet site. To subscribe to a new Fixlet site, perform the following steps:

1. Go to a computer with the console installed.
2. Download the masthead.
3. When prompted to open or save the file, click **Open** to open the console.
4. Log into the console with your username and password.
5. After logged in, the console asks if you wish to subscribe to the Patches for Mac OS X Fixlet site, click **OK**.
6. Type in your private key password and click **OK**.
7. After the console subscribes to the site, it starts gathering new Fixlet messages from the site.

AIX Installation Instructions

To install the client perform the following steps:

1. Download the corresponding client package file to the IBM AIX computer.
2. Copy the BESAgent to the IBM AIX computer.
3. Run the following command:
   ```
   installp –agqYXd ./BESAgent-9.1.xxx.x.ppc_aixxx.pkg BESClient
   ```
4. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
5. Start the client by running the following command:
   ```
   /etc/rc.d/rc2.d/SBESClientd start
   ```

AIX Fixlet Content:

To get the Fixlet content for the AIX agent, subscribe your server to the appropriate Fixlet site. To subscribe to a new Fixlet site, perform the following steps:

1. Go to a computer with the console installed.
2. Download the masthead.ly.)
3. When prompted to open or save the file, click **Open** to open the console.
4. Log into the console with your username and password.
5. After logged in, the console asks if you wish to subscribe to the Patches for AIX Fixlet site, click **OK**.
6. Type in your private key password and click **OK**.
7. After the console subscribes to the site, it starts gathering new Fixlet messages from the site.

ESX Fixlet Content

To get the Fixlet content for the ESX agent, subscribe your server to the appropriate Fixlet site. To subscribe to a new Fixlet site, perform the following steps:

1. Go to a computer with the Endpoint Manager console installed.
2. Download the masthead.
3. When prompted to open or save the file, click **Open** to open the console.
4. Log into the console with your username and password.
5. After you logged in, the console asks if you wish to subscribe to the Patches for ESX Fixlet site, click **OK**.
6. Type your private key password and click **OK**.

After the console subscribes to the site, it starts gathering new Fixlet messages from the site.

Note: Ensure that the firewall ports are opened.

Ubuntu Debian (32-bit) Installation Instructions

To install the client perform the following steps:

1. Download the corresponding client DEB package file to the Ubuntu Debian computer.
2. Install the DEB by running the command
   ```
   dpkg -i client_package_path
   ```
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
4. Start the client by running the command:
   ```
   /etc/init.d/besclient start
   ```

Ubuntu/Debian (64-bit) Installation Instructions

To install the client perform the following steps:

1. Download the corresponding client DEB package file to the Ubuntu/Debian computer.
2. Install the DEB by running the command
   ```
   dpkg -i client_ package_path
   ```
3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
4. Start the client by running the command:
   ```
   /etc/init.d/besclient start
   ```

CentOS Installation Instructions

To install the client perform the following steps:

1. Download the corresponding client RPM file to the Red Hat computer.
2. Install the RPM by running the command

   ```
   rpm -ivh client_RPM_path
   ```

3. Copy your actionsite masthead to the client computer (the masthead contains configuration, license, and security information). The action site masthead (`actionsite.afxm`) can be found in your BES Installation folders (by default they are placed under `C:\Program Files (x86)\BigFix Enterprise\BES Installers\Client` on Windows and `/var/opt/BESInstallers/Client/` on Linux). If the masthead is not named `actionsite.afxm`, rename it to `actionsite.afxm` and place it on the computer at the following location: `/etc/opt/BESClient/actionsite.afxm`.

   Note: The directory `/etc/opt/BESClient/` is not automatically created by the installer. If it does not exist, create it manually.
   The masthead file for each server is downloadable at `http://`*`servername`*`:`*`port`*`/masthead/masthead.afxm` (example: `http://bes.Endpoint Manager.com:52311/masthead/masthead.afxm`).
4. Start the client by running the command:

   ```
   /etc/init.d/besclient start
   ```

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 of the Windows server and in the `/ServerInstaller_9.1.`*`xxx.x`*`-rhe6.x86_64/repos/ClientMSI` folder of the Linux server.

To install the Windows client perform the following steps:

1. Copy the `BESClientMSI.msi` program on the `c:\BESInstallers\ClientMSI` folder of a Windows system.
2. If you do not run the `BESClientMSI.msi` program located in the `BESInstallers\ClientMSI` folder of the Windows server, you must copy the `actionsite.afxm` masthead located in the server, to the client installation directory that can be the default installation directory, `%PROGRAM FILES%\BigFix Enterprise\BES Client`, or a specific installation directory, `INSTALLDIR="c:\myclient"`.
3. Run the `BESClientMSI.msi` program in one of the following ways:

   -
     ```
     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 specified directory (`INSTALLDIR="c:\myclient"`).

   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 7. Transform file list

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 Command-Line Options. To create a Group Policy Object (GPO) for BESClientMSI deployments, see the Microsoft knowledge base article: http://support.microsoft.com/kb/887405.

4. Start the BES client service.

Running the Administration Tool

The installation script `install.sh` automatically downloads the 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 ob enable and disable enhanced security, resign all of the users content in the database, rotate the server private key, configure the Console and Web Reports login, resign the database content and synchronize the masthead with the updated license.

Run this script as super user from the command prompt using the following syntax:

```
./BESAdmin.sh -service { arguments }
```

where *service* can be one of the following:

```
changeprivatekeypassword
editmasthead
findinvalidsignatures
minimumSupportedClient
repair
reportencryption
resignsecuritydata
rotateserversigningkey
securitysettings
setadvancedoptions
syncmastheadandlicense
```

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

Each service has the following *`arguments`* :

changeprivatekeypassword

You can use this service to be prompted for a new password to associate to the license.pvk file. Use the following syntax to run the command:

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

editmasthead

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

```
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)

advRequireFIPScompliantCrypto (optional, boolean)
```

The syntax to run this service is:

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

For additional information, see the *IBM Endpoint Manager Configuration Guide*.

findinvalidsignatures

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

-resignInvalidSignatures (optional)
Attempts to resign any invalid signatures that BESAdmin finds.

-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
[ -resignInvalidSignatures | -deleteInvalidlySignedContent ]
```

minimumSupportedClient

This service defines the minimum version of the Agents used in your environment.

Note: Based on this setting, the components can decide when it is safe to assume the existence of newer functions across all the component in the deployment. Individual agent interactions might be rejected if the interaction does not comply with the limitations imposed by this setting.

The currently available values are:

- **8.2** which means that no activity issued by Agents V8.2, such as registration to server, archive files and reports uploads, are prevented from running or limited. This behavior applies also if the `minimumSupportedClient` service is not set.
- **9.0** which means that:
  - Initial or regular registrations of V8.2 Clients to a Relay or to the Server succeed.
  - Reports sent by V8.2 Clients are discarded by FillDB.
  - The upload of an archive file generated on a V8.2 Client, by an **archive now** command for example, fails.

If you ran a fresh installation of V9.1.11 the `minimumSupportedClient` is not set and so all the agents, regardless of their version, can join your environment.

The syntax to run this service is:

```
./BESAdmin.sh -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>]
   -minimumSupportedClient:<version>.<release>
```

If you omit to specify `[sitePvkPassword=<password>]` you are prompted to enter the password when the **BESAdmin.sh** runs.

For example, if you want to state that agents V8.2 are not supported in your environment, you can run the following command:

```
./BESAdmin.sh -sitePvkLocation=/license/license.pvk -minimumsupportedclient:9.0
```

repair

You can use a repair utility to handle an inconsistency between the keys stored in the database and those stored on the filesystem. When the following command is run the key on the file system are recreated from the keys stored on the database:

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

reportencryption

You can generate, rotate, enable and disable encryption for report messaging by running:

```
BESAdmin.sh -reportencryption { -status |
  -generatekey [-privateKeySize=<min|max>]
               [-deploynow=yes | -deploynow=no -outkeypath=<path>]
               -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>] |
  -rotatekey [-privateKeySize=<min|max> ]
             [-deploynow=yes | -deploynow=no -outkeypath=<path> ]
             -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>] |
  -enablekey -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>] |
  -disablekey -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>] }
```

where:

status Shows the status of the encryption and which arguments you can use for that status

generatekey
Allows you to generate a new encryption key.

rotatekey
Allows you to change the encryption key.

enablekey
Allows you to enable the encryption key.

disablekey
Allows you to put the encryption key in PENDING state. If you issue again the `reportencryption` command with the `disablekey` argument, the encryption changes from PENDING state to DISABLED.

For more information about this command and its behavior, see Managing Client Encryption.

resignsecuritydata

You can resign all of the users content in the database to enable user login to the Console. The command resigns security data using the existing key file. You can specify the following parameter:

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

The complete 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 command creates a new server signing key, resigns all existing content using the new key, and revokes the old key.

The syntax to run this service is:

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

securitysettings

You can configure enhanced security options to follow the NIST security standards by running the command:

```
./BESAdmin.sh -securitysettings -sitePvkLocation=<path+license.pvk>
[ -sitePvkPassword=<password> ]
{ -status | -enableEnhancedSecurity [-requireSHA256Downloads]
| -disableEnhancedSecurity | -requireSHA256Downloads
| -allowSHA1Downloads} }
```

where:

status Shows the status of the security settings set in your environment.

Example:

```
BESAdmin.sh -securitysettings -sitePvkLocation=/root/backup/license.pvk
-sitePvkPassword=mypassw0rd -status

Enhanced security is currently ENABLED
SHA-256 downloads are currently OPTIONAL
```

enableEnhancedSecurity | disableEnhancedSecurity
Enables or disables the enhanced security that adopts the SHA-256

cryptographic digest algorithm for all digital signatures as well as content verification and the TLS 1.2 protocol for communications among the Endpoint Manager components.

Note: If you use the **enableEnhancedSecurity** setting you break the backward compatibility because version 9.0 or earlier components cannot communicate with the version 9.1 server or relays.

requireSHA256Downloads

Ensures that data has not changed after you download it using the SHA-256 algorithm.

Note: The **Require SHA-256 Downloads** option is available only if you selected to **Enable Enhanced Security**.

allowSHA1Downloads

Ensures that the file download integrity check is run using the SHA-1 algorithm.

For more information about the Enhanced Security feature and the supported security configuration, see Chapter 4, "Security Configuration Scenarios," on page 23.

setadvancedoptions

You can list or configure any global settings that apply to your particular installation. For example you can set your Console or Web Report login banner to be displayed by entering the following command:

```
./BESAdmin.sh -setadvancedoptions -sitePvkLocation=/root/backup/license.pvk
-sitePvkPassword=pippo000 -update loginWarningBanner='new message'
```

The complete syntax to run this service is:

```
./BESAdmin.sh -setadvancedoptions -sitePvkLocation=<path+license.pvk>
[-sitePvkPassword=<password>]
{ -list | -display
| [ -f ] -delete option_name
| [ -f ] -update option_name=option_value }
```

These are some of the advanced options that you can specify:

Table 8. Advanced Settings Names

Name	Value
loginWarningBanner	If set with text, any user who logs into the Console or Web Reports will be shown the text after they log in. The user will have to click **OK** to continue.
timeoutLockMinutes	The amount of idle time in minutes before the console requires to authenticate again. This is different from **loginTimeoutSeconds** in that timeout lock will hide the entire console to prevent any other user to see or use it. Idle time refers to the lack of any type of input to the session including key buttons, mouse clicks, and mouse movements.

Note: Non efficient mime advanced option is no longer is supported by the 9.1 server. Existing actions continue to run on clients but the server is no longer able to generate non efficient mime actions.

syncmastheadandlicense

When you upgrade the product you must use this option to synchronize the update license with the masthead and resign all content in the database with SHA-256. The syntax to run this service is:

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

Removing the Primary Server on Linux systems

To uninstall the 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
   ```

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. Ensure you specify the identifier of the server to delete. You must log in to the DB2 database and run the following procedure:

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

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

Chapter 10. Post-installation configuration steps

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

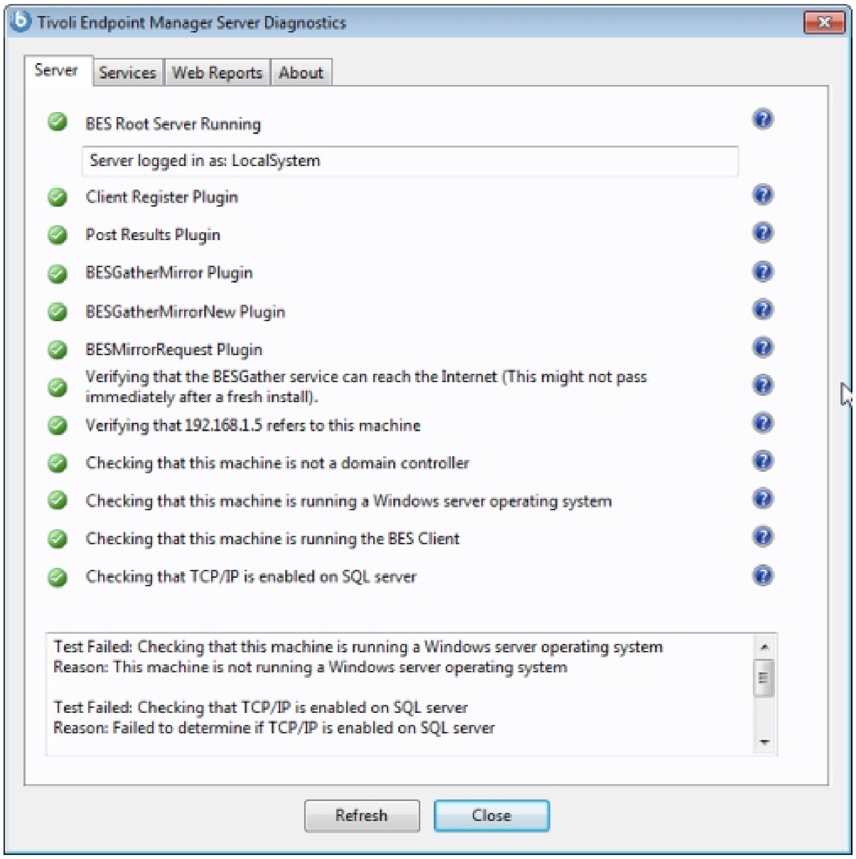
Post-installation steps

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 Server Diagnostics tool to verify that all the installation and configuration steps completed successfully.

   ✓ BES Root Server Running

   Server logged in as: LocalSystem

   ✓ Client Register Plugin

   ✓ Post Results Plugin

   ✓ BESGatherMirror Plugin

   ✓ BESGatherMirrorNew Plugin

   ✓ BESMirrorRequest Plugin

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

   ✓ Verifying that 192.168.1.5 refers to this machine

   ✓ Checking that this machine is not a domain controller

   ✓ Checking that this machine is running a Windows server operating system

   ✓ Checking that this machine is running the BES Client

   ✓ Checking that TCP/IP is enabled on SQL server

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

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

   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.

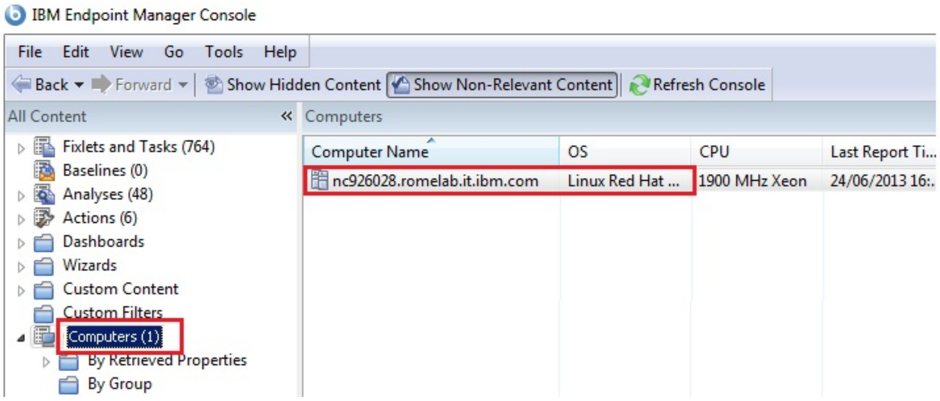
   On Linux:

   Ensure that the following services are up and running:

   ```
   besfilldb
   besgatherdb
   besserver
   beswebreports
   ```

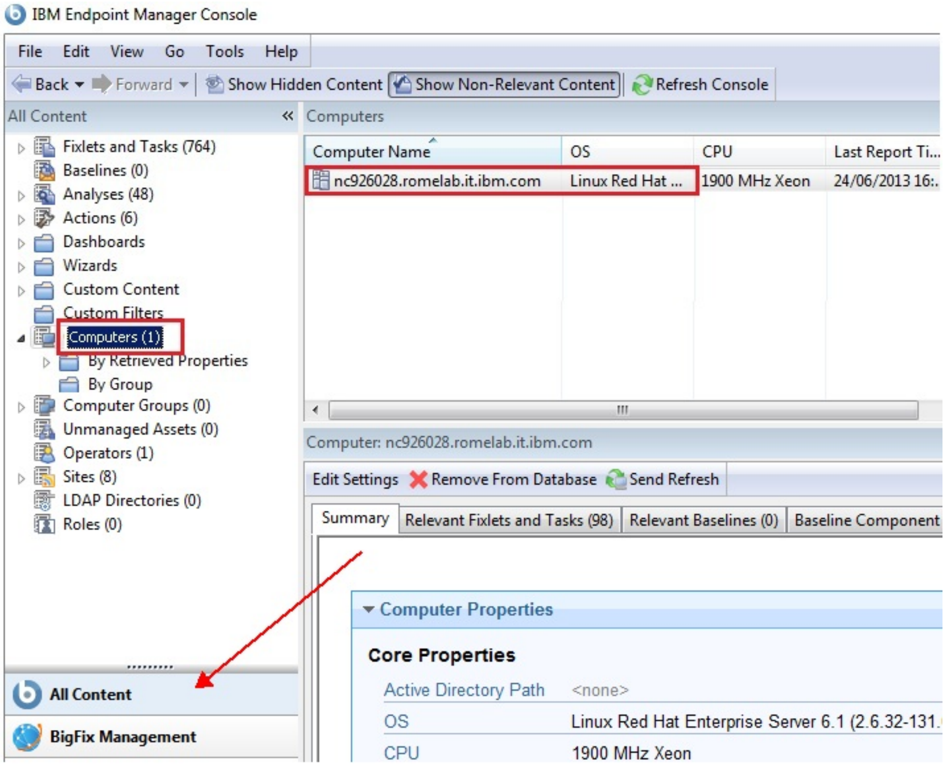
Use the command `service` *`service`* `status` to check the status of the services.

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



Computer Name	OS	CPU	Last Report Ti...
nc926028.romelab.it.ibm.com	Linux Red Hat ...	1900 MHz Xeon	24/06/2013 16:.

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

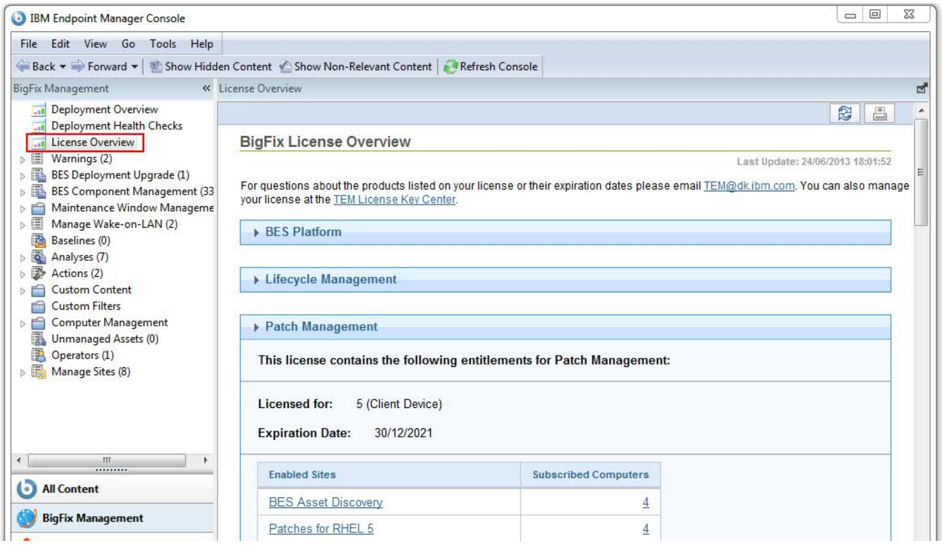


Computer Name	OS	CPU	Last Report Ti...
nc926028.romelab.it.ibm.com	Linux Red Hat ...	1900 MHz Xeon	24/06/2013 16:.

Computer: nc926028.romelab.it.ibm.com

Active Directory Path	<none>
OS	Linux Red Hat Enterprise Server 6.1 (2.6.32-131.
CPU	1900 MHz Xeon

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 client. Subscribe to these sites from the **BigFix Management** domain, by selecting the **License Overview** dashboard:



BigFix License Overview

Last Update: 24/06/2013 18:01:52

For questions about the products listed on your license or their expiration dates please email TEM@dk.ibm.com. You can also manage your license at the TEM License Key Center.

BES Platform

Lifecycle Management

Patch Management

This license contains the following entitlements for Patch Management:

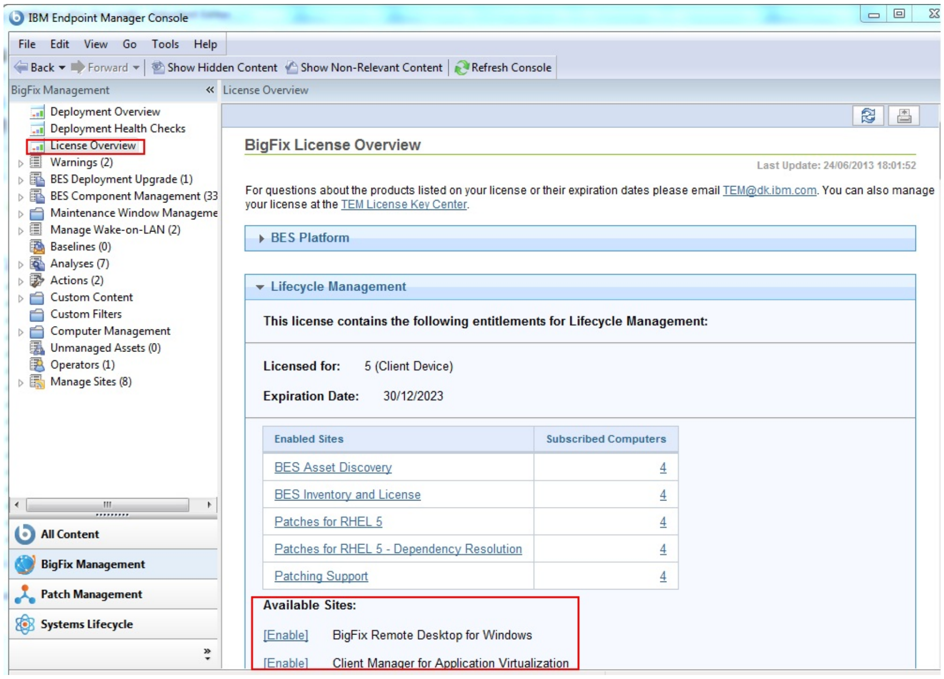
Licensed for: 5 (Client Device)

Expiration Date: 30/12/2021

Enabled Sites	Subscribed Computers
BES Asset Discovery	4
Patches for RHEL 5	4

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:



BigFix License Overview

Last Update: 24/06/2013 18:01:52

For questions about the products listed on your license or their expiration dates please email TEM@dk.ibm.com. You can also manage your license at the TEM License Key Center.

BES Platform

Lifecycle Management

This license contains the following entitlements for Lifecycle Management:

Licensed for: 5 (Client Device)

Expiration Date: 30/12/2023

Enabled Sites	Subscribed Computers
BES Asset Discovery	4
BES Inventory and License	4
Patches for RHEL 5	4
Patches for RHEL 5 - Dependency Resolution	4
Patching Support	4

Available Sites:

[Enable] BigFix Remote Desktop for Windows

[Enable] Client Manager for Application Virtualization

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.

Starting and stopping the IBM Endpoint Manager server

Complete the following steps to start and stop IBM Endpoint Manager server installed on a Windows system:

Steps to start IBM Endpoint Manager:
Start the following Windows services in the specified order:

```
BES Root Service
BES FillDB
BES GatherDB
BES Client
BES Web Reports Service
```

Steps to stop IBM Endpoint Manager:
Stop the following Windows services in the specified order:

```
BES Web Reports Service
BES Client
BES GatherDB
BES FillDB
BES Root Service
```

Complete the following steps to start and stop IBM Endpoint Manager server installed on a Linux system:

Steps to start IBM Endpoint Manager:
Run the following services in the specified order:

```
service besserver start
service besfilldb start
service besgatherdb start
service beswebreports start
service besclient start
```

Steps to stop IBM Endpoint Manager:
Run the following services in the specified order:

```
service besclient stop
service beswebreports stop
service besgatherdb stop
service besfilldb stop
service besserver stop
```

Subscribing to Fixlet sites

Sites are collections of Fixlet 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 .

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 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 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.

Chapter 11. Managing 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 improve performance by:

- **Relieving downstream traffic**. Using relays, the server does not need to distribute files, such as patches or software packages, and Fixlets to every Client. Instead, the file is sent once to the relay, which in turn distributes it to the clients.
- **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, the server sends only a single copy to the relay (if it needs it). That relay, in turn, distributes the file to the other computers in the remote office over its own fast LAN.

Establishing the appropriate relay structure is one of the most important aspects of deploying 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.

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

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.

For additional information about relays see the Relays page.

Relay requirements and recommendations

Generally, a relay uses minimal resources and does not have a noticeable impact on the performance of the computer running it. However, if several clients simultaneously request files from a relay, a significant amount of the computer's resources might be used to serve those files.

The requirements for a relay computer vary widely depending on three main factors:

- The number of connected clients that are downloading files.
- The size of each download.
- The period of time allotted for the downloads.

The relay system requirements are similar to those for a workgroup file server. For details about relay requirements, seeIBM Endpoint Manager 9.1 - System Requirements.

Here are some further recommendations:

- Computers running the relays must have agent installed.
- Workgroup file servers and other server-quality computers that are always turned on are good candidates for installing a relay.
- The relay must have a two-way TCP connection to its parent (which can be a server or another relay).
- Computers running the relays must have at least Internet Explorer 4.0 or later to work correctly.
- The 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.
- It is recommended to have at least one Relay per geographic location for bandwidth reasons.
- Consider throttling the bandwidth usage for Relays downloading files on very slow pipes. It is recommended to throttle the bandwidth usage for Clients that are connecting on dial-up or slow VPN connections. For more information about bandwidth throttling, see Bandwidth Throttling.

Setting up a relay

To set up a relay, you must designate a Windows, Red Hat Enterprise Linux, or Solaris computer that is running a client to act as the relay. For more information about the supported operating systems, see IBM Endpoint Manager 9.1 - System Requirements.

The clients on your network detect the new relays and automatically connect to them. To configure a client computer as a relay, run the following steps:

1. Log in to the console.
2. Open the **Fixlets and Tasks** icon in the Domain Panel and click **Tasks Only**.
3. Double-click the task labeled **Install 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.
4. Choose your deployment option by selecting one of the actions in the task. You can target single or multiple computers with this action.

After the relays have been created, Clients can be made to automatically discover and connect to them, always seeking the Relay that is the fewest hops away.

Assigning relays to clients

When you have set up a relay you must direct IBM Endpoint Manager clients on your network to gather from that relay, instead of from your server. You can:

- Assign relays manually as it is described in the following topics:
  - "Assigning relay at client installation time" on page 125
  - "Manually assigning relays to existing clients" on page 127
- Assign relays automatically, that means to allow clients to identify the closest relay to connect to, as it is described in the following topics:
  - "Automatically assigning relays at client installation time" on page 127
  - "Automatically assigning relays to existing clients" on page 127

  If you select this method, you can also choose to exploit the relay affiliation functionality. Using this functionality you create groups of affiliated clients and you assign relays to the affiliation group. For more information about this functionality and how to use it, see "Using relay affiliation" on page 128.

For more information and considerations about automatic relay assignment, see "Notes about automatic relay assignment" on page 129.

Assigning relay at client installation time

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

If you want you can configure the client to assign a specific 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"
- "UNIX Clients"
- "Mac Clients"

Windows Clients

Create a three line file called `clientsettings.cfg`, with the following content, and include this file in the 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 client installation package.

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-9.1.`*xxx.x*`-BigFix_MacOSX`*xx.x*`.pkg/Contents/Resources`.

In the Finder, right-click `BESAgent-9.1.`*xxx.x*`-BigFix_MacOSX`*xx.x*`.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 relay, see http://www-01.ibm.com/support/docview.wss?uid=swg21506065.

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)):

Manually assigning relays to existing clients

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. 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** .

Automatically assigning relays at client installation time

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.

Automatically assigning relays to existing clients

You can configure clients to 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. Clients can determine which relays are the fewest number of hops away, so your topology is optimized.

This behavior is key when your network configuration is constantly shifting as laptops dock and undock, as computers start up or shut down, or as new hardware is added or removed. Clients can dynamically assess the configuration to maintain the most efficient connections as your network changes.

To make sure that your clients are set up to automatically discover relays run the following steps:

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

2. Shift- and ctrl-click to select the set of computers you want to 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**.

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 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.

Choosing relay affiliation group names

There are no predefined relay affiliation group names; you can choose any group names that are logical to your deployment of . 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 support site.

Assigning clients to relay 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
```

Associating relays and server to 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.

Notes about automatic relay assignment

The 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 support site.

Adjusting the Server and Relays

To get the best performance from , you might need to adjust the server and the relays. There are two important ways of adjusting the flow of data throughout your network, throttling and caching:

Throttling Outgoing Download Traffic

Throttling allows you to set the maximum data rate for the IBM Endpoint Manager Server. Here is how to change the data rate:

1. Open **Fixlets and Tasks** icon in the Domain Panel navigation tree and then click **Tasks Only**.
2. In the find window above the Tasks List, type "throttle" to search for the appropriate Task.

3. From the resulting list, click the task labeled **Server Setting: Throttle Outgoing Download Traffic**. A task window opens below. Make sure the **Description** tab is selected. There are three choices:
   - **Set the limit on total outgoing download traffic.** This choice allows you to directly set the maximum number of kilobytes per second you want to grant to the server.
   - **Disable the setting.** This option lets you open the download traffic on the Server to full throttle.
   - **Get more information.** This option opens a browser window with more detailed information about bandwidth throttling.
4. If you select a throttle limit, then from the subsequent **Take Action** dialog you can select a set of computers to throttle. Click **OK** to propagate the task.

Download Cache Size

Servers and Relays maintain a cache of the downloads most recently requested by Clients, helping to minimize bandwidth requirements.

1. Open **Fixlets and Tasks** icon in the Domain Panel navigation tree and then click **Tasks Only**.
2. In the find window above the Tasks List, type "cache" to search for the appropriate Task.
3. From the resulting list, click the task labeled **Relay / Server Setting: Download Cache Size**. A task window opens below. Make sure the **Description** tab is selected. Select the link to change the download cache size on the listed computers. This list might include Relays as well as the Server.
4. Enter the number of megabytes to cache. The default is 1024 MB, or one gigabyte.
5. From the subsequent **Take Action** dialog, select a set of computers and click **OK**.

Dynamic bandwidth 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 elsewhere, it is possible to simply set a maximum value (throttle) for the data rates, and for this there are broad-based policies you can follow. You might, for example, throttle a IBM Endpoint Manager Client to 2Kb/s 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 do not use any more than 10% of the available bandwidth whenever the program detects existing network traffic. Dynamic throttling also provides for a minimum data rate, in the case the busy percentage is too low to be practical.

When you enable dynamic throttling for any given link, the program 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, the program throttles the data rate to the specified percentage or the minimum rate, whichever is higher. You must enable dynamic throttling on both the server and the client side to have it work correctly.

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

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

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

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

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

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

The specific variable names include:

The IBM Endpoint Manager server and 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 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 choosees the smaller value of the two.

Assigning a relay when the server is unreachable

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

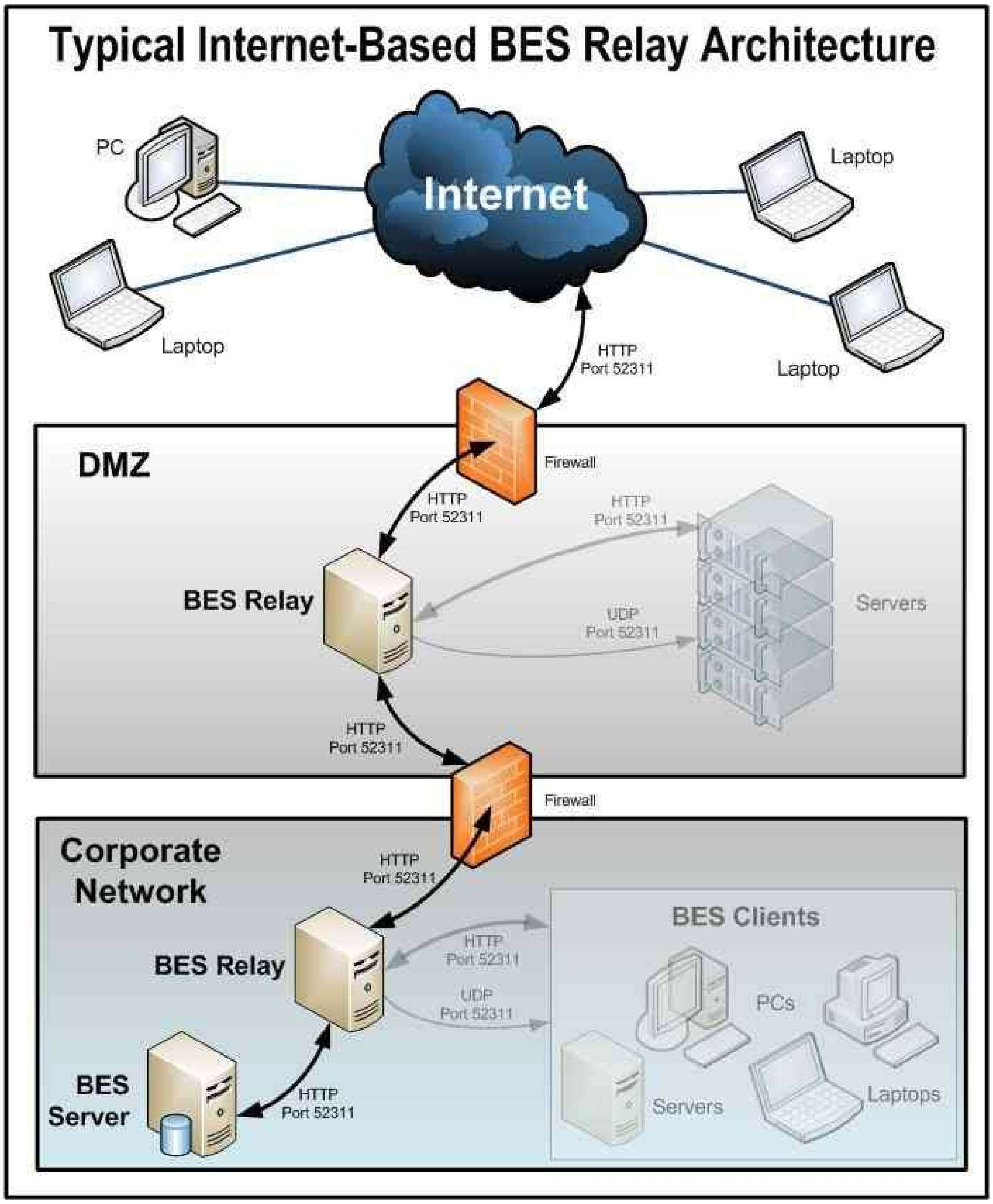
Setting internet relays

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 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:



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 relay architecture:

1. A relay is deployed in a DMZ and the internal DMZ firewall allows only 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 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 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 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.

Client Authentication

Client Authentication (introduced in version 9) extends the security model used by IBM Endpoint Manager to encompass trusted client reports and private messages. This feature is not backward-compatible, and clients prior to version 9.0 will not be able to communicate with an authenticating relay or server.

Starting from version 9.1.11, you can use the **minimumSupportedClient** setting to specify the minimum version of BigFix Agents that are used in your environment. If the minimum version required is 9.0 or above, the client authentication is required for all the clients to register and operate. For more information about this configuration, see “Additional administration commands” on page 76 for Windows system, or “Running the Administration Tool” on page 111 for Linux systems.

The original security model has two central capabilities:

- **Clients trust content from server.** All commands and questions that clients receive are signed by a key that is verified against a public key installed on the client.
- **Clients can submit private reports to server.** The client can choose to encrypt reports that it sends up to the server, so that no attacker can interpret what is contained in the report. This feature is disabled by default, and is switched on with a setting.

Client Authentication extends the security model to provide the mirror image of these two capabilities:

- **Server can trust reports from clients (non-repudiation).** Clients sign every report that they submit to the server, which is able to verify that the report does not come from an attacker.
- **Server can send private data to clients (mailboxing).** The server can encrypt data that it sends to an individual client, so that no attacker can interpret the data.

Communication using an authenticated relay is a two-way trusted and private communication channel that uses SSL to encrypt all communications. However, communication between a non-authenticating relay and its children is not encrypted unless it is an encrypted report or a mailboxed action or file.

This level of security is useful for many purposes. Your company may have security policies that require authenticating relays on your internet-facing nodes, in your DMZ, or any network connection that you don’t totally trust. With authentication, you can prevent clients that haven’t yet joined your deployment from getting any information about the deployment.

Authenticating relays

Relays can be configured as authenticating relays to authenticate agents. This way, only trusted agents can gather site content or post reports. Use authenticating relay configuration for an internet-facing relay in the DMZ.

A relay configured to authenticate agents only performs SSL communication with child agents or relays that present an SSL certificate issued and are signed by the server during a key exchange.

To configure an authenticating relay, set the client setting `_BESRelay_Comm_Authenticating` to 1 or use the related task in the BES Support site. To configure an open relay again, set `_BESRelay_Comm_Authenticating` to `0` or use the related task in the BES Support site. The default value is `(0)`, open relay.

Handling the key exchange

When an agent tries to register and does not have a key and certificate, it automatically tries to perform a key exchange with its selected relay. If the relay is a non-authenticating relay, it forwards the request up the relay chain to the server, which signs a certificate for the agent. This certificate can later be used by the agent when connecting to an authenticating relay.

Authenticating relays deny these automatic key exchange operations. The following is a typical scenario:

When you deploy a new 9.1 environment or upgrade an existing environment to 9.0 all agents automatically perform the key exchange with their relays. If the administrator configures the internet facing relay as an authenticating relay, the existing agents already have the certificate and work correctly. No further action is required. When you connect new agents to the authenticating relay they do not work, until the manual key exchange procedure is run on them.

Manual key exchange

If an agent does not have a certificate and can only reach an authenticating relay on the network, connected through the internet, you can manually run the following command on the agent so it can perform the key exchange with an authenticating relay:

```
BESClient -register <password> [http://<relay>:52311]
```

The client includes the password in its key exchange with the authenticating relay, which verifies it before forwarding the key exchange to its parent.

You can configure the password as:

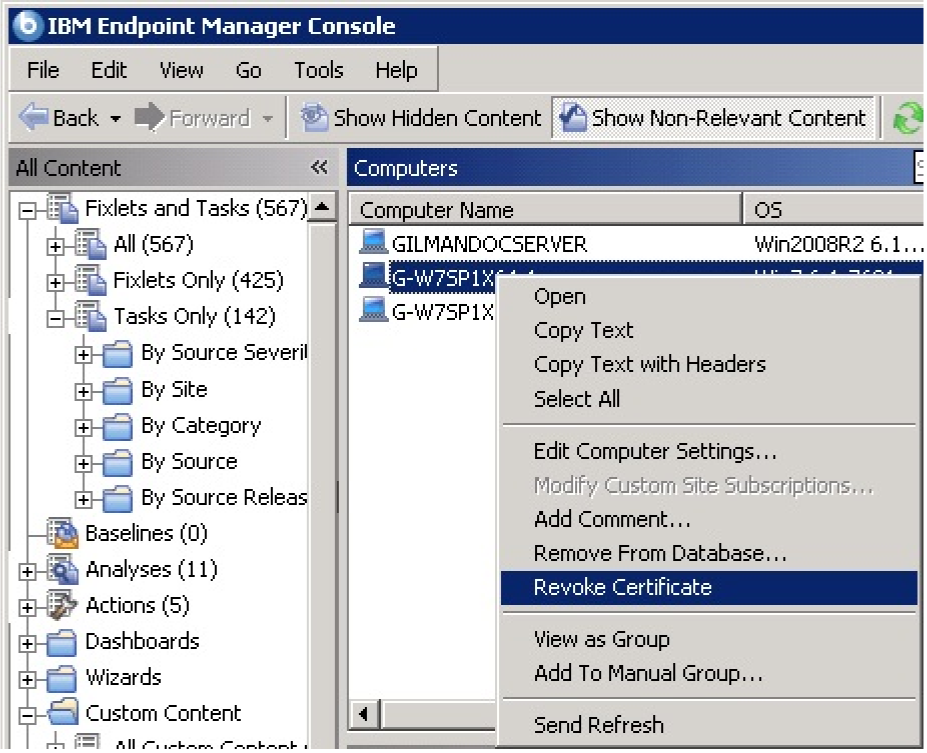
- A single password in the client setting `_BESRelay_Comm_KeyExchangePassword` on the relay.
- A newline-delimited list of one-time passwords stored in a file named `KeyExchangePasswords` in the relay storage directory (value **StoragePath** of `HKLM\SOFTWARE\BigFix\Enterprise Server\GlobalOptions`).

Revoking Client Certificates

After a client authenticates, you can revoke its certificate if you have any reason to doubt its validity. When you do, that client is no longer authenticated for trusted communication. It is removed from the console and a revocation list is updated and collected by all relays, so that the client's key can no longer be used to communicate with authenticating relays.

To revoke a computer:

1. Right-click a computer in any list of computers.



2. From the pop-up menu, click **Revoke Certificate**.
3. From the confirmation dialog click **OK** if you are sure you want to remove the computer's certificate.

This sends revocations down to the relays. Once revoked, that client can no longer use its private key to gather content from the authenticating relays. The revoked client disappears from the computer list in the console.

Re-registering a revoked client

When a certificate is revoked, the compromised key is discarded. However, the client can rejoin the network in two ways.

- In an authenticating environment, if the client can only access authenticating relays, the client is required to use the manual exchange method if automatic key exchange did not previously take place.
- In an open (non-authenticating) environment, the client can re-register itself with a non-authenticating relay.

In all cases, the computer gets a fresh certificate and a new computer id.

Important: In an authenticating environment, if the client can access a non-authenticating relay or server, the client can exchange keys and re-register automatically even if it was explicitly revoked.

Mailboxing

With Client Mailboxing you can send an encrypted action to any given client, instead of broadcasting it to all clients. This improves efficiency, since the client doesn’t need to qualify every action, and it minimizes network traffic. As a consequence,

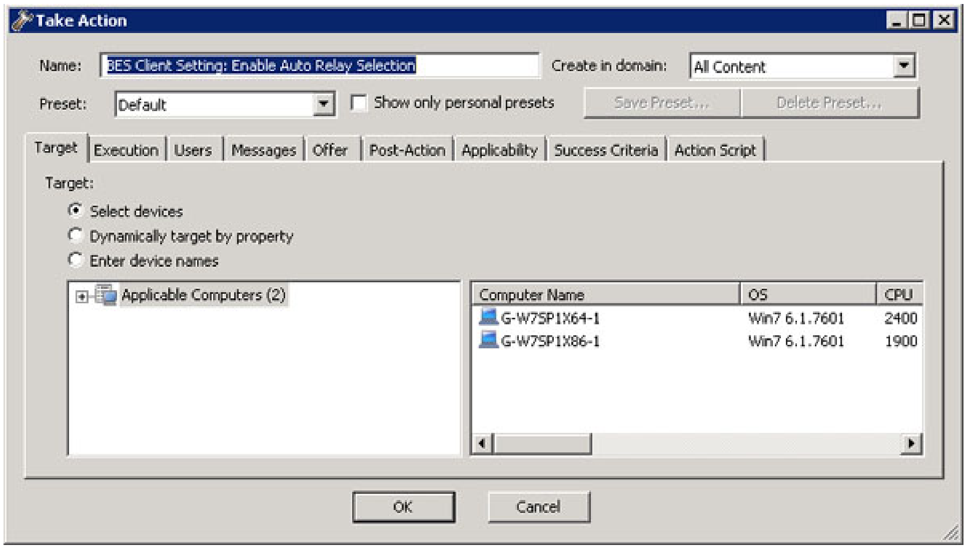
- Clients are only interrupted when they are targeted.
- Clients don't have to process actions that are not relevant to them for reporting, evaluating, gathering, and action processing.

Privacy is assured because the message is encrypted specifically for each recipient; only the targeted client can decrypt it.

A client's mailbox is implemented as a specialized action site, and each client is automatically subscribed to it. The client knows to scan for actions in this site as well as the master site and operator sites.

To send an encrypted action directly to a client mailbox, follow these steps:

1. Open the **Take Action** dialog (available from the Tools menu and various other dialogs).



Take Action

Name: BES Client Setting: Enable Auto Relay Selection

Create in domain: All Content

Preset: Default

□ Show only personal presets

Target:

● Select devices
○ Dynamically target by property
○ Enter device names

Applicable Computers (2)

Computer Name	OS	CPU
G-W7SP1X64-1	Win7 6.1.7601	2400
G-W7SP1X86-1	Win7 6.1.7601	1900

2. Click the **Target** tab.
3. Click **Select devices** or **Enter device names**. Mail-boxing is only available when you specify a static list of clients. Dynamically targeted computers will not be encrypted and will instead be sent in the open to the master site or a specific operator site. If you target clients with versions prior to 9.0, the action will also go into the master or operator site.
4. Click **OK**. Actions targeted by computer ID or name will now be encrypted and sent to the client mailbox.

The identifier of the operator who deploys the action is included with the action. Before a client takes the action, it first determines if it is currently administered by that operator. If not, it refuses to run the action.

Viewing which relay is assigned to a client

To see which clients are selecting which relays run the following steps:

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 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 support site.

Monitoring relays health

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.

Chapter 12. Setting up a proxy connection

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

The proxy connection is also used by the 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 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 up a proxy connection on the server" on page 143. 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 145.

A client needs to connect to the Internet through a proxy to communicate with its parent relay.
To set this configuration, run on the client the steps that are described in "Setting up a proxy connection on a client" on page 146.

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

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 version 9.1 or on an older version.

The following tables list, for each component, the steps to complete to set up the proxy configuration.

Table 9. . Steps to configure communication through a proxy on an version 9.1 server

Server	
Linux	Windows

Table 9. (continued). Steps to configure communication through a proxy on an version 9.1 server

Server	
In the besserver.config file set, add the keys: Proxy ProxyUser ProxyPass ProxyExceptionList For details, see "Setting up a proxy connection on the server" on page 143.	Run the BESAdmin command as described in "Setting up a proxy connection on the server" on page 143.
or	
Set the concatenated key Proxy = [<proxy_user>:<proxy_password>@]<proxy_hostname>[:<proxy_port>] as described in "Setting up a proxy connection on the server" on page 143.	

Table 10. . Steps to configure communication through a proxy on an version 9.1 relay

Relay	
Linux and Windows	
To communicate with the parent component (relay or server):	To download files from the Internet:

Set the client connection settings that are specified in "Setting up a proxy connection on a relay" on page 145.
Optionally, use the proxy exception list setting to specify local computers or domains that must be reached without using the proxy.
	Set
	_BESGather_Download_CheckInternetFlag = 1
	_BESGather_Download_CheckParentFlag = 0
	as described in "Setting up a proxy connection on a relay" on page 145.

Table 11. . Steps to configure communication through a proxy on an version 9.1 client

Client
Linux and Windows
Set the client connection settings that are specified in h. Optionally, use the proxy exception list setting to specify local computers or domains that must be reached without using the proxy.

Note: The configuration settings that are used in version 9.1 do not use the `BESGatherService`, which is deprecated.

The configuration to communicate through a proxy might differ if you upgrade to version 9.1 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 version 8.2 environment to version 9.1, 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 version 9.1.

Setting up a proxy connection on the server

On version 9.1 server, 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 stored in the Windows registry.

Run the following command to create or modify the proxy configuration in the registry:

```
C:\Program Files\BigFix Enterprise\BES Server\BESAdmin.exe /setproxy /proxy:<proxy_host>[:
[/user:<proxy_username> /pass:<proxy_password>] [/exceptionlist:<proxy_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 using the keys:

```
Proxy = <proxy_host>[:<proxy_port>]
ProxyUser = <proxy_username>
ProxyPass = <proxy_password>
ProxyExceptionList = <proxy_exceptionlist>
```

If you want to set a proxy configuration you must edit the `besserver.config` file manually.

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

proxy_host[:proxy_port]

It specifies the hostname or IP address and, optionally, the port number of the proxy machine. Specify either the *`<hostname>`* or the *`<IP_address>`* as `<proxy_host>`.

proxy_username

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

If you installed your server on a Windows system and your proxy requires Kerberos Authentication, use the format *user@mydomain.com*.

If you installed your server on a Windows system and your proxy requires NTLM Authentication, specify the NTLM user.

If your proxy requires the domain/realm, the user might need to be specified as *user@mydomain.com* or as *mydomain/user*.

Note: On Windows the user that you specify must log in to the server and configure its Internet Options to use the proxy.

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

proxy_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.

proxy_exceptionlist

This is an optional setting that you can use to specify computers, domains and subnetworks that must be reached without passing through the proxy. Specify its value using this format:

```
"hostname1, hostname2, IP_Addr_A, IP_Addr_B, domain_Z, domain_Y, ..."
```

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

These are sample values that you can assign to `<proxy_exceptionlist>`:

```
example.com
example.com,8.168.117.0
"example.com, 8.168.117.0"
```

To prevent diverting internal communications towards the proxy agent, add `localhost, 127.0.0.1` when specifying `<proxy_exceptionlist>`.

The proxy exception list was introduced in version 9.0.835.0 (Patch 5) for Windows and Linux systems. If you are using version 9.0 and you have problems using content that downloads files from the local server, upgrade to version 9.0.835.0.

On 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 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 the following table:

Table 12. Proxy 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 Mandatory: Yes
`_Enterprise Server _ClientRegister _ProxyPort`	Sets the port that is used by the proxy server.	Default Value: None Setting Type: String Value Range: N/A Mandatory: Yes
`_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 Mandatory: No (depending on the authentication method)
`_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 Mandatory: No (depending on the authentication method)

6. Optionally specify the proxy exception list setting if the relay must communicate to its parent relays without passing through the proxy.

Table 13. Proxy optional configuration settings

Setting Name	Setting Value	Details
`_Enterprise Server _ClientRegister _ProxyExceptionList`	Specifies the computers, domains and subnetworks that must be reached by the relay without passing through the proxy. Use the following format: "*hostname1, hostname2, IP_Addr_A, IP_Addr_B, domain_Z, domain_Y, ...*"	Default Value: None (always passes through the proxy) Setting Type: String Value Range: N/A Mandatory: No

   For more information about how to specify the proxy exception list, see "Setting up a proxy connection on the server" on page 143.

7. Click **OK** to send out the configuration settings, which take effect immediately.

Specify the proxy exception list setting if the relay must communicate to its parent relays without passing through the proxy.

Depending on which platform the relay is installed, add the proxy exception list 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.

The syntax used to specify the proxy exception list is described in "Setting up a proxy connection on the server" on page 143.

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

To set the proxy connection on the client complete the following steps:

1. Open the console and go to the **Computer** section under the **All Content** domain.
2. Select the computer where the client 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** as described in the following table:

Table 14. Proxy client configuration settings

Setting Name	Setting Value	Details
`_BESClient_Comm _ProxyServer`	Sets the hostname that is used to reach the proxy.	Default Value: None Type: String Value Range: N/A Mandatory: Yes
`_BESClient_Comm _ProxyPort`	Sets the port that is used to communicate with the proxy.	Default Value: None Type: Numeric Value Range: N/A Mandatory: No
`_BESClient_Comm _ProxyUser`	Sets the user name that is used to authenticate with the proxy if the proxy requires authentication.	Default Value: None Type: String Value Range: N/A Mandatory: No (depending on the authentication method)

Table 14. Proxy client configuration settings (continued)

Setting Name	Setting Value	Details
`_BESClient_Comm _ProxyPass`	Sets the password that is used to authenticate with the proxy if the proxy requires authentication.	Default Value: None Type: String Value Range: N/A Mandatory: No (depending on the authentication method)
`_BESClient_Comm _ProxyManualTryDirect`	Specifies whether direct connections can be used. This setting applies if the connection to the proxy uses the hostname or IP Address and port number that are specified in `_BESClient_Comm _ProxyServer` and `_BESClient_Comm _ProxyPort`. These values are available: **0** Do not try direct connection. **1** Try direct connection if a proxy connection cannot be established. **2** Try direct connection first.	Default Value: 0 Type: Numeric Value Range: 0-2 Mandatory: No

Note: On Linux systems, at run time, the searches and, if specified, uses the configuration stored in the client configuration file. If the requested configuration is not specified in the client configuration file, the product searches for it in the server configuration file, or in the relay configuration file. Consider this behavior when defining the proxy configuration on the server or relay.

If the client is installed on a Windows system where Internet Explorer is configured to use a proxy, then, by default, uses the Internet Explorer configuration to communicate with the proxy. The following table shows the additional settings and behaviors that you can optionally specify on Windows platform:

Table 15. Proxy client additional configuration settings on Windows systems

Setting Name	Setting Value	Details
_BESClient_Comm _ProxyAutoDetect	Specifies whether the system uses the proxy configuration settings that are specified for Internet Explorer. The following values are available: **0** Use the values that are specified in _BESClient_Comm _ProxyServer and _BESClient_Comm_ ProxyPort. **1** Use the Internet Explorer configuration settings. When the connection to the relay succeeds, the resulting proxy is locked in for subsequent communications and the values of proxy server and proxy port are saved in the registry under the key HKLM\Software\BigFix\EnterpriseClient\GlobalOptions as AutoProxyServer and AutoProxyPort. **Important:** Ensure that at least one user is logged in to the client to be able to get the Internet Explorer configuration settings.	Default Value: 1 Type: Boolean Value Range: 0-1 Mandatory: No
_BESClient_Comm _ProxyAutoDetectTryDirect	Specifies whether direct connections can be used when the system uses the proxy configuration settings that are specified for Internet Explorer. This setting is valid only if _BESClient_Comm _ProxyAutoDetect = 1. The following values are available: **0** Do not try direct connection. **1** Try direct connection if a proxy connection cannot be established. **2** Try direct connection first.	Default Value: 1 Type: Numeric Value Range: 0-2 Mandatory: No
AutoProxyRawProxyList	Specifies a blank space delimited list of proxies to try to connect to. **Note:** This setting is saved in the registry under the following key HKLM\Software\BigFix\EnterpriseClient\GlobalOptions.	Default Value: None Type: string Value Range: N/A Mandatory: No

Table 15. Proxy client additional configuration settings on Windows systems (continued)

Setting Name	Setting Value	Details
AutoProxyRawBypassList	Specifies a blank space delimited list of URLs to contact directly without passing through the proxy. You can use the "*" as a wildcard. **Note:** This setting is saved in the registry under the following key HKLM\Software\BigFix\EnterpriseClient\GlobalOptions.	Default Value: None Type: String Value Range: N/A Mandatory: No

6. 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 also upstream communication on the client with the following settings:

Table 16. Prerequisites to configure a proxy communication on a client

Setting	Description
_BESClient_Comm_CommandPollEnable = 1	Enables the client to poll its parent relay for new actions.
_BESClient_Comm_CommandPollIntervalSeconds = *nnn*	Determines how often the client checks with its parent relay to gather or refresh content if _BESClient_Comm_CommandPollEnable is enabled. To prevent performance degradation, avoid specifying settings that are less than 900 seconds. Value range is 0-4294967295.

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

   Important: If you skip this step, the relays cannot communicate with child nodes through the proxy.

7. Click **OK** to activate the settings.

For additional configuration settings that you can use to configure your environment, see Configuration Settings on the Wiki.

Best practices to consider when defining a proxy connection in V9.0 and V9.1

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 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 BFEnteprise 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 Diagnostic Tools to verify that the server, still reported as BESGatherService, can successfully reach the Internet.
- Check the GatherDB.log file that is in the BES Server\GatherDBData folder to verify that the server can gather from the Internet.
- Check in the firewall rules if any file types 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 did not expire.
- 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 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 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 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 version 9.0.835.0 for Windows and Linux systems. If you are using version 9.0 and you have problems using content that downloads files from the local server, upgrade to version 9.0.835.0 or later.
- On the server installed on a Linux system, at runtime the client configuration file is read before the server configuration file. Ensure that you update common settings on both components to avoid conflicts.
- 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_TimeoutSeconds. The _HTTPRequestSender_Connect_TimeoutSeconds setting affects all the , including the Console and the Client, running on the machine for which this setting is set. No other 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.

Chapter 13. Running backup and restore

You can schedule periodic backups (typically nightly) of the server and database files, to reduce the risk of losing productivity or data when a problem occurs by restoring the latest backup.

Consider, however, that when you run a disaster recovery, you restore a backup of an earlier working state of on the server computer or another computer. Depending on how old the backup is you can lose the latest changes or data.

Important: After restoring the data from the last backup, the server might restart at an earlier state with a disalignment between its mailbox and that of each relay. In this case the server needs to resynchronize with the relays that have continued to process requests, otherwise the relays might ignore the requests of the server. To realign the mailboxes, send some actions to the clients until the mailbox versions are the same.

You can also restore a single DSA server when an unrecoverable failure occurs.

Note: Do not restore the failed DSA server entirely from backup. Due to the complexity of DSA replication we recommend that you install a new server with the same FQDN and follow these procedures: DSA Recovey on Windows and DSA Recovey on Linux.

If all DSA servers are lost, follow the server restore procedure, Server Recovery Procedure on Windows and Server Recovery Procedure on Linux.

On Windows systems

If you back up the database and the Server files, when needed you can restore the environment on a Windows computer.

Server Backup

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 Server:
   - `[IEM Server folder]\UploadManagerData`.
   - `[IEM Server folder]\BESReportsData\<`*`rootserverhostname`*`>\masthead.afxm`.
   - `[IEM Server folder]\BESReportsServer\wwwroot\ReportFiles` -- Support files for custom Web Reports.
   - `[IEM Server folder]\Encryption Keys` -- Private encryption keys (if using Message Level Encryption).
   - `[IEM 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 Server, can be rebuilt automatically by the server if a failure occurs, back them up for faster recovery.
   - `[IEM Server folder]\Mirror Server\Inbox\bfemapfile.xml`. Information necessary for IBM Endpoint Manager Agents to get actions and Fixlets.

- `[IEM Server folder]\wwwrootbes\bfsites`. Information necessary for Agents to get actions and Fixlets.
- `[IEM Server folder]\wwwrootbes\bfmirror\bfsites`. Information necessary for Agents to get actions and Fixlets.
- `[IEM 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` and `license.crt` files are critical to the security and operation of . 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 server configuration. This file can be exported via the Masthead Management tab of the Administration tool.
5. Complete the following steps to decrypt the encrypted server signing key (`[IEM Server folder]\EncryptedServerSigningKey`):
   a. Copy the `EncryptedServerSigningKey` to a backup folder.
   b. Change directory to the backup folder and go to the following link ServerKeyTool.zip to download the ServerKeyTool.
   c. Run the following command to decrypt the server signing key:
   ```
   ServerKeyTool.exe decrypt UnencryptedServerSigningKey
   ```
   d. Securely back up the `UnencryptedServerSigningKey`.

Server Recovery

1. Using either the previous 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 server.
2. Ensure that the new 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`).

   Note: To avoid issues when the clients connect to the server before it is fully restored, ensure that the server is not available on the network until the recovery is complete.
3. Restore the BFEnterprise and BESReporting databases from backup.
4. Restore the backed up files and folders creating the directory structure.
5. Encrypt the `UnencryptedServerSigningKey` using the ServerKeyTool and copy the new encrypted file (`EncryptedServerSigningKey`) to `[IEM Server folder]\` folder.
6. Install the server components using the masthead file and specifying the same path used in the original installation option.
7. In a command window, change to the server directory and run `BESAdmin.exe /rotateServerSigningKey`.

Note: : If you have HTTPS enabled, ensure that you restore the server settings for Web Reports.

Verifying restore results

To ensure that your Server has been restored, perform the following steps:

1. Check the Diagnostics to verify that all services are started.
2. Log in to the console and verify that the logins work and that the database information was restored.
3. Ensure that the clients and 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.

   Note: If a remote datasource is defined in the Web Reports configuration, Web Reports connects to the datasource only after you re-enter the datasource credentials in the Web Reports **Administration > Datasource Settings > Edit** page.

DSA Recovery

When recovering a lost DSA server, all top-level relays (and therefore the entire deployment) should already be pointing to the remaining DSA server. It is recommended to leave all relays and clients reporting up to the working DSA server during this recovery procedure. If your existing relay settings do not allow this, isolate the server being restored on the network such that only the working DSA server can connect to it.

1. If the master DSA server fails, run the following procedure on the BFEnterprise SQL database to promote the secondary DSA server to master during restoration and replication of the failed server.

   ```
   declare @ServerID varchar(32)
   select @ServerID = convert(varchar(32),ServerID) from DBINFO
   execute [BFEnterprise].[dbo].[update_adminfields] 'Z:masterDatabaseServerID',@ServerID
   ```

   In this way you can install a new DSA server and you can run the Administration Tool on the secondary DSA server during the restoration of the failed server.
2. On the existing DSA server delete the failed DSA server id from the database.
   a. First see what the existing DSA server id is by executing the following SQL statement.

      ```
      select ServerID from DBINFO
      ```

   b. List the IDs of the DSA servers:

      ```
      select * from REPLICATION_SERVERS
      ```

   c. After identifying the failed server ID, run the following procedure:

      ```
      execute BFEnterprise.dbo.delete_replication_server <ID>
      ```

3. Restore the server operating system and database software in a pristine state without any server or the database remnants.
4. Restore the following items from backup:
   - `[IEM Server folder]\BESReportsServer\wwwroot\ReportFiles`

- [IEM Server folder]\Encryption Keys (can be optionally restored by copying from the secondary server, or a new key generated by the Administration Tool)
- [IEM Server folder]\UploadManagerData (optional, for faster recovery of SUA data if lost server was the SUA Source)
- [IEM Server folder]\wwwrootbes\bfmirror\downloads\ActionURLs
- [IEM Server folder]\wwwrootbes\bfmirror\downloads\sha1 (optional, for faster recovery of cached files)
- cert.pem file for Web Reports, if using HTTPS
- BESReporting database in SQL Server

5. Install server using the installer and the existing masthead. For additional information see "Installing Additional Windows Servers" on page 58.
6. Set the following registry values:

   For 32-bit Windows systems, go to [HKLM\Software\BigFix\Enterprise Server\FillDB] or for 64-bit Windows systems, go to [HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB] and then set the following values:

   ```
   "PerformanceDataPath"[REG_SZ] = "[IEM Server folder]\FillDB\FillDBperf.log"
   "UnInterruptibleReplicationSeconds"[DWORD] = 14400 (decimal)
   ReplicationDatabase=<DBName>
   ReplicationUser=<DBUser>
   ReplicationPassword=<DBPassword>
   ```
7. Restart the BES FillDB service.
8. Install client and console.
9. After replication completes, run the following procedure on in the SQL database to promote this newly restored server to be the master server.

   ```
   declare @ServerID varchar(32)
   select @ServerID = convert(varchar(32),ServerID) from DBINFO
   execute [BFEnterprise].[dbo].[update_adminfields] 'Z:masterDatabaseServerID',@ServerID
   ```
10. Reinstall and reconfigure the plugins. Configuration information can be gathered from the currently operating DSA server or from installation notes and configuration details kept by the Administrator.
11. Set the following registry values:

    For 32-bit Windows systems, go to [HKLM\Software\BigFix\Enterprise Server\FillDB] or for 64-bit Windows systems, go to [HKLM\Software\Wow6432Node\BigFix\Enterprise Server\FillDB] and then set the following values:

    ```
    "PerformanceDataPath"[REG_SZ] = ""
    "UnInterruptibleReplicationSeconds"[DWORD] = 120 (decimal)
    ```
12. Restart the BES FillDB service.
13. Launch the Administration Tool and update the replication interval on this restored server to the desired level. Typically, this value should match the interval set on the other DSA Server.

    Note: Depending on the size of the deployment, the replication process might take multiple days to complete. To validate its completion, look for a Replication Completed message in the FillDBperf.log file. Connecting a separate console to each DSA server and comparing contents is another way to check that the data is synchronized in both deployments.

On Linux systems

If you back up the database and the Server files, when needed you can restore the environment on a Linux computer.

Server Backup

To back up the Server, perform the following steps:

1. Stop all the processes, including running plug-ins if any, 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. 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
   ```

   These databases might have different names if, at installation time, one of these commands has been used: -opt BES_DB_NAME=<*SERVER_DB_NAME*> or -opt WR_DB_NAME=<*WEBREPORTS_DB_NAME*>.

3. Manually back up the following folders:

   ```
   /var/opt/BESClient
   /var/opt/BESServer
   /var/opt/BESWebReportsServer
   ```

4. Back up site credentials, license certificates and masthead files.

   The license.pvk and license.crt files are critical to the security and operation of . 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 server configuration. To back it up, either copy the /etc/opt/BESServer/actionsite.afxm file in a backup directory renaming it masthead.afxm, or open the masthead file from a browser, http://hostname:52311/masthead/masthead.afxm, and then save it to the backup directory.

Server Recovery

1. Remove all the installed components, including any plug-in.
2. Remove the following folders:

   ```
   /var/opt/BES*
   /var/log/BES*
   /etc/opt/BES*
   /opt/BES*
   /tmp/BES*
   ```

3. 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
```

4. Restore the previously saved folders and files:

   ```
   /var/opt/BESClient
   /var/opt/BESServer
   /var/opt/BESWebReportsServer
   ```

5. Download the same version and run the installation with option `-reuseDB`:

   ```
   ./install.sh -reuseDb
   ```

6. Install the server components using the masthead file and specifying the same path used in the original installation option.
7. Run the following command:

   ```
   ./BESAdmin.sh -rotateServerSigningKey
   ```

Verifying restore results

To ensure that your Server has been restored, perform the following steps:

1. Check the Diagnostics to verify that all services are started.
2. Log in to the console and verify that the logins work and that the database information was restored.
3. Ensure that the clients and 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.

   Note: If a remote datasource is defined in the Web Reports configuration, Web Reports connects to the datasource only after you re-enter the datasource credentials in the Web Reports **Administration > Datasource Settings > Edit** page.

DSA Recovery

When recovering a lost DSA server, all top-level relays (and therefore the entire deployment) should already be pointing to the remaining DSA server. It is recommended to leave all relays and clients reporting up to the working DSA server during this recovery procedure. If your existing relay settings do not allow this, isolate the server being restored on the network such that only the working DSA server can connect to it.

1. If the master DSA server fails, run the following procedure on the `BFEnterprise` SQL database to promote the secondary DSA server to master during restoration and replication of the failed server.

   ```
   db2
     set schema dbo
     select serverid from DBINFO (take count of SERVERID)
     set current function path dbo
     call update_adminFields('Z:masterDatabaseServerID','<serverid>') - Replace
   SERVERID with the value from the previous query
   ```

In this way you can install a new DSA server and you can run the Administration Tool on the secondary DSA server during the restoration of the failed server.

2. On the existing DSA server delete the failed DSA server id from the database.
   a. First see what the existing DSA server id is by executing the following SQL statement.
      ```
      select ServerID from DBINFO
      ```
   b. List the IDs of the DSA servers:
      ```
      select * from REPLICATION_SERVERS
      ```
   c. After identifying the failed server ID, run the following procedure:
      ```
      call dbo.delete_replication_server(ID)
      ```
3. Restore the server operating system and database software in a pristine state without any server or the database remnants.
4. Restore the following items from backup:
   - /var/opt/BESWebReportsServer/
   - [IEM Server folder]/Encryption Keys (can be optionally restored by copying from the secondary server, or a new key generated by the Administration Tool)
   - [IEM Server folder]/UploadManagerData (optional, for faster recovery of SUA data if lost server was the SUA Source)
   - [IEM Server folder]/wwwrootbes/bfmirror/downloads/ActionURLs
   - [IEM Server folder]/wwwrootbes/bfmirror/downloads/sha1 (optional, for faster recovery of cached files)
   - cert.pem file for Web Reports, if using HTTPS
   - BESReporting database in SQL Server
5. Install server using the installer and the existing masthead. For additional information see "Installing Additional Linux Servers (DSA)" on page 97.
6. Set the following keywords in the besserver.config file and restart the BES FillDB service:
   ```
   PerformanceDataPath = <Performance_Data_Path_filename>
   UnInterruptibleReplicationSeconds = 14400
   ReplicationDatabase=<DBName>
   ReplicationUser=<DBUser>
   ReplicationPassword=<DBPassword>
   ```

   where <Performance_Data_Path_filename> might be /var/opt/BESServer/FillDBData/FillDBPerf.log.
7. Restart the FillDB service:
   ```
   service besfilldb start
   ```
8. Install the client and console.
9. After replication completes, run the following procedure on in the SQL database to promote this newly restored server to be the master server.
   ```
   db2
     set schema dbo
     select serverid from DBINFO (take count of SERVERID)
     set current function path dbo
     call update_adminFields('Z:masterDatabaseServerID','<serverid>') - Replace
   SERVERID with the value from the previous query
   ```
10. Reinstall and reconfigure the Plugins. Configuration information can be gathered from the currently operating DSA server or from installation notes and configuration details kept by the Administrator.

11. Set the following keywords in the besserver.config file and restart the BES FillDB service:

```
PerformanceDataPath = ""
UnInterruptibleReplicationSeconds = 120
```

12. Launch the Administration Tool and update the replication interval on this restored server to the desired level. Typically, this value should match the interval set on the other DSA server.

    Note: Depending on the size of the deployment, the replication process might take multiple days to complete. To validate its completion, look for a Replication Completed message in the FillDBperf.log file. Connecting a separate console to each DSA server and comparing contents is another way to check that the data is synchronized in both deployments.

Chapter 14. Upgrading on Windows systems

Important: The Fixlet upgrade is not available in V9.1; you must upgrade the components manually.

Ensure you upgrade the server and all the 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 components (clients and relays) can work with the upgraded version of the server without problems. However, it is recommended that you upgrade the clients and relays whenever possible to take advantage of the new functions.

During the upgrade process, you might experience an increased network load on all the clients. This increase occurs because, during the upgrade to V9.1, all the content must be re-signed, therefore the content is gathered again from the external sites, signed again and then delivered to the subscribed clients. To avoid low performance during this process, ensure that all the relays defined in your network are up and running.

For upgrading a DSA environment see “Manual upgrade” on page 162.

Note: You can roll back to a previous version of only if you did not enable the enhanced security option after the upgrade completed. After you enable it in your environment, you cannot roll back to a previous version of even if you disable it.

Upgrade Paths to V9.1

The following tables describe the upgrade paths to V9.1:

- **Server upgrade**

Table 17. Server Upgrade

Upgrade from	Windows Upgrade
7.x	No
8.x	Yes
9.0	Yes

Note: If you are upgrading from a version previous to V9.0 and plan to enable the enhanced security feature, before enabling it run the following command for all the `FileOnlyCustomSite` created before the upgrade::

```
PropagateFiles.exe CreateFileOnlyCustomSiteUserAuthorization <masthead license pvk>
<masthead license pvk password> bes_bfenterprise bigfix <bigfix user password> FileOnlyCustomSi
```

- **Client upgrade**

Table 18. Client Upgrade

Upgrade from	Windows Upgrade	UNIX Upgrade	Mac Upgrade
7.x	Yes	Yes	Yes
8.x	Yes	Yes	Yes
9.0	Yes	Yes	Yes

Before upgrading

Perform these steps before upgrading the components:

1. Close all consoles.
2. Back up your server and database.
3. Upgrade SQL Databases. SQL 2000 database is no longer supported.
4. Back up your `license.pvk`,`license.crt`, and `masthead.afxm` to a separate location on the 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 the Configuration Guide..
6. Upgrade the 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.

   Note: Existing V9.1 proxy configurations are automatically migrated to the V9.2 proxy configuration settings and behavior. For more information about V9.2 proxy configuration settings, see Chapter 12, “Setting up a proxy connection,” on page 141.
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 Administration Tool to update the data with SHA-2 signature, to update a remote database and to set the NIST security standards, if needed.

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 server to process this backlog after the upgrade has completed.

Manual upgrade

Use the manual upgrade instead of the Fixlet upgrade when you upgrade a DSA multiple server environment or an server which uses a remote database.

Note: During the upgrade of a DSA server, ensure that no services are running on all the other DSA servers to prevent the upgrading system from becoming unstable when a replication process starts against it.

Upgrading the Installation Generator

1. From the computer where you installed the Installation Generator, download and run the new 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.

Upgrading the Server

1. Copy the Server installation folder (default location is `C:\Program Files\BigFix Enterprise\BES Installers\Server`) to the Server computer.
2. Run the Server installer (`setup.exe`) on the 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.
4. Run the Administration Tool `BESAdmin.exe` to distribute the updated license.
5. 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 Console installation folder (default location is `C:\Program Files\BigFix Enterprise\BES Installers\Console`) to all computers that are running the Console.
2. Run the Console installer (`setup.exe`) on all the computers currently running the Console.

Upgrading the relays

relays can be upgraded from the console by applying the **Updated Windows Relay** Fixlet to all relevant relays.

Upgrading the Clients

- Clients can be upgraded individually by copying the Client installation folder (default location is `C:\Program Files\BigFix Enterprise\BES Installers\Client`) to each computer that is running the Client, and then running `setup.exe`.
- 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 Client installer on the computer that has the old Client.

Upgrading the Web Reports

To upgrade stand-alone Web Reports, run `BigFix-BES-Server-9.1.`*`xxx`*`.`*`x`*`.exe`, which detects Web Reports installation and offers to upgrade it for you.

If Web Reports is installed on the server, it is upgraded along with the server.

Note: If you have a remote database, run the upgrade as a user with DBO permissions to the database.

Server Recovery

1. Using either the previous 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 server.
2. Ensure that the new 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`).

   Note: To avoid issues when the clients connect to the server before it is fully restored, ensure that the server is not available on the network until the recovery is complete.
3. Restore the BFEnterprise and BESReporting databases from backup.
4. Restore the backed up files and folders creating the directory structure.
5. Encrypt the `UnencryptedServerSigningKey` using the ServerKeyTool and copy the new encrypted file (`EncryptedServerSigningKey`) to `[IEM Server folder]\` folder.
6. Install the server components using the masthead file and specifying the same path used in the original installation option.
7. In a command window, change to the server directory and run `BESAdmin.exe /rotateServerSigningKey`.

Note: : If you have HTTPS enabled, ensure that you restore the server settings for Web Reports.

Chapter 15. Upgrading on Linux systems

Important: The Fixlet upgrade is not available in V9.1; you must upgrade the components manually.

Ensure you upgrade the server and all the 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 components (clients and relays) can work with the upgraded version of the server without problems. However, it is recommended that you upgrade the clients and relays whenever possible to take advantage of the new functions.

During the upgrade process, you might experience an increased network load on all the clients. This increase occurs because, during the upgrade to V9.1, all the content must be re-signed, therefore the content is gathered again from the external sites, signed again and then delivered to the subscribed clients. To avoid low performance during this process, ensure that all the relays defined in your network are up and running.

For upgrading a DSA environment see "Manual upgrade" on page 166.

Note: You can roll back to a previous version of only if you did not enable the enhanced security option after the upgrade completed. After you enable it in your environment, you cannot roll back to a previous version of even if you disable it.

Upgrade paths to V9.1

The following tables show the upgrade paths to V9.1:

- **Server upgrade**

Table 19. Server Upgrade

Upgrade from	UNIX Upgrade
7.x	No
8.x	No
9.0	Yes

- **Client upgrade**

Table 20. Client Upgrade

Upgrade from	Windows Upgrade	UNIX Upgrade	Mac Upgrade
7.x	Yes	Yes	Yes
8.x	Yes	Yes	Yes
9.0	Yes	Yes	Yes

Before upgrading

Perform these steps before upgrading the components:

1. Close all consoles.
2. Back up your server and database.
3. Back up your `license.pvk`, `license.crt`, and `masthead.afxm` to a separate location on the server or to a USB key.
4. 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 the Configuration Guide..
5. Upgrade the components according to the following order:
   a. Servers and consoles (console and server must have the same version 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 functions of the new release.

   Note: Existing V9.1 proxy configurations are automatically migrated to the V9.2 proxy configuration settings and behavior. For more information about V9.2 proxy configuration settings, see Chapter 12, “Setting up a proxy connection,” on page 141.
6. 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 server to process this backlog after the upgrade has completed.

Manual upgrade

Use the manual upgrade instead of the Fixlet upgrade when you upgrade a DSA multiple server environment.

Note: During the upgrade of a DSA server, ensure that no services are running on all the other DSA servers to prevent the upgrading system from becoming unstable when a replication process starts against it.

Upgrading the server

1. Copy the IBM Endpoint Manager server installable image to the server computer and extract it to a folder.
2. On the server computer run the server upgrade script:

```
./install.sh -upgrade [-opt BES_LICENSE_PVK=<path+license.pvk>]
            [-opt BES_LICENSE_PVK_PWD=<password>]
```

   where:

-opt BES_LICENSE_PVK=<path+license.pvk>
Specifies the private key file (*filename*.pvk). This private key file and its password are required to update the product license and perform the required SHA-256 signature updates in the database.

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

-opt BES_LICENSE_PVK_PWD=<password>
Specifies the password associated to the private key file (*filename*.pvk).

The `install.sh` server script upgrades all the components it detects on the local server.

3. Run the Administration Tool (`./BESAdmin.sh` on Linux) to distribute the updated license:

```
/opt/BESServer/bin/BESAdmin.sh -syncmastheadandlicense -sitePvkLocation=<path+license.pvk>
                    -sitePvkPassword=<password>
```

Note: For troubleshooting information see `/var/log/BESInstall.log` and `/var/log/BESAdminDebugOut.txt` files.

Upgrading the console

1. Copy the console installation folder (default is: `/var/opt/BESInstallers/Console`) to all Windows computers that are running the console.
2. Run the console installer (`setup.exe`) on all the Windows computers currently running the console.

   Note: The console does not run on Linux computers.

Upgrading the relays

relays can be upgraded from the console by applying the **Updated Red Hat Enterprise Linux Relay** Fixlet to all relevant relays.

Upgrading the Clients

- clients can be upgraded individually by copying the client installable image to each computer that is running the client, and then running the setup program.
- clients can also be upgraded by using the Client Deployment Tool, with a log in script, or with another deployment technology. Simply run the new Client installer on the computer with the old client.

Upgrading the Web Reports

To upgrade a stand-alone Web Reports server, run the `install.sh` server upgrade script:

```
./install.sh -upgrade
```

Server Recovery

1. Remove all the installed components, including any plug-in.
2. Remove the following folders:

```
/var/opt/BES*
/var/log/BES*
/etc/opt/BES*
/opt/BES*
/tmp/BES*
```

3. 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
   ```

4. Restore the previously saved folders and files:

   ```
   /var/opt/BESClient
   /var/opt/BESServer
   /var/opt/BESWebReportsServer
   ```

5. Download the same version and run the installation with option `-reuseDB`:

   ```
   ./install.sh -reuseDb
   ```

6. Install the server components using the masthead file and specifying the same path used in the original installation option.
7. Run the following command:

   ```
   ./BESAdmin.sh -rotateServerSigningKey
   ```

Appendix A. Component Log Files

These are the log files of the components:

Server Audit log: The server keeps an audit log and traces the following types of audit events:

```
AuditStream() << "approver \"" << checkResult.user
<< "\" approved an activity performed by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " was made a reader for custom site \""
<< parameters.siteName.GetString() << "\"" << "by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " was removed as a reader from custom site \""
<< parameters.siteName.GetString() << "\"" << "by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " was made a writer for custom site \""
<< parameters.siteName.GetString() << "\"" << "by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " was removed as a writer from custom site \""
<< parameters.siteName.GetString() << "\"" << "by " << "user "{name}" ({id})";
AuditStream() << "role "{name}"" << " was created by " << "user "{name}" ({id})";
AuditStream() << "role "{name}"" << " was deleted by " << "user "{name}" ({id})";
AuditStream() << "role "{name}"" << " has been given " << ( it->second
== UserRoleSitePrivileges::SiteWriter ? "write" : it->second == UserRoleSitePrivileges:
:SiteReader ? "read" : "ownership" ) << " privileges on " << SiteAuditText( it->first )
<< " by " << UserAuditText( user );
AuditStream() << "user "{name}" ({id})" << " has been added to " << "role "{name}"" <<
" by " << "user "{name}" ({id})";
AuditStream() << "ldap group "{name}" (DN={dn})" << " has been added to " << "role
"{name}"";
AuditStream() << "site {site}" << " removed from " << "role "{name}"" << " by " <<
"user "{name}" ({id})";
AuditStream() << "site {site}" << " added to " << "role "{name}"" << " by " << "user
"{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " added to " << "role "{name}"" << " by " <<
"user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " removed from " << "role "{name}"" <<

" by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " was assigned to " << "role "{name}"" <<
" by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " was removed from " << "role "{name}"" <<
" by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " privileges updated by " << "user "{name}
" ({id})" << ": "
<< PrivilegesAuditText( iface.db, userInfo, isMasterOperator, canCreateCustomContent,
showOtherUsersActions, unmanagedAssetPrivilege, loginPermission, approverRoleID );
AuditStream() << "ldap user \"{name}\" (DN={dn})" << " created by " << "user "{name}"
({id})";
AuditStream() << "user "{name}" ({id})" << " password changed by " << "user "{name}"
({id})";
AuditStream() << "user "{name}" ({id})" << " changed their own password";
AuditStream() << "user "{name}" ({id})" << " was removed by " << "user "{name}" ({id})";
AuditStream() << "user "{name}" ({id})" << " management rights updated by " << "user
"{name}" ({id})";
AuditStream() << oldUserAuditText << " converted to ldap user " << "ldap user \"{name}\
" (DN={dn})" << " by " << initiator;
AuditStream() << "role "{name}"" << " was modified by " << "user "{name}" ({id})" <<
": " << PrivilegesAuditText( iface.db, role.UserRolePrivileges() );
AuditStream() << "user "{name}" ({id})" << " created by " << "user "{name}" ({id})
" << ": "
AuditStream() << "ldap user \"{name}\" (DN={dn})" << " created based on membership
of role(s): " << roleNames.Ref();
```

These are the default locations of the audit logs for each operating system:

- Windows: `%PROGRAM FILES%\BigFix Enterprise\BES Server\server_audit.log`
- Linux: `/var/opt/BESServer/server_audit.log`

BES Root Server log:

- Windows: `C:\Program Files (x86)\BigFix Enterprise\BES Server\BESRelay.log`
- Linux: `/var/log/BESRelay.log`

Gather log: Only for Windows operating systems `http://127.0.0.1:52311/cgi-bin/bfenterprise/BESGatherMirrorNew.exe`

FillDB log:

- Windows: `C:\Program Files (x86)\BigFix Enterprise\BES Server\FillDBData\FillDB.log`
- Linux: `/var/opt/BESServer/FillDBData/FillDB.log`

GatherDB log:

- Windows: `C:\Program Files (x86)\BigFix Enterprise\BES Server\GatherDBData\GatherDB.log`
- Linux: `/var/opt/BESServer/GatherDBData/GatherDB.log`

Relay log:

- Windows: `C:\Program Files (x86)\BigFix Enterprise\BES Relay\logfile.txt`
- Linux: `/var/log/BESRelay.log`

Client log: The client records its current activity into a log file with the current date as the file name in the format `[year][month][day].log`. If an active log reaches 512K in size it will be moved to a backup (.bkg) file and a new log will be started for the current day. If the log reaches 512K again the backup will overwrite the existing backup. Both the active and backup logs will be deleted after ten days. These are the default locations of the client logs for each operating system:

- Windows clients: `C:\Program Files\BigFix Enterprise\BES Client\__BESData\__Global\Logs`
- UNIX, Linux clients: `/var/opt/BESClient/__BESData/__Global/Logs`
- Mac clients: `/Library/Application Support/Bigfix/BES Agent/__BESData/__Global/Logs`

The directory of the **BES Server Plugin Service log** is `C:\Program Files\BigFix Enterprise\BES Server\Applications\Logs`.

Appendix B. 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 .

Client Software installed on each networked computer to be managed under the . 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 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 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 system.

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

Installation Generator
An application that creates installers for the core 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 process, including URLs that point to where trusted Fixlet content is available. The Client brings content into the enterprise based on subscribed mastheads.

Mirror server
A server required in the 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 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 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 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 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 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 Server, or simply Server.

Signing password
The password (specified when the 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 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 system to satisfy more than the basic reporting and data storage needs. A step up from SQLite

Standard deployment
A deployment of the 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 Server where the Server software and related files (including Console and Client installers) will be installed.

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

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 C. **** MISSING FILE ****

This file was generated during the publishing process

**** MISSING FILE ****

This file was generated during the publishing process

Printed in USA