IBM Endpoint Manager
Version 9.1

Configuration Guide

IBM

IBM Endpoint Manager
Version 9.1

Configuration Guide

Note

Before using this information and the product it supports, read the information in "Notices" on page 77.

This edition applies to version 9, release 1, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Introduction

This guide explains additional configuration steps that you can run in your environment after installation.

In this guide you find information about:

- Chapter 2, "Additional configuration steps," on page 5
- Chapter 3, "Maintenance and Troubleshooting," on page 55
- Chapter 4, "Upload and archive manager settings," on page 57
- Chapter 5, "Command-Line Interface," on page 65

What is new in V9.1

IBM Endpoint Manager 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 Security Configuration Scenarios.

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 for Windows systems or in Running the Endpoint Manager Administration Tool for Linux systems.
- Inactivity timeout for Console and Web Reports.

  To configure the inactivity timeout, specify the option **timeoutLockMinutes** as described in Advanced Options for Windows systems or in Running the Endpoint Manager Administration Tool 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 IBM Endpoint Manager terms, but are used throughout the guide without being labeled every time with IBM Endpoint Manager:

Agent means a computer where the IBM Endpoint Manager client is installed

Console
means IBM Endpoint Manager console

Client means IBM Endpoint Manager client

Server means IBM Endpoint Manager server

Relay means IBM Endpoint Manager relay

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might see which components labeled with "BigFix" or "BigFix Enterprise Suite" (BES), which is legacy terminology, now superseded by "IBM Endpoint Manager."

Chapter 2. Additional configuration steps

These topics explain additional configuration steps that you can run in your environment.

Managing operators and permissions

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

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

Master Operators
Have access to all IBM Endpoint Manager computers and the authority to create and manage the other console operators. Any master operator can create, distribute, and revoke publisher keys and management rights that allow console operators to deploy actions. For more information, see "Operators permissions" on page 6.

Operators
Manage the day-to-day operations of IBM Endpoint Manager, including Fixlet management and action deployment, typically on a subset of computers subject to the management rights assigned by the master operator. For more information, see "Operators permissions" on page 6.

Often these administrative roles overlap and one person might be assigned multiple tasks. The network and database tasks are limited to minimal setup procedures, which are described in this document.

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

Site administrator responsibilities

The site administrator has the following primary responsibilities:

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

- Setting global system options
- Editing Mastheads
- Administering Distributed Server Architecture (DSA)

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

Preparing the Server

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

Installing the various components

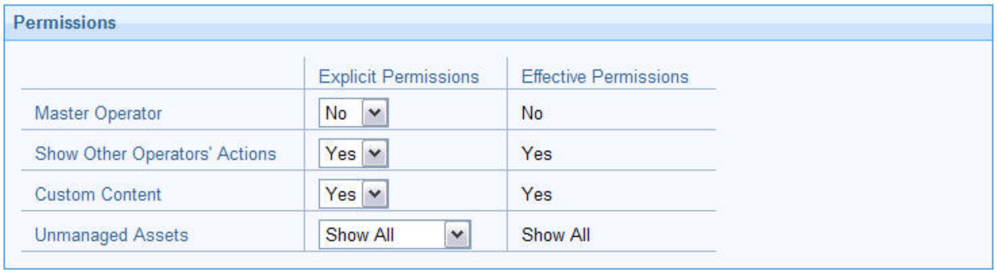
The site administrator installs the IBM Endpoint Manager Client, Server, Relay, and Console modules.

Maintaining the Server

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

Operators permissions

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



Permissions

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

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

Table 1. Master operator and operator authorizations

Activities	Master Operator	Operator
Initialize Action Site	Yes	No
Manage Fixlet Sites	Yes	No
Change Client heartbeats	Yes	No
Create Fixlets	If Custom Content is set to YES	If Custom Content is set to YES
Create Tasks	If Custom Content is set to YES	If Custom Content is set to YES
Create Analyses	If Custom Content is set to YES	If Custom Content is set to YES
Create Baselines	If Custom Content is set to YES	If Custom Content is set to YES
Create Groups	Yes	Manual Groups Only
Activate/Deactivate Analyses	All	Administered
Take Fixlet/Task/Baseline Action	All	Administered

Table 1. Master operator and operator authorizations (continued)

Activities	**Master Operator**	**Operator**
Take Custom Action	If Custom Content is set to YES	If Custom Content is set to YES
Stop/Start Actions	All	Administered
Manage Administrative Rights	Yes	No
Manage Global Retrieved Properties	Yes	No
View Fixlets	All	Administered
View Tasks	All	Administered
View Analyses	All	Administered
View Computers	All	Administered
View Baselines	All	Administered
View Computer Groups	All	Administered
View Unmanaged Assets	Administered	Administered
View Actions	All	Administered
Make Comments	All	Administered
View Comments	All	Administered
Globally Hide/Unhide	Yes	No
Locally Hide/Unhide	Yes	Yes
Use Wizards	If Custom Content is set to YES	If Custom Content is set to YES
Remove computer from database	All	Administered
Create Manual Computer Groups	Yes	Yes
Delete Manual Computer Groups	Yes	No
Create Automatic Computer Groups	Yes	If Custom Content is set to YES
Delete Automatic Computer Groups	Yes	If Custom Content is set to YES and Administered
Create Custom Site	Yes	No
Modify Custom Site Owners	Yes	No
Modify Custom Site Readers/Writers	Yes	Site Owners
Administered: The operator must own or have permissions. **Requires Custom Authoring**: Granted by the site administrator through the console.		

Operators and analyses

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

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

Adding console operators

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

These are the types of operators that can be created:

- Local operator (local IBM Endpoint Manager account). For information about how to add local operators, see the *IBM Endpoint Manager Console Operator's guide*.
- LDAP operator (operator whose credentials are authenticated via Active Directory or LDAP). For information about how to add LDAP operators, see the *IBM Endpoint Manager Console Operator's guide*.
- LDAP Group to a role. For information about how to assign a LDAP group to an existing role, see the *IBM Endpoint Manager Console Operator's guide*.

Note: For LDAP operator and LDAP Group, you must first add an Active Directory or LDAP domain to IBM Endpoint Manager.
For information about additional operations that can be run against operators, see the *IBM Endpoint Manager Console Operator's guide*.

Integrating Linux Server with Active Directory

To ensure a secure communication between Linux Endpoint Manager server and Active Directory, use the Kerberos protocol.

This protocol is available in the Linux Endpoint Manager server package because it is a prerequisite of the Endpoint Manager server installation.

To integrate the Linux Endpoint Manager server with the Windows Active Directory domain using LDAP with Kerberos authentication, perform the following steps:

1. Ensure that the host names and the time service are set correctly in both the Linux Endpoint Manager server and the Active Directory server
2. Install the NSS and PAM libraries
3. Configure the Kerberos LDAP security and authentication
4. Modify the local LDAP name
5. Configure the NSS and PAM libraries

Preliminary Checks

Before running the integration between the Endpoint Manager server running on a Red Hat Enterprise Linux 6 or Linux 7 system and the Active Directory server, ensure that:

- The DNS host names of both the Red Hat Enterprise Linux 6 or Linux 7 system and the Active Directory server are resolved correctly, by performing the following steps on the Red Hat Enterprise Linux 6 system:
  1. Open the file `/etc/host` and ensure that both DNS host names are specified as fully qualified domain names.

2. Open the file /etc/sysconfig/network and ensure that the host name of the Red Hat Enterprise Linux 6 or Linux 7 system is specified as fully qualified domain name.

- The time between the Active Directory and the Linux Endpoint Manager server is synchronized. If needed, you can synchronize the time service on the Red Hat Enterprise Linux 6 or Linux 7 system and the Active Directory server with the time source server, by performing the following steps:
  1. In the file /etc/ntp.conf on the Red Hat Enterprise Linux 6 or Linux 7 system, replace the following lines:
     ```
     server hostname
     ```
     with:
     ```
     server time_source_server_name
     ```
     where *time_source_server_name* is the server hostname or IP address of the time source server used to synchronize the time.
  2. When DNS lookups are not reliable, configure the Red Hat Enterprise Linux systems to perform DNS lookups from the Active Directory server by editing the /etc/resolv.conf file as follows:
     ```
     domain my.domain.com
     search my.domain.com
     nameserver1 ipaddress1
     nameserver2 ipaddress2
     ```
  3. Activate the change on the Red Hat Enterprise Linux 6 or Linux 7 system by:
     - Stopping the **ntp** daemon:
       ```
       service ntpd stop
       ```
     - Updating the time:
       ```
       ntpdate Red_Hat_server_IP
       ```
     - Starting the **ntp** daemon:
       ```
       service ntpd start
       ```
  4. Synchronize the Active Directory server with the time source server by entering:
     ```
     w32tm /config /manualpeerlist:"time_source_server_name"
           /syncfromflags:manual /update
     ```
     where *time_source_server_name* specifies the list of DNS names or IP addresses for the NTP time source with which the Linux server synchronizes. For example, you can specify time.windows.com as the NTP time server. When you specify multiple peers, use a space as the delimiter and enclose the names of the peers in quotation marks.
  5. On the Active Directory server, run the following command to ensure that the time is synchronized with the time source server
     ```
      w32tm /query /status | find "Source"
      w32tm /query /status | find "source"
     ```
  6. On the Red Hat Enterprise Linux 6 system configure the **ntpd** daemon to start at system boot:
     ```
     chkconfig ntpd on
     ```

Installing the NSS and PAM libraries

Ensure that the following NSS and PAM packages are installed:

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

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

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

Configuring Authentication

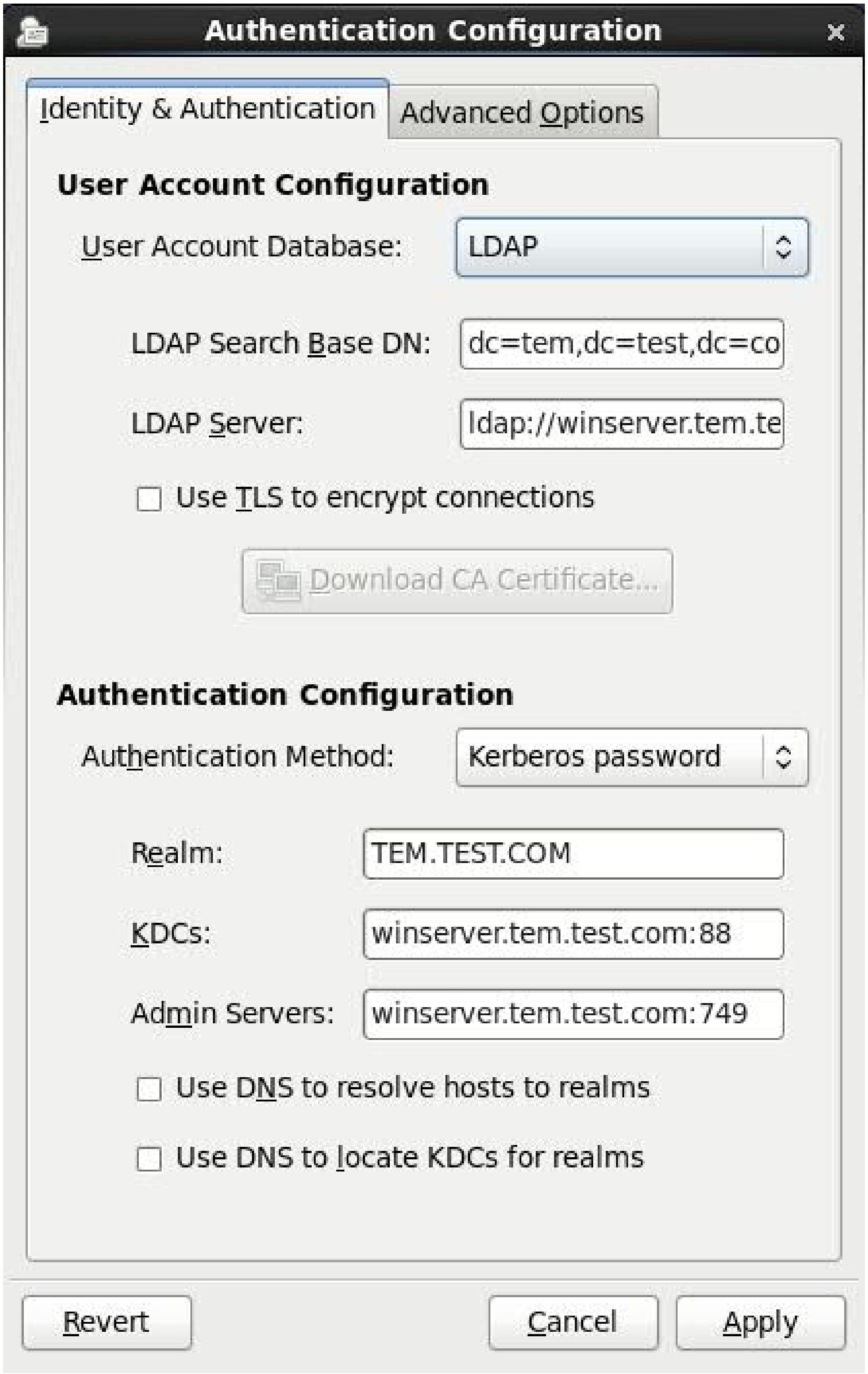
To configure the Kerberos protocol, the LDAP security and the authentication files for Active Directory integration, you can use one of the following methods:

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

Using the system-config-authentication graphical tool:

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

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



Authentication Configuration
Identity & Authentication
Advanced Options
Download CA Certificate...
Revert
Cancel
Apply

User Account Configuration

User Account Database: LDAP

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

LDAP Server: ldap://winserver.tem.te

□ Use TLS to encrypt connections

Authentication Configuration

Authentication Method: Kerberos password

Realm: TEM.TEST.COM

KDCs: winserver.tem.test.com:88

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

□ Use DNS to resolve hosts to realms

□ Use DNS to locate KDCs for realms

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

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

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

Using the authconfig command-line tool:

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

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

where:

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

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

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

--enablekrb5
Enables the Kerberos password authentication method.

--krb5realm
Configures the realm for the Kerberos server, such as `TEM.TEST.COM`. Ensure you specify the realm name in uppercase.

--krb5kdc
Specifies the *Key Distribution Center* (KDC) for issuing Kerberos tickets, such as `winserver.tem.test.com`.

--krb5adminserver
Specifies the administration servers running `kadmind`, such as `winserver.tem.test.com`.

--update
Applies all the configuration settings.

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

Modifying the local LDAP name

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

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

```
cp -p /etc/nslcd.conf /etc/nslcd.conf.bk
```

2. Modify the value of the base and uri settings in the /etc/nslcd.conf file as in the following example:

```
base dc=tem,dc=test,dc=com
uri ldap://winserver.tem.test.com
```

3. Restart the local LDAP name service daemon:

```
service nslcd restart
```

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

```
 chkconfig nslcd on
```

Configuring the NSS and PAM libraries

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

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

to LDAP (**ldap**):

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

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

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

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

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

Using multiple servers (DSA)

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

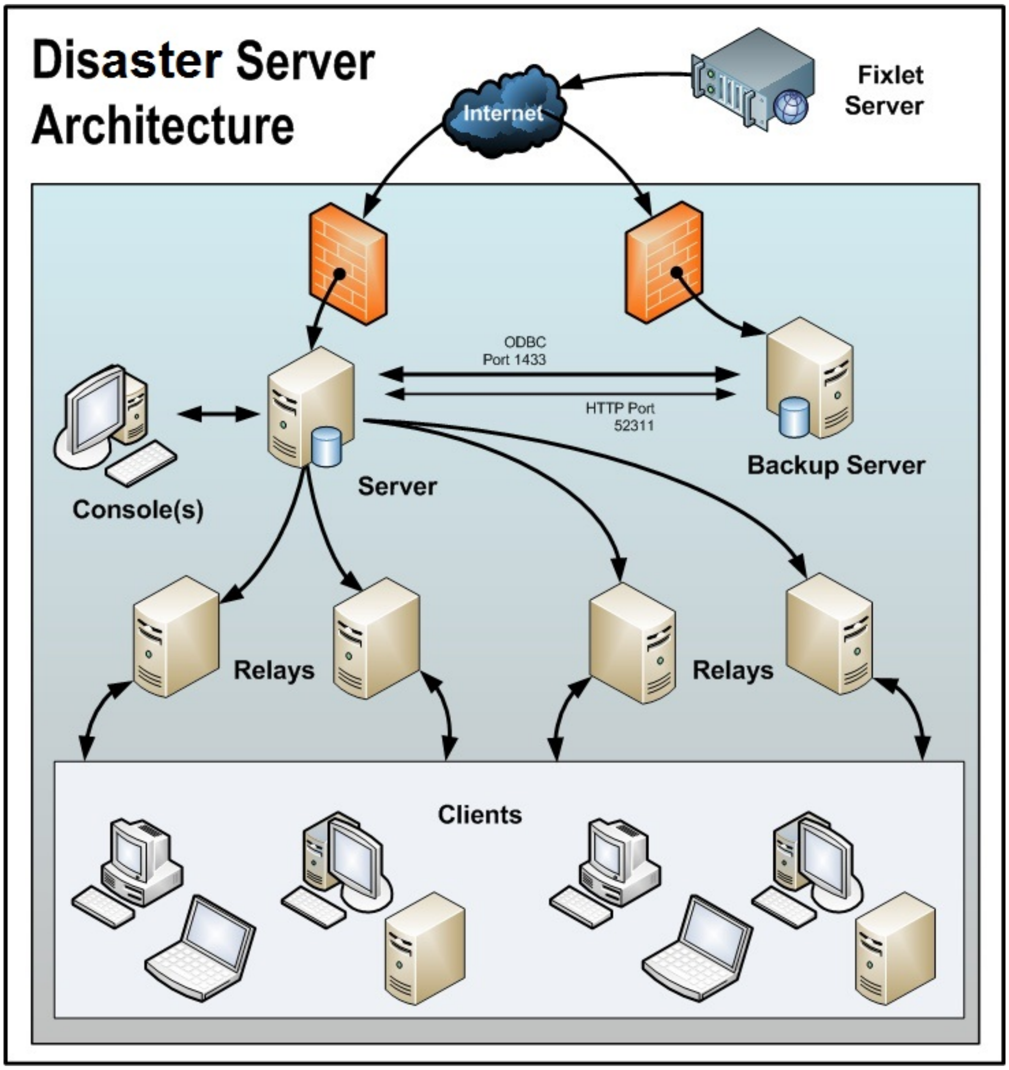
- Servers communicate on a regular schedule to replicate their data. You review the current status and adjust the replication interval through **IBM Endpoint Manager Administration Tool > Replication**.
- When each server is ready to replicate from the other servers in the deployment, it calculates the shortest path to every other server in the deployment. Primary links are assigned a length of 1, secondary links 100, and tertiary links 10,000. Links that resulted in a connection failure the last time they were used are considered to be non-connected.

- When an outage or other problem causes a network split, it is possible for a custom Fixlet or a retrieved property to be modified independently on both sides of the split. When the network is reconnected, precedence goes to the version on the server with the lowest Server ID.
- If multiple copies of **Web Reports** are installed, they operate independently. Each Web Report server can connect to the server that is most convenient, because they all contain equivalent views of the database.
- By default, server 0 (zero) is the master server. The **IBM Endpoint Manager Administration Tool** only allows you to perform certain administrative tasks (such as creating and deleting users) when connected to the master server.
- Depending on the platform where you installed the server, you can switch the master to another server as it is explained in "Managing Replication (DSA) on Windows systems" on page 17 or "Managing Replication (DSA) on Linux systems" on page 17.

Disaster Server Architecture (DSA)

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

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" on page 15.

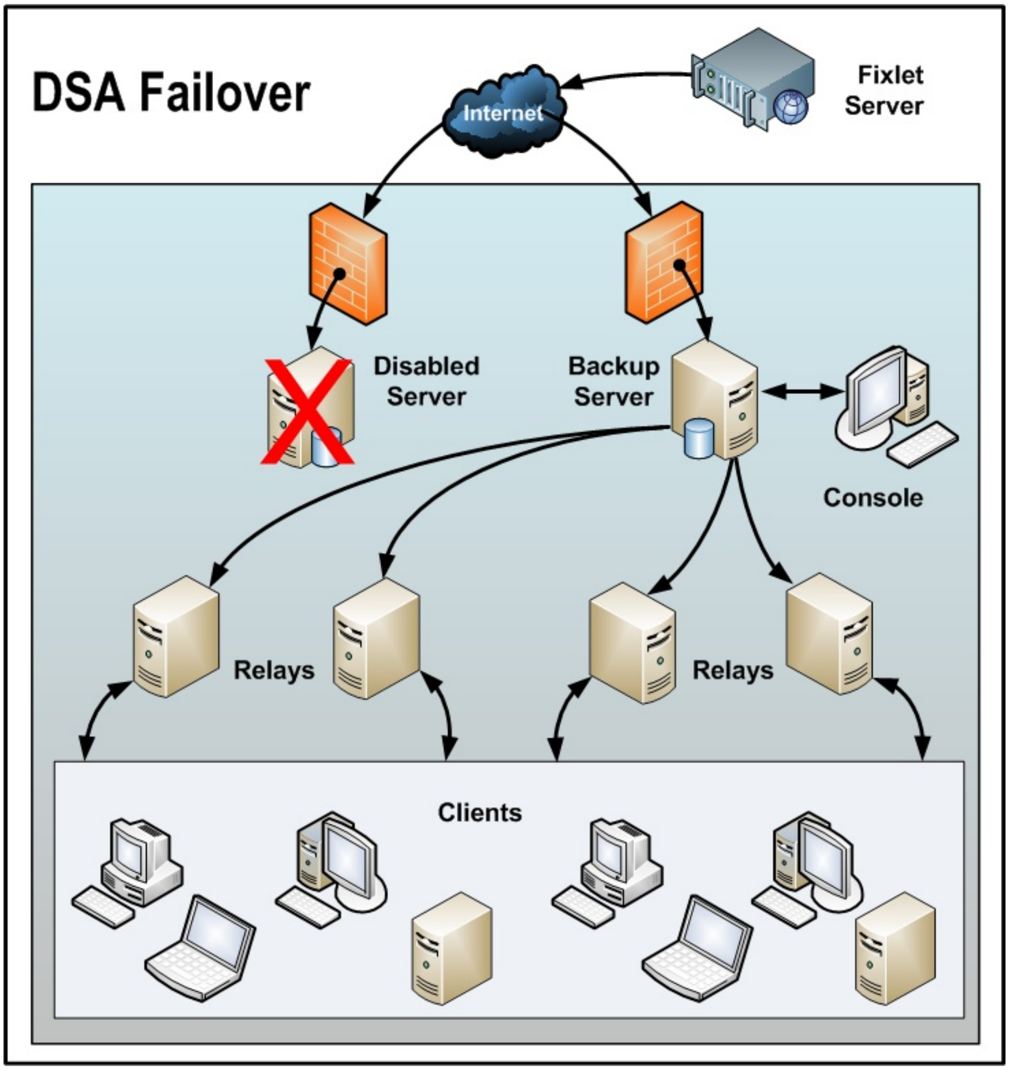


Configuring relay failover

If an Endpoint Manager server goes down, whether due to disaster or planned maintenance, the DSA server might be used to find a new server connection. When the disabled server comes back online, its data will automatically be merged with the data on the healthy server.

In order for the failover process to successfully occur set the DSA server as the secondary relay in client settings using `__RelayServer2` for the top-level relays (or via the console Computer right-click settings user interface). When a failure on the primary IBM Endpoint Manager server occurs and lower level IBM Endpoint Manager relays are unable to report, they use the secondary IBM Endpoint Manager relay value during normal relay selection process to find and report to the secondary IBM Endpoint Manager server.

Note: The setting `_BESClient_RelaySelect_ResistFailureIntervalSeconds` specified on the client system can have an impact on failover timing. Its value can range from 0 seconds to 6 hours and it defines how many seconds the client ignores reporting failures before attempting to find another parent relay. The default value is 10 minutes. In case of a failover configuration, ensure that, if defined, `_BESClient_RelaySelect_ResistFailureIntervalSeconds` is set to a low value.



Message Level Encryption and DSA

If Message Level Encryption is enabled and clients are set using **Task: BES Client Setting: Encrypted Reports**, move the Endpoint Manager server encryption key to the secondary Endpoint Manager DSA server. This enables the Endpoint Manager DSA server to process reports from encrypted Endpoint Manager clients during normal operations or in the event of an outage on the primary Endpoint Manager server.

Copy the encryption key (`.pvk`) from the Endpoint Manager server directory:

- Windows 32-bit server: `C:\Program Files\BigFix Enterprise\BES Server\Encryption Keys\`
- Windows 64-bit server: `C:\Program Files (x86)\BigFix Enterprise\BES Server\Encryption Keys\`
- Linux server: `/var/opt/BESServer/Encryption Keys`

to the DSA secondary server.

Managing Replication (DSA) on Windows systems

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

Changing the replication interval on Windows systems

On Windows systems if you have multiple servers in your deployment, you can schedule when each one replicates. The default is five minutes, but you can shorten the time for greater recoverability or increase it to limit network activity:

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

Switching the master server on Windows systems

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

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

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

Managing Replication (DSA) on Linux systems

Replication servers are simple to set up and require minimal maintenance. You might want to change the interval or allocate your servers differently. Most of these changes are done through the `iem` command line. Here you can see the current settings for your servers and make the appropriate changes.

Changing the replication interval on Linux systems

On Linux systems if you have multiple servers in your deployment, you can schedule when each one replicates. The default is five minutes, but you can shorten the time for greater recoverability or increase it to limit network activity:

To change the replication interval, perform the following steps:

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

   ```
   ./iem login --server=servername:serverport --user=username
   --password=password
   ```

2. From the `/opt/BESServer/bin` command prompt, run the following command:

   ```
   ./iem get replication/server/0 > /appo/replicationServer0.xml
   ```

3. In the `/appo/replicationServer0.xml` file, edit the following keyword:

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

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

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                               xsi:noNamespaceSchemaLocation="BESAPI.xsd">
      <ReplicationServer Resource="http://9.87.126.68:52311/api/replication
                                                               /server/0">
              <ServerID>0</ServerID>
              <URL>http://nc926068.romelab.it.ibm.com:52311</URL>
              <DNS>nc926068.romelab.it.ibm.com</DNS>
         <ReplicationIntervalSeconds>300</ReplicationIntervalSeconds>
         <ReplicationLink Resource="http://9.87.126.68:52311/api/replication
          /server/0/link/3">
                 <SourceServerID>0</SourceServerID>
                 <DestinationServerID>3</DestinationServerID>
                 <Weight>1</Weight>
                 <IsConnected>0</IsConnected>
                 <LastReplication>Fri, 01 Mar 2013 11:17:12 +0000
                 </LastReplication>
                 <LastError>19NoMatchingRecipient - Fri, 01 Mar 2013 11:17:12 +0000
                 </LastError>
         </ReplicationLink>
         <ReplicationLink Resource="http://9.87.126.68:52311/api/replication/server/
                                             3/link/0">
                      <SourceServerID>3</SourceServerID>
                      <DestinationServerID>0</DestinationServerID>
                      <Weight>1</Weight>
                      <IsConnected>1</IsConnected>
                      <LastReplication>Fri, 01 Mar 2013 11:17:18 +0000
                      </LastReplication>
         </ReplicationLink>
      </ReplicationServer>
   </BESAPI>
   ```

4. Upload the modified file by running the following command:

   ```
   ./iem post /appo/replicationServer0.xml  replication/server/0
   ```

Switching the master server on Linux systems

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

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

   ```
   ./iem login --server=servername:serverport --user=username --password=password
   ```

2. From the /opt/BESServer/bin command prompt, run the following command:

   ```
   ./iem get admin/fields > /appo/switchmaster.xml
   ```

3. In the /appo/switchmaster.xml file, add or edit the following keyword and its value:

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

   to switch the master server to another master server:

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

4. Upload the modified file by running the following command:

   ```
   ./iem post /appo/switchmaster.xml admin/fields
   ```

After the value has successfully replicated to the new server, it become the master server. If a server suffers a failure while it is the master, another server must be made the master server by direct manipulation of the ADMINFIELDS table in the database.

Configuring ODBC

This topic describes how to use Open DataBase Connectivity (ODBC) to set up and configure ODBC Data Sources with Endpoint Manager. Each ODBC Data Source is identified by an ODBC Data Source Name (DSN), like bes_bfenterprise used to access data in a variety of DBMS such as Microsoft SQL or IBM DB2 in an easier way. DSNs are stored locally on the computer used to reach the database. Each DSN is used to save authentication and setting information for a database connection. In this way users can connect with a database once and save the information for future use.

To access a database easier, a DSN can be used to save authentication and setting information for a database connection. In this way users can connect with a database once and save the information for future use. DSNs are stored locally on the computer used to reach the database. Each DSN is identified by a name, like bes_bfenterprise.

Endpoint Manager can use several DSNs to connect to the same database. Each DSN has different settings and each one can be used to connect to the database in different ways. For example, the primary distinction between the bes_bfenterprise and bes_EnterpriseServer DSNs is that bes_bfenterprise connects to the Endpoint Manager database using Windows NT authentication and bes_EnterpriseServer connects using SQL authentication.

You can view your DSNs by running **Control Panel > Administrative Tools > Data Sources (ODBC)**, which launches the ODBC Data Source Administrator tool. The first tab, **User DSN**, specifies DSNs that are available only to the currently logged in user. Most of the Endpoint Manager DSNs are found and created in the **System DSN** which contain DSNs that are available to anyone using the machine and by the System account of the machine itself. Only a user with Administrative privileges can make changes in the **System DSN** tab. If you create a new DSN it uses `SQL Server` as a Driver.

Microsoft SQL Database Connection

To configure an ODBC connection for Microsoft SQL database, you must define the following settings of the DSN used by Endpoint Manager:

Name The name of the DSN used to identify stored an ODBC Data Source. Endpoint Manager looks for DSNs with names like `enterprise_setup` and `bes_bfenterprise`. Endpoint Manager components expect a DSN with a certain name to exist and automatically attempts to use those DSNs to connect to the database. For example the Console and the Administration Tool use any DSN with the `bes_` prefix on it even if these DSNs are displayed without the prefix when launched.

Server This field specifies the machine where the Endpoint Manager database, to which the DSN connects, resides. If you are setting a remote database, change this field to point to the database machine for all DSNs that are created automatically by Endpoint Manager installers.

When you perform any upgrade, the system resets the DSNs to point to the Endpoint Manager Server. Therefore, after any upgrade to the Endpoint Manager Consoles or to the Endpoint Manager Server, ensure that you set again the DSNs to the values previously specified.

Authentication Method
You can set two types of authentication: Windows NT or SQL authentication.

The Windows NT authentication method uses your Windows Login and Password as the Login ID and Password to the database.

The SQL authentication method requires a Login ID and Password supplied manually every time a connection to the database is made.

You can set up the Endpoint Manager components to use either of these two authentication methods. Choose one approach and maintain the use of that scheme for configuring DSNs, apart from the `bes_EnterpriseServer` DSN which must always use the SQL authentication.

Default Database
The default database is the database instance that this DSN uses. The defaultEndpoint Manager database instances are: `bfenterprise` and `BESReporting` by default. If the DSN is going to be used for Web Reports it will default to the `BESReporting` database instance. Otherwise the DSN uses `bfenterprise` by default. Your authentication information is used to access this database instance as well. There are two levels of permissions on SQL Server, the first is to access the database itself and the second to access database instances.

Note: Select **Connect to SQL Server to obtain default settings for the additional configuration options** and provide an ID and password only if you want to test the connection. The Login ID and Password you provide are not stored with the DSN. They are used to obtain default settings and test the DSN. After the configuration of the DSN is complete, this information is discarded. You must provide the same credentials every time the SQL authenticated DSN attempts to connect to the database.

Table 2. Endpoint Manager Components and DSNs

Endpoint Manager Component	DSN	Authentication Methods
Endpoint Manager server installation	`enterprise_setup`	NT
Endpoint Manager server	`bes_bfenterprise`	NT or SQL
Endpoint Manager console	any DSN beginning with `bes_`	NT or SQL
Endpoint Manager Administration tool	any DSN beginning with `bes_`	NT or SQL
Endpoint Manager Web Reports	`LocalBESReportingServer` **Note:** the LocalBESReportingServer DSN contains configuration and login data and not data shown in Web Reports reports. In Web Reports on the Database Settings page when adding a new database or configuring a remote database, use the `bes_bfenterprise` DSN.	NT or SQL

DB2 Database Connection

Before setting the server ODBC connections, download the latest version of `BES\Shared\Database\DB2Schema` and create the IEM database on the Windows operating system using the command:

```
<script_location>\DB2createdb.bat <DB2 Admin User> <DB2 Admin Password> <drive letter>
```

as shown in the following example:

```
C:\TEMDB2\DB2createdb.bat db2admin db2_password C:
```

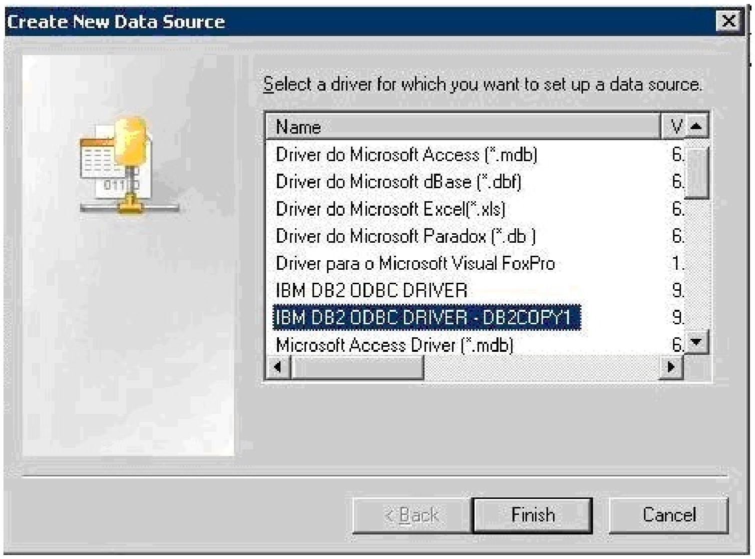
After you create the database, perform the following steps to set the Server ODBC connections:

1. Open the Microsoft Open Database Connectivity (ODBC) Data Source Administrator tool and create a new data source `bes_bfenterprise_db2` as shown in the next steps.

   A 64-bit version of the Windows operating system (such as Windows 2008 R2) includes the following versions of the ODBC Data Source Administrator tool (Odbcad32.exe):

   - The 32-bit version of the Odbcad32.exe file is located in the `%systemdrive%\Windows\SysWoW64` folder.
   - The 64-bit version of the Odbcad32.exe file is located in the `%systemdrive%\Windows\System32` folder

   This tool adds a new user data source.
2. In the Create New Data Source window, choose the driver for which you are adding a user data source and click **Finish**:

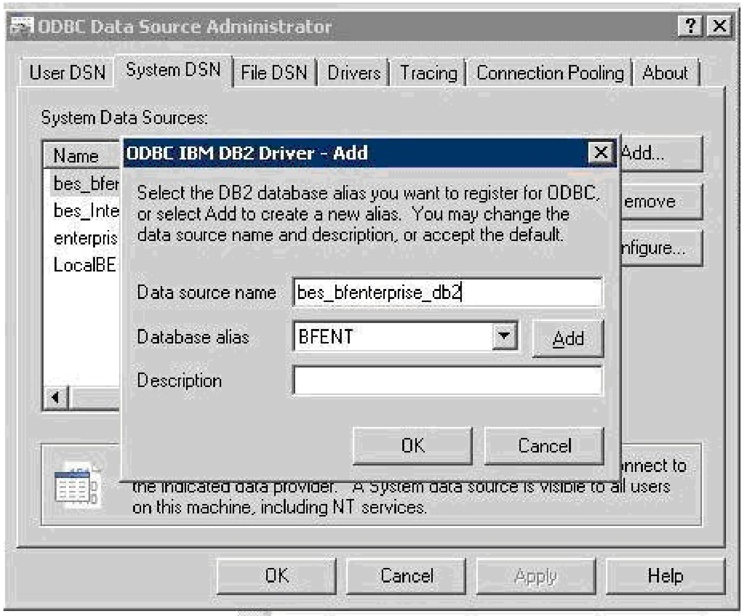


Create New Data Source

Select a driver for which you want to set up a data source.

Name	V
Driver do Microsoft Access (*.mdb)	6.
Driver do Microsoft dBase (*.dbf)	6.
Driver do Microsoft Excel(*.xls)	6.
Driver do Microsoft Paradox (*.db)	6.
Driver para o Microsoft Visual FoxPro	1.
IBM DB2 ODBC DRIVER	9.
IBM DB2 ODBC DRIVER - DB2COPY1	9.
Microsoft Access Driver (*.mdb)	6.

3. In the driver-specific setup dialog box enter the data source name, the DB2 database alias, and a description.



ODBC Data Source Administrator

System Data Sources:

Name
bes_bfer
bes_Inte
enterpris
LocalBE

ODBC IBM DB2 Driver - Add

Select the DB2 database alias you want to register for ODBC, or select Add to create a new alias. You may change the data source name and description, or accept the default.

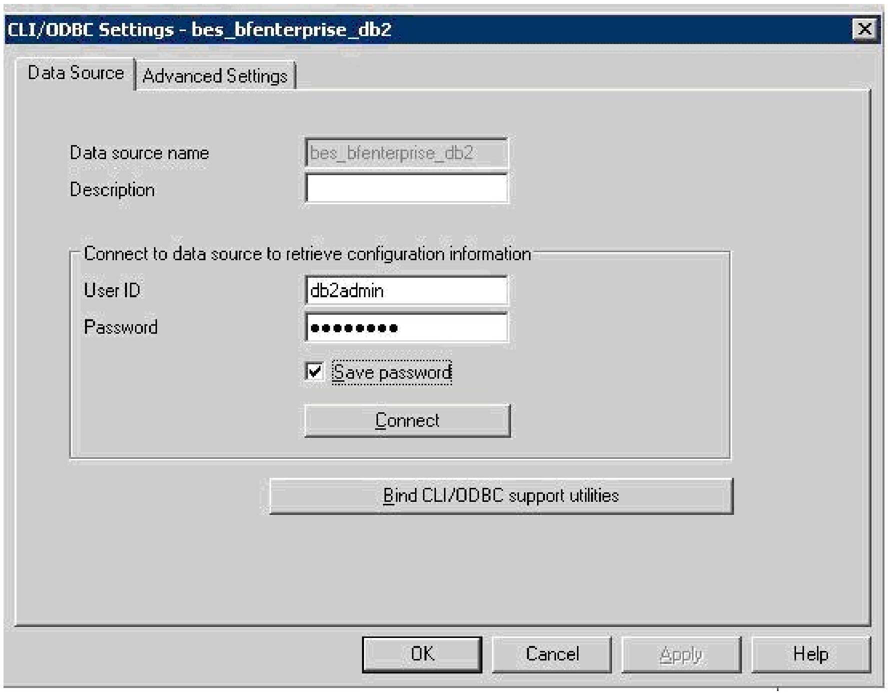
Data source name: bes_bfenterprise_db2

Database alias: BFENT

Description:

nnect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

4. In the CLI/ODBC Settings window, click **Advanced Settings**:


CLI/ODBC Settings - bes_bfenterprise_db2

Data Source | Advanced Settings

Data source name: bes_bfenterprise_db2

Description:

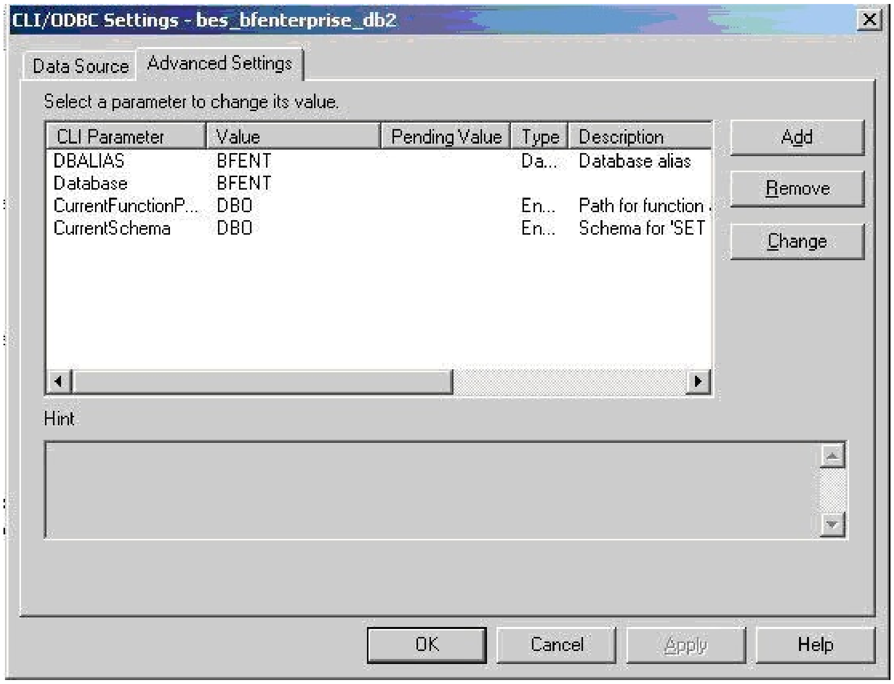
Connect to data source to retrieve configuration information

User ID: db2admin

Password: ●●●●●●●●●

☑ Save password

5. Add the following ODBC parameters:


CLI/ODBC Settings - bes_bfenterprise_db2

Data Source | Advanced Settings

Select a parameter to change its value.

CLI Parameter	Value	Pending Value	Type	Description
DBALIAS	BFENT		Da...	Database alias
Database	BFENT			
CurrentFunctionP...	DBO		En...	Path for function .
CurrentSchema	DBO		En...	Schema for 'SET

Hint

6. Test the ODBC connection, then remove the MSSQL ODBC created by the IEM installation.

7. Create the following registry keys to run the BESAdmin Administration tool:

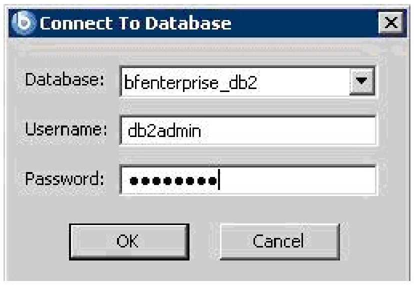
- `HKEY_CURRENT_USER\Software\BigFix\BFEadmin\Database`

  ```
  name = dsn
  type = REG_SZ
  Value = bes_bfenterprise_db2
  ```

- `HKEY_CURRENT_USER\Software\BigFix\BFEadmin\Settings`

```
name = AllowCustomUsername
type = REG_DWORD
Value = 1
```

8. Run `BESAdmin.exe` to create a schema and populate the database. See the following log files: `BESAdmin.log` located under `C:\Documents` and `BESAdminDebugOut.txt` located under `Settings\Administrator\Local Settings\Application Data\BigFix`.
9. Enter the user name and the password to connect to the DB2 database:



Connect To Database

Database: bfenterprise_db2

Username: db2admin

Password: ●●●●●●●●

10. Connect the `BESRootServer` service to DB2, by creating the following registry keys:

```
name = User
type = REG_SZ
Value = db2admin
name = Password
type = REG_SZ
Value = Bigfix11
name = DSN
type = REG_SZ
Value = bes_bfenterprise_db2
```

under:

- `HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\Database` on Windows x86 operating systems
- `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\Enterprise Server\Database` on Windows x64 machines

11. Before working with the DB2 database, remove the content of the following server folders:

```
C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\bfsites
C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\bfsites
C:\Program Files\BigFix Enterprise\BES Server\Mirror Server\Inbox
```

12. Restart all IEM services.

Increasing the size of the FillDB buffer directory

The FillDB buffer directory temporarily stores reports from the clients before they are stored into the database.

By default the directory is full if it contains 1GB of files or if it has more than 10,000 files. The consequence is that the information is not sent to the IEM server quickly, and it might be a severe problem.

You can configure the FillDB buffer directory and the maximum number of hold files by performing the following steps:

On Windows systems:

1. Add the following keys to the registries HKLM\Software\BigFix\Enterprise Server\PostResults (on 32-bit systems) and HKLM\Software\Wow6432Node\BigFix\Enterprise Server\PostResults (on 64-bit systems):

   BufferDirectoryMaxSize
   It defines the maximum size of the FillDB buffer directory, in bytes. The default value is 1GB.

   BufferDirectoryMaxCount
   It defines the maximum number of files allowed in the FillDB buffer directory. The default value is 10,000.
2. Restart the FillDB service.

On Linux systems:

1. Add the following lines to the /var/opt/BESServer/besserver.config file:

   ```
   [Software\BigFix\Enterprise Server\PostResults]
   BufferDirectoryMaxSize = <SIZE_IN_BYTES>

   [Software\BigFix\Enterprise Server\PostResults]
   BufferDirectoryMaxCount = <MAX_NUMBER_OF_FILES>
   ```

   where:

   BufferDirectoryMaxSize
   It defines the maximum size of the FillDB buffer directory, in bytes. The default value is 1GB.

   BufferDirectoryMaxCount
   It defines the maximum number of files allowed in the FillDB buffer directory. The default value is 10,000.
2. Restart the FillDB service.

HTTPS Configuration for Web Reports

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

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

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

[ req_attributes ]
challengePassword = bigcopasswrd
```

To use HTTPS:

1. Install OpenSSL if it is not already available.
2. Save your configuration file as something like `mynewconfig.conf`, and issue your certificate request. This also generates a private key (in the file named `keyfile.pem`). On Windows you can use this command:

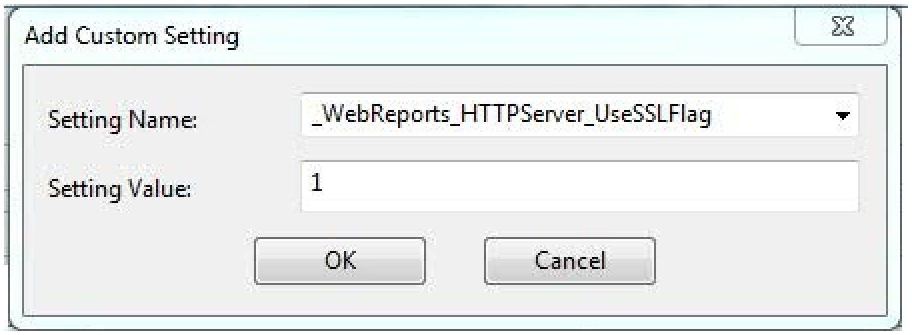
   ```
   openssl req -new -config "mynewconfig.conf" > cert.csr
   ```
3. Remove the password from your private key file:

   ```
   openssl rsa -in keyfile.pem -out nopwdkey.pem
   ```
4. Create a certificate file:

   ```
   openssl x509 -in cert.csr -out cert.pem -req -signkey nopwdkey.pem -days 365
   ```
5. Open `nopwdkey.pem` in a text viewer, copy the contents, and paste them below the certificate in `cert.pem`.
6. Save this file; it is your SSL certificate.

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

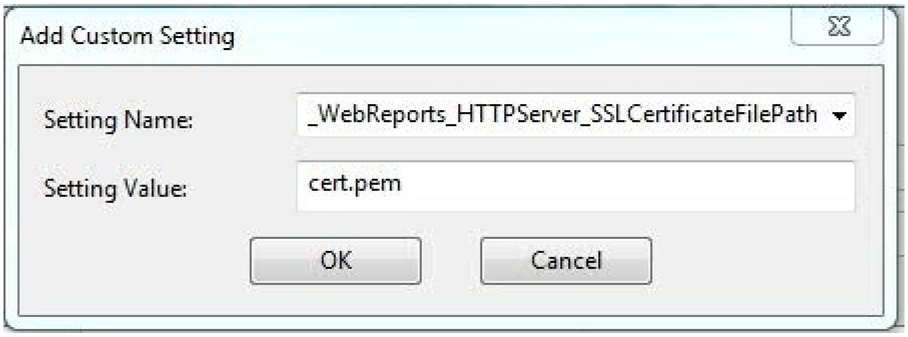
1. From the Endpoint Manager Console select the **Computers** tab.
2. Select the computer to configure and **Edit Computer Settings** from the **Edit** menu.
3. Look for **_WebReports_HTTPServer_UseSSLFlag** setting. If it exists, do not create a second one, but edit its value to 1 to enable HTTPS. If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



Setting Name: _WebReports_HTTPServer_UseSSLFlag

Setting Value: 1

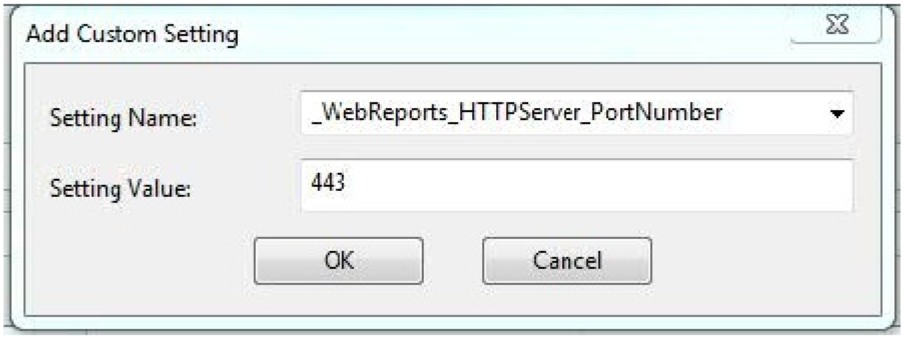
4. Look for **_WebReports_HTTPServer_SSLCertificateFilePath** setting. If it exists, do not create a second one, but edit its value to the full path name of the SSL certificate (`cert.pem`). If it does not exist, add it:



Setting Name: _WebReports_HTTPServer_SSLCertificateFilePath

Setting Value: cert.pem

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



Setting Name: _WebReports_HTTPServer_PortNumber

Setting Value: 443

6. When SSL is enabled define the forwarding port by setting the following: `_WebReports_HTTPRedirect_Enabled` to 1 and `_WebReports_HTTPRedirect_PortNumber` to the port listening for HTTP connection and redirecting the client to HTTPS.
7. Restart the **BESWebReports** service.

   On Windows, open **Services**, select **BESWebReports** and on the **Action** menu, click **Restart**.

   On Linux run from the prompt: `service beswebreports restart` or `/etc/init.d/beswebreports restart`

The SSL certificate must be in standard OpenSSL PKCS7 (`.pem`) file format. If the certificate meets all of the trust requirements of the connecting browser, then the browser connects without any intervention. If the certificate does not meet the trust requirements of the browser, then you are prompted with a dialog asking if it is OK to proceed with the connection, and giving you access to information about the certificate.

Typically, a trusted certificate is one that is signed by a trusted authority (for example, Verisign), contains the correct host name, and is not expired. The `.pem` file is your SSL certificate, which you must obtain from your CA. If you do not require authentication back to a trusted root, you can also generate a self-signed certificate using OpenSSL utilities. For more information about how to create a self-signed certificate or request a signed certificate from a trusted Certificate Authority, see Setup for SSL on IBM Endpoint Manager Web Reports.

Configuring HTTPS manually on Windows systems

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

1. Run **regedit** and locate `HKEY_LOCAL_MACHINE\Software\BigFix\EnterpriseClient\Settings\Client` for x32 systems and `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\EnterpriseClient\Settings\Client` x64 systems.

   You need to add or modify subkeys for the HTTPS flag, for the location of the SSL certificate, for the HTTPS port number, and for the redirection to HTTPS.
2. Create a subkey of **Client** called `_WebReports_HTTPServer_UseSSLFlag` (it might already exist).
3. Create a string value (reg_sz) for the key `_WebReports_HTTPServer_UseSSLFlag` called **value** and set it to 1 to enable HTTPS.
4. Create a subkey of **Client** called `_WebReports_HTTPServer_SSLCertificateFilePath` (it might already exist).

5. Create a string value (reg_sz) for the key `_WebReports_HTTPServer_SSLCertificateFilePath` called **value** and set it to the full path name of the SSL certificate (cert.pem).
6. Create a subkey of **Client** called `_WebReports_HTTPServer_PortNumber` (it might already exist).
7. Create a string value (reg_sz) for the key `_WebReports_HTTPServer_PortNumber` called **value** and set it to the port number you want to use (typically 443).
8. Create a subkey of **Client** called `_WebReports_HTTPRedirect_Enabled` (it might already exist).
9. Create a string value (reg_sz) for the key `_WebReports_HTTPRedirect_Enabled` called **value** and set it to 1 to enable the browser redirection to HTTPS.
10. Create a subkey of **Client** called `_WebReports_HTTPRedirect_PortNumber` (it might already exist).
11. Create a string value (reg_sz) for the key `_WebReports_HTTPRedirect_PortNumber` called **value** and set it to the number of the port listening for HTTP connection and redirecting the client to HTTPS.
12. Restart the **BESWebReports** service.

Configuring HTTPS manually on Linux systems

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

To define the port number you want to use:

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

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

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

To enable HTTPS:

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

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

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

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

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

Configuring the number of Web Reports results

To avoid excessive use of memory when displaying Web Reports results on `Explore Computers` reports, you can configure the `MaxReportResults` keyword. This keyword sets the maximum number of rows that can be displayed in a web report. Its default value is `1000000`. The valid value range of the keyword is 1-4294967295.

When you get the message:

```
Unable to update data table: server aborted or there was an error processing your request
```

on the report page and you see the exception:

```
Too many results returned from computer report. Report execution has been aborted
```

in the log files, indicating that the number of lines to be displayed exceeds the default value, tune the keyword value by taking into account the type of report, the computer properties, and the resources of the system where Web Reports is running.

You can set this keyword both on Windows and Linux systems where Web Reports is running, by completing the following steps:

On Windows systems:

Run **regedit** and locate the path `HKEY_LOCAL_MACHINE\Software\Wow6432Node\BigFix\Enterprise Server\BESReports`.

Create the string value (reg_sz) `MaxReportResults` and set it to the identified value.

```
"MaxReportResults"[REG_SZ] = "1000000"
```

On Linux systems:

Create the `MaxReportResults` keyword in the `[Software\BigFix\Enterprise Server\BESReports]` section of the `beswebreports.config` file and set it to the identified value:

```
MaxReportResults = 1000000
```

Downloading files in air-gapped environments

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

These utilities can also help download patch contents in a Fixlet site or single file downloads from a url. For downloading about these utilities, see Utilities.

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

On Windows systems

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

You can download the Windows Endpoint Manager Airgap utility (`BESAirgapTool.exe`), from the Utilities page.

Step 1: Setting up the network

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

Step 2: Transferring Fixlet content

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

1. From the Endpoint Manager server installation directory , run the `BESAirgapTool.exe` on the Endpoint Manager server computer to create a Fixlet update request file. Save this request to a portable drive together with the `BESAirgapTool.exe`, and the following dlls: `libBEScrypto.dll`**,** and `libBEScryptoFIPS.dll`. In addition, Microsoft C/C++ Runtime Libraries are added to the portable drive.

   The `BesAirgapTool.exe` does not run successfully without the dll files included in the same directory as the `BESAirgapTool.exe` tool.
2. Bring the portable drive to a computer with Internet connectivity and run the `BESAirgapTool.exe`. This exchanges the request file for a response file.
3. Take the portable drive back to the Endpoint Manager server computer and run the `BESAirgapTool.exe` again. This imports the response file with Fixlet content and license updates into your deployment.

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

On Linux

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

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

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

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

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

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

  ```
  libBEScrypto.dll
  libBEScryptoFIPS.dll
  ```

  In addition, Microsoft C/C++ Runtime Libraries are needed.

  ```
  msvcm90.dll
  msvcp90.dll
  msvcr90.dll
  Microsoft.VC90.CRT.manifest
  ```

  You can copy these libraries from the folder where you installed the Endpoint Manager client. The default folder is `%PROGRAM FILES%\Bigfix Enterprise\BES Client`. You can find these libraries also in the following folder: `%PROGRAM FILES%\Bigfix Enterprise\BES Server\IEM CLI`.

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

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

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

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

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

   where:

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

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

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

   -help Lists the Airgap usage.
3. On the Linux computer, extract the `airgap.tar` file with the following command under the `airgap` sub-folder::

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

.

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

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

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

Transferring Downloaded Files

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

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

You can download the current utility from http://software.bigfix.com/download/bes/util/BESDownloadCacher.exe. To see the list of available options run `BESDownloadCacher.exe /?`. If the Endpoint Manager server or an Endpoint Manager relay is installed on the system where you run the BES Download Cacher utility, the `-x` utility parameter is optional because the utility detects relevant local BES settings and reuse them as defaults

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

These sites require a three step process:

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

Transferring all files from Fixlet sites

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

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

   ```
   BESDownloadCacher.exe -m BES Asset Discovery.efxm -x downloads
   ```

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

3. When the download finishes, copy the contents of the downloads folder (just the files, not the folder) into the sha1 folder on the main Endpoint Manager server. The default location for the sha1 folder is:
   - On Windows 32-bit: `C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1`
   - On Windows 64-bit: `C:\Program Files (x86)\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1`
   - On Linux: `/var/opt/BESServer/wwwrootbes/bfmirror/downloads/sha1`

   The Endpoint Manager server uses these files instead of trying to download them from the Internet.

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

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

```
BESDownloadCacher.exe -c 1024
```

The default size of the cache is 1024 MB.

Note: Use the `-c` option only when the Endpoint Manager server or a relay is installed on the system where you run the BES Download Cacher utility. If no Endpoint Manager component is installed, cache has no limit.

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

Transferring a single file

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

1. Run the BES Download Cacher utility with the following command:

   ```
   BESDownloadCacher.exe -u http://www.mysite/downloads/myplugin.exe -x downloads
   ```

2. When the download finishes, copy the contents of the downloads folder (just the file, not the folder) into the sha1 folder on the main Endpoint Manager server. The default location for the sha1 folder is:
   - On Windows 32-bit: `C:\Program Files\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1`
   - On Windows 64-bit: `C:\Program Files (x86)\BigFix Enterprise\BES Server\wwwrootbes\bfmirror\downloads\sha1`
   - On Linux: `/var/opt/BESServer/wwwrootbes/bfmirror/downloads/sha1`

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

```
BESDownloadCacher.exe -c 1024
```

The default size of the cache is 1024 MB.

Note: Use the `-c` option only when the Endpoint Manager server or a relay is installed on the system where you run the BES Download Cacher utility. If no Endpoint Manager component is installed, cache has no limit.

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

FIPS 140-2 cryptography in the Endpoint Manager environment

Endpoint Manager uses the BigFix Cryptographic Module to perform cryptographic functions throughout its environment. For instance, every time an operator logs into the Endpoint Manager console, creates a new user, initiates an action, or subscribes to new content there are cryptographic operations performed by this module.

The BigFix Cryptographic Module has been certified by NIST as compliant with the FIPS (Federal Information Processing Standard) 140-2 standard. Successful validation under the FIPS 140-2 standard means that these software routines have received an exceptional level of scrutiny and testing by a government approved laboratory. FIPS 140-2 has four evaluation levels with Levels 1 and 2 applicable to software. Endpoint Manager chose the more stringent Level 2 validation and was certified on 12 computing platforms. Endpoint Manager stops to run or does not start if the BigFix Cryptographic Module enters an error state.

Configuring FIPS 140-2 on the Endpoint Manager Server

You can configure the Endpoint Manager server to use FIPS 140-2. In this way when the state of BigFix Cryptographic Module is in error, Endpoint Manager does not start or stops running.

To verify the appropriate setup and initialization of the module you must check the client log file by completing the following steps:

1. On the Endpoint Manager server launch the Endpoint Manager Admin Tool by selecting **Start > All Programs > Tivoli Endpoint Manager > Tivoli Endpoint Manager Administration Tool**.
2. Browse to the location of your site license and click **OK**
3. Select the **Masthead Management** tab.
4. Click **Edit Masthead**.
5. Check **Require use of FIPS 140-2 compliant cryptography** to enable FIPS 140-2.
6. Click **OK**.

7. Enter the Administrator password to perform the action.
8. To ensure that the setting has been enabled check the client log file (default log path: `C:\Program Files\BigFix Enterprise\BES Client\__BESData\__Global\Logs\YYYYMMDD.log` for the following types of messages:
   - **FIPS 140-2 Enable log file message**

     ```
     At 14:36:12 -0700 -
     FIPS mode enabled by masthead.
     At 14:36:13 -0700 -
     Cryptographic module initialized successfully in FIPS mode.
     ```
   - **FIPS 140-2 Disabled log file message**

     ```
     At 14:58:28 -0700 -
     FIPS mode disabled by default.
     Unrestricted mode
     ```

You can enforce the FIPS mode, by setting the `__BESClient_Cryptography_FipsMode` value on the client. In this way the client does not run in FIPS mode when the Cryptographic Module encounters an error at startup.

To force Endpoint Manager components to use only the FIPS validated Cryptographic library, complete the following steps:
1. Launch the Endpoint Manager Console.
2. From the **Computers** tab, right-click any listed computer and choose **Edit Computer Settings**.
3. Click **Add**.
4. In the Add Custom Settings dialog enter: `__BESClient_Cryptography_FipsMode` in the **Setting Name** and `required` in the **Setting Value**
5. Click **OK**.
6. In the **Target** tab select `All computers`. When FIPS mode is enabled all cryptographic operations such as digital signatures, encryption and SHA1, SHA2 hashing are performed using the FIPS 140-2 Level 2 certified cryptographic module.
7. In the **Execution** tab of the dialog choose **Reapply this action whenever it becomes relevant again** and click **OK**

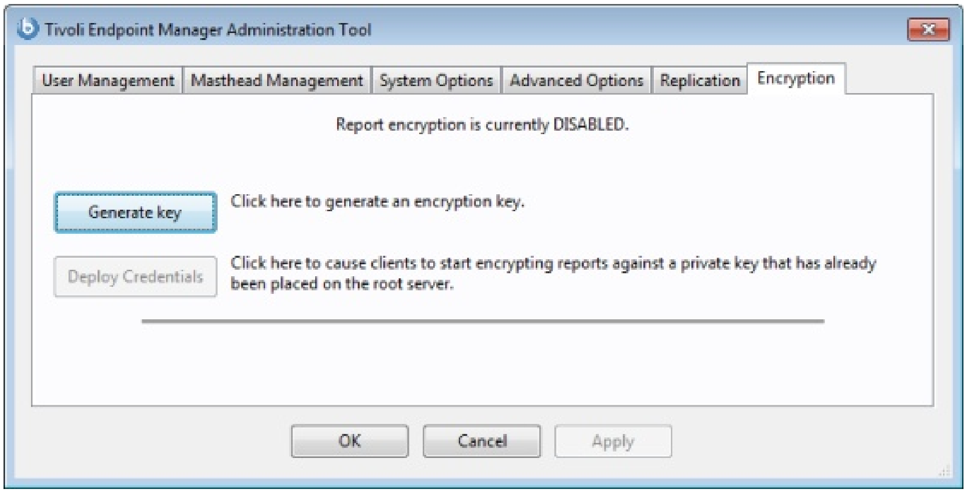
Note:
- The most common error related to the FIPS mode startup occurs on AIX and HP-UX systems when there is not enough system entropy available for the Cryptographic Module.
- The FIPS Mode setting and the Message Level Encryption (MLE) setting are independent. You can set FIPS without setting the MLE and viceversa.

For information on Message Level Encryption see “Message Level Encryption (MLE) Overview” on page 38 and “Message Level Encryption and DSA” on page 16

Managing Client Encryption

Server and relay-bound communications from clients can be encrypted to prevent unauthorized access to sensitive information. To enable it, you must generate a key and provide a setting value. The value is set in the console and is described in the *IBM Endpoint Manager Installation Guide*. The key is generated from the **Encryption** tab of the IBM Endpoint Manager Administration Tool:

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



Report encryption is currently DISABLED.

Click here to generate an encryption key.

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

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

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

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

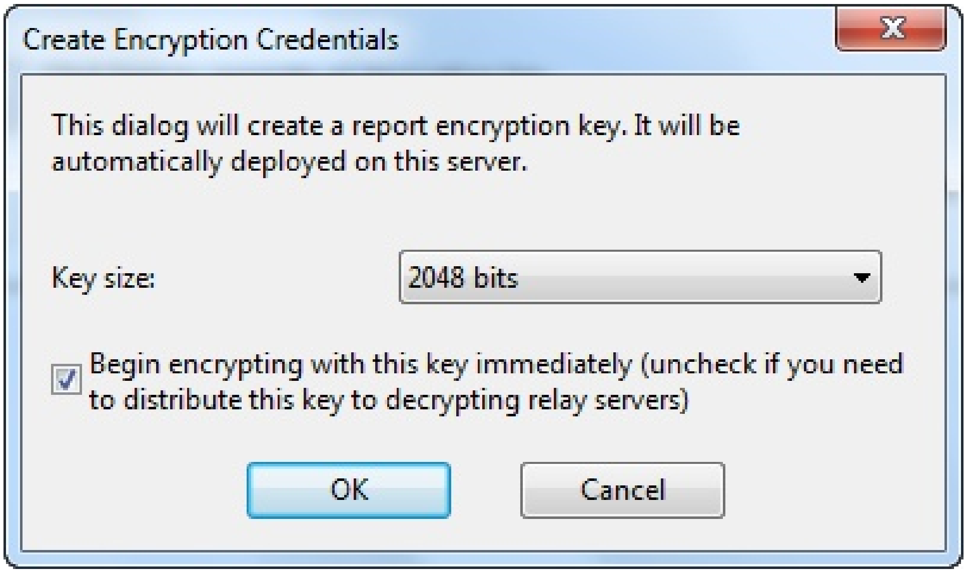
Enabled
In this state, an encryption certificate has been found in your deployment masthead, which means that you are able to turn on encryption (using the setting discussed previously) for any of the clients in your deployment. At any time, you can click **Generate new key** to create a new encryption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

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

Generating a new encryption key

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

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



Create Encryption Credentials

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

Key size: 2048 bits

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

4. From this dialog, select the key size. The default is 2048, which is adequate for most purposes. Check the box to use this key immediately. However, if you have established relays that use encryption, leave this box unchecked until you can distribute the new key to those relays.
5. Click **OK** to distribute this new key to your clients. You must provide your Site Administration Private Key to propagate the action. A final dialog asks for confirmation. For more information about encryption key sizes and server requirements, see the knowledge-base article on server requirements at the IBM Endpoint Manager support site.

Creating top-level decrypting relays

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

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

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

On Windows systems:

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

On Linux systems:

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

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

On Windows systems:

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

On Linux systems:

```
var/opt/BES Relay/Encryption Keys
```

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

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

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

Message Level Encryption (MLE) Overview

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

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

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

There are three levels of report encryption:

Required
Clients require encryption of reports and uploads. The client does not report or upload files if it cannot find an encryption certificate or if its parent relay does not support receipt of encrypted documents.

Optional
Clients prefer, but do not require encryption of reports and uploads. If encryption cannot be performed, reports and uploads are done in clear-text.

None Clients do not encrypt, even if an encryption certificate is present.

For more information about how to set encryption on Clients, see the Administration Guide.

Changing the Client Icon

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

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

On Linux systems:

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

   where: */IEM/newicon.ico* represents the full path of the new icon and `admin/icon` is the parameter to use to upload the new icon.

The icon is propagated to the clients, but it is not incorporated into the interface until the client restarts. After that, when a client interface opens (in response to an action, a dashboard or an offer), it includes the graphic icon you specified.

Optimizing the servers

IBM Endpoint Manager operates efficiently, with minimal impact on network resources. However, there might be installations that stretch the recommended configurations, where there are too many clients for the allotted server power. The best solution is to choose a server with the required characteristics for your environment; you might be able to modify some preferences to get better performance. Most of these optimizations involve a trade-off between throughput and responsiveness, so proceed with caution. Your IBM Software Support has more information about which modifications might be best for your particular deployment.

Here are some possible optimization techniques:

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

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

Optimizing the consoles

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

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

- **Use high-speed network connections** between your consoles and servers, preferably with LAN connections of at least 100 MBPS. The IBM Endpoint Manager Database can be sizeable for a large network, so running the console from a computer with a slow connection often results in very long load times.
- **Use remote control software**. With so much data to load and display, operating the console in a remote office over a slow link can be tedious. In situations like this, you might be able to benefit from solutions such as Citrix, Terminal Services, or other remote control software. Set up the remote control server on a computer with fast access to the server. Allow that machine to present instances of the console and have the branch office run these consoles remotely. The database stays in the main office, and the remote office has optimal performance. For more information, see the *IBM Endpoint Manager Installation Guide*.
- **Delete old actions**. The IBM Endpoint Manager database stores information about old actions, which the console loads in at startup and saves out at shutdown. If you do not need to track these old actions, you can delete them, allowing the console to load and close faster. Note that deleted actions continue to exist in the database, but are not loaded into the console or Web Reports and can be undeleted if necessary.
- For more information about how to enhance performance, seePerformance Configurations.

Managing Bandwidth

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

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

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

For more information about bandwidth throttling, see Overview of Bandwidth Throttling.

Dynamic Throttling

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

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

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

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

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

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

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

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

Note: A zero for this setting is the same as 100%.

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

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

```
_BESRelay_HTTPServer_DynamicThrottleEnabled
_BESRelay_HTTPServer_DynamicThrottleMaxKBPS
_BESRelay_HTTPServer_DynamicThrottleMinKBPS
_BESRelay_HTTPServer_DynamicThrottlePercentage
```

The IBM Endpoint Manager **Client settings:**

```
_BESClient_Download_DynamicThrottleEnabled
_BESClient_Download_DynamicThrottleMaxBytesPerSecond
_BESClient_Download_DynamicThrottleMinBytesPerSecond
_BESClient_Download_DynamicThrottlePercentage
```

The IBM Endpoint Manager **Gathering settings:**

```
_BESGather_Download_DynamicThrottleEnabled
_BESGather_Download_DynamicThrottleMaxBytesPerSecond
_BESGather_Download_DynamicThrottleMinBytesPerSecond
_BESGather_Download_DynamicThrottlePercentage
```

Note: For any of these settings to take effect, you must restart the affected services (server, relay, or client).

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

For more information about bandwidth throttling, see Overview of Bandwidth Throttling.

Managing Downloads

IBM Endpoint Manager uses several methods to ensure that downloads are efficient and make the best use of available bandwidth. Among other techniques, caching is used extensively by all the IBM Endpoint Manager elements, including servers, relays, and clients.

When an action on a client needs to download a file, the local cache is checked first. If the client cannot find it locally, it requests the file from its parent, typically a relay. When the file is requested, the relay checks its own cache. If it finds the file, it immediately sends it down to the requesting client. Otherwise, it passes the request up to its parent, which might be another relay and the process continues. Ultimately, a server retrieves the file from an internal server or the Internet, caches it, and then passes it back down the chain. After receiving the file, each relay in the chain caches it, and continues to forward it down to the original client, which also caches it. The agent runs the download now command while the action is running, and collects the file by requesting it from the url listed in the action script.

Each cache retains the file until it runs out of space. At that point, the cache is purged of the least-recently used (LRU) files to provide more space. You can view the relay cache size and other relay information by activating the **Analysis ID# 227 BES Relay Cache Information** available from the BES Support Site. The default cache size is 1 GB, but you can change it by using the **Task ID# 148 BES Relay/Server Setting: Download Cache Size**, also from the BES Support site.

There might be situations that require files to be manually downloaded and cached, typically because such files are not publicly available, in which case you must download the files directly from the source. Review the **Fixlet Description** tab for more information about specific manual cache requirements. You can pre-populate the download cache by copying files to the download cache location. You can also delete these files manually.

The caches are stored as subfolders of the program folder, which is created by default at `C:\Program Files\BigFix Enterprise` on Windows 32-bit systems, `C:\Program Files (x86)\BigFix Enterprise` on Windows 64-bit, and `/var/opt/BES`

Server on Linux systems. The server download cache is BES Server\wwwrootbes\bfmirror\downloads\sha1, and the client download cache is found at BES Client__BESData__Global__Cache\Downloads.

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

For information about troubleshooting relays, including bandwidth and downloading, see Relay Health.

The client collects the file by requesting it from the url listed in the action script in one of the following ways:

- When the complete set of downloads can be computed by parsing the action script, the complete set of downloads is computed by the server. The agent can ask the relay with a single request if the prefetch downloads are available for a specific action. In this request, the agent sends up the action ID, and the server response indicates all the files are available, or they are not. If these are all available, the agent starts requesting the files by their ordinal number (1 indicates the first file in the script, 2 indicates the second file in the script, etc.). If the files are not available, the relay informs the agent they are not and begins the process of fetching them, and the agent notifies that it is waiting for downloads to be available and put itself into a pending downloads state for that action for 10 minutes, at which time it asks the relay again, if the downloads are available for the specific action.

  When the downloads for an action become available on a relay, a notification is sent to the children of the relay, which uses the notification to accelerate requesting the downloads again. If notification messages are blocked for any reason, the agents 10 minute 'ask the relay again' behavior will eventually result in the agent detecting that the downloads are available, and begin to collect them. Child relays are also notified by their parent when the downloads based on the action ID and the ordinal numbers become available. They use this notification to accelerate their own request for the downloads again.
- For downloads where any of the download url, size, and hash value are listed in the action script such that only the agents can compute them, the agents query their parent relay using an itemized downloads available request. The request contains a list of download items the particular agent needs. The relay and client behave the same way as described above, delaying subsequent requests, waiting for notifications

Dynamic download White-lists

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

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

This flexibility entails extra scrutiny. Because any client can use dynamic downloading to request a file, it creates an opportunity for people to use your server to host files indiscriminately. To prevent this, dynamic downloading uses a white-list. Any request to download from a URL (that is not explicitly authorized by use of a literal URL in the action script) must meet one of the criteria specified in a white-list of URLs that is contained in the following file:

On Windows systems:

```
<Server Install Path>\Mirror Server\Config\DownloadWhitelist.txt
```

On Linux systems:

```
<Server Install Path>/Mirror Server/config/DownloadWhitelist.txt
```

The `DownloadWhitelist.txt` file contains a newline-separated list of regular expressions using a Perl regex format, such as the following:

```
http://.*\.site-a\.com/.*
http://software\.site-b\.com/.*
http://download\.site-c\.com/patches/JustThisOneFile\.qfx
```

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

Creating custom client dashboards

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

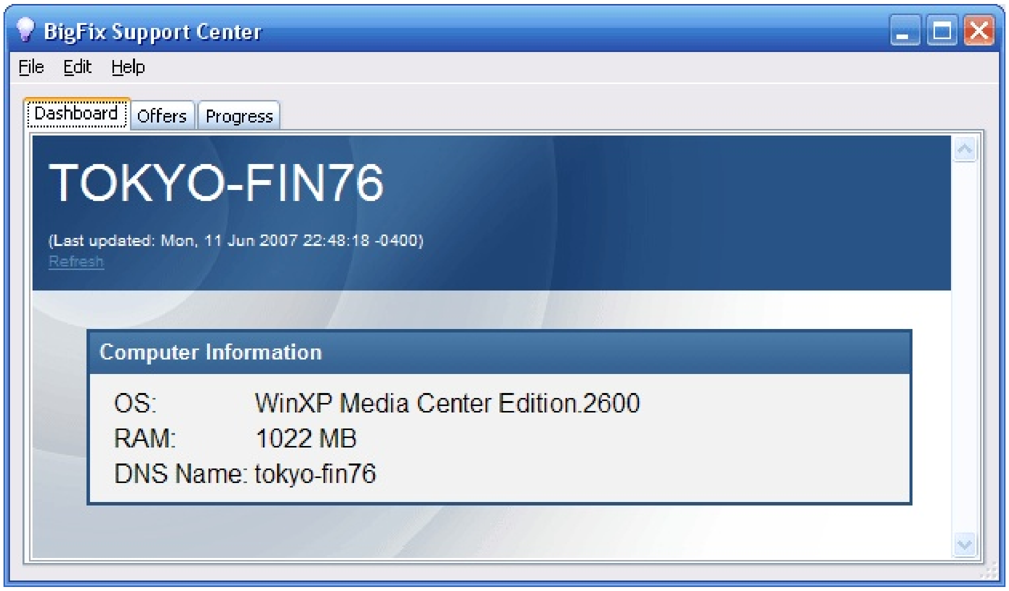
You can use style sheets to format the output. You can use the default style-sheet, **offer.css** for some preset formatting. Here is an example of a Dashboard with a title, a header, a refresh link, and a section of retrieved property values:

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

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

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

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

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

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



TOKYO-FIN76

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

Computer Information

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

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

Geographically locating clients

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

1. In the console, go to the **BigFix Management** domain, click **Computer Management** , and then click **Location Property Wizard** . A wizard document opens.
2. The wizard creates a named property allowing the clients to identify themselves based on their subnet, IP range, or other information. Read the instructions in the wizard to create the property.

Locking clients

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

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

To lock or unlock a computer, follow these steps:

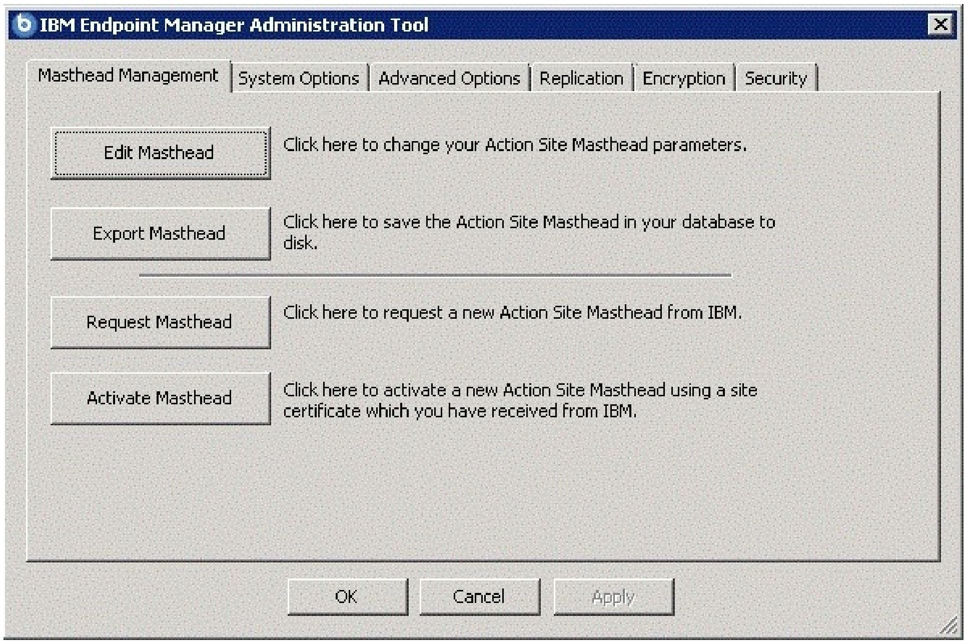
1. Click the **Computers** icon in the Domain Panel navigation tree to see the List Panel of networked IBM Endpoint Manager client computers.
2. Select the computers that you want to lock.
3. Right-click and select **Edit Computer Settings** from the pop-up menu (or select **Edit Computer Settings**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

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

Editing the Masthead on Windows systems

You can change default parameters stored in the masthead by using the **IBM Endpoint Manager Administration Tool**:

1. Launch the program from **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Administration Tool**.
2. Browse to the private key (`license.pvk`) and click **OK**.
3. Select the **Masthead Management** tab and click **Edit Masthead**.



Click here to change your Action Site Masthead parameters.

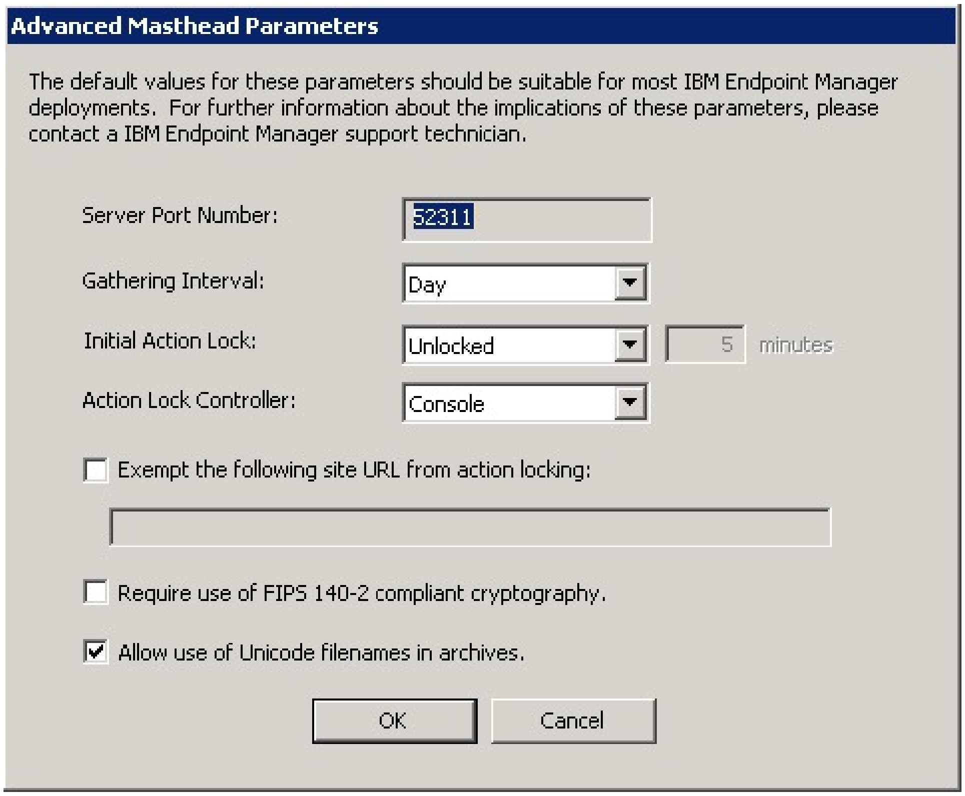
Click here to save the Action Site Masthead in your database to disk.

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

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

4. 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.



Advanced Masthead Parameters

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 edit the following options:

Server Port Number:
In general, you do not need to change this number. 52311 is the recommended port number, but you can choose a different port if that is more convenient for your particular network. Typically, you choose a port from the IANA range of private ports (49152 through 65535). You can use a reserved port number (ports 1-1024), but this might reduce the ability to monitor or restrict traffic correctly and it prevents you from using port numbers for specific applications. Do not change the server port number *after* installing the clients and creating the masthead, because Endpoint Manager might not work correctly. For additional information, see *Modifying port numbers* in the next section.

Gathering Interval:
This option determines how long the clients wait without hearing from the server before they check whether new content is available. In general, whenever the server gathers new content, it attempts to notify the clients that the new content is available through a UDP connection, circumventing this delay. However, in situations where UDP is blocked by firewalls or where network address translation (NAT) remaps the IP address of the client from the servers perspective, a smaller interval becomes necessary to get a timely response from the clients. Higher gathering rates only slightly affect the performance of the server, because only the differences are gathered; a client does not gather information that it already has.

Initial Action Lock:
You can specify the initial lock state of all clients, if you want to lock a client automatically after installation. Locked clients report which Fixlet messages are relevant for them, but do not apply any actions. The default is

to leave them unlocked and to lock specific clients later on. However, you might want to start with the clients locked and then unlock them on an individual basis to give you more control over newly-installed clients. Alternatively, you can set clients to be locked for a certain period of time (in minutes).

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

`Exempt the following site URL from action locking:`
In rare cases, you might need to exempt a specific URL from any locking actions. Check this box and enter the exempt URL. You can specify only one site URL and it must begin with `http://`.

Note: Baseline components are not exempt from action locking because they can come from different sites.

`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 IBM Endpoint Manager component attempts to go into FIPS mode. By default, the client continues in non-FIPS mode if it fails to correctly enter FIPS, which might be a problem with certain legacy operating systems. Be aware that checking this box can add a few seconds to the client startup time.

`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.

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

Note: The masthead changes do NOT affect clients that are already deployed, but you can export the masthead using the Administration Tool (**Masthead Management** tab) and replace the masthead in the BES Installers directory of the Endpoint Manager server (default directory: `<drive>:\Program Files\BigFix Enterprise\BES Installers`) so that newly deployed or installed clients use these changes.

Editing the Masthead on Linux systems

To modify the masthead, run the following command as super user:

```
./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> ]
```

where:

-sitePvkLocation=<path+license.pvk>
Specifies the private key file (*filename*.pvk). This private key file and its password are required to run the Administration Tool. Only users with access to the site level signing key and password are able to create new Endpoint Manager operators.

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

-sitePvkPassword=<password>
Specifies the password associated to the private key file (*filename*.pvk). This setting is optional, if you omit it you'll be asked to specify the password interactively when the command runs.

-display
Displays the current settings for the masthead.

advGatherSchedule (optional, integer)
Determines how long the clients wait without hearing from the server before they check whether new content is available. In general, whenever the server gathers new content, it attempts to notify the clients that the new content is available through a UDP connection, circumventing this delay. However, in situations where UDP is blocked by firewalls or where network address translation (NAT) remaps the IP address of the client from the servers perspective, a smaller interval becomes necessary to get a timely response from the clients. Higher gathering rates only slightly affect the performance of the Server, because only the differences are gathered; a client does not gather information that it already has. Valid values are:

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

advController (optional, integer)
Determines who can change the action lock state. The default is **Console**, which allows any Console operator with management rights to change the lock state of any client in the network. If you want to delegate control over locking to the user, you can select **Client**, but this is not recommended. Valid values are:

```
0=console,
1=client,
2=nobody
```

advInitialLockState (optional, integer)
Specifies the initial lock state of all clients. Locked clients report which Fixlet messages are relevant for them, but do not apply any actions. The default is to leave them unlocked and to lock specific clients later on. However, you might want to start with the clients locked and then unlock them on an individual basis to give you more control over newly-installed clients. Alternatively, you can set them to be locked for a certain period of time. Valid values are:

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

advInitialLockDuration (optional, integer)
Defines the period of time in seconds the clients must be locked.

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

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

advRequireFIPScompliantCrypto (optional, boolean)
Implements the Federal Information Processing Standard on your network. This changes the masthead so that every IBM Endpoint Manager component attempts to go into FIPS mode. By default, the client continues in non-FIPS mode if it fails to correctly enter FIPS, which might be a problem with certain legacy operating systems. Be aware that checking this box can add a few seconds to the client startup time

Modifying Global System Options

To modify a few basic system defaults, such as the minimum refresh time and the Fixlet visibility perform the following steps:

On Windows systems:

1. Launch the Administration Tool from **Start > Programs > IBM Endpoint Manager > IBM Endpoint Manager Administration Tool**.
2. Select the **System Options** tab.
3. At the top, you can set the global **Minimum Refresh**. The default is 15 seconds, which is a good balance between responsiveness and low network load. If you find that these communications are impacting your network, you can increase the minimum to 60 seconds or more.
4. External sites are visible to all console operators by default, but you can change that in the section marked **Default Fixlet Visibility**. Click the lower button to make external content invisible to all except Master Operators.

On Linux systems:

1. From the `/opt/BESServer/bin` command prompt start the command line:
   ```
   ./iem login --server=servername:serverport --user=username --password=password
   ```
2. From the `/opt/BESServer/bin` command prompt run the following command:
   ```
   ./iem get admin/options  > /appo/options.xml
   ```
3. In the `/appo/options.xml` file:
   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:noNamespaceSchemaLocation="BESAPI.xsd">
       <SystemOptions Resource="https://nc926065:52311/api/admin/options">
           <MinimumRefreshSeconds>15</MinimumRefreshSeconds>
           <DefaultFixletVisibility>Visible</DefaultFixletVisibility>
       </SystemOptions>
   </BESAPI>
   ```

   edit the following keywords to set the minimum refresh time in seconds and the external sites as visible to all the console operators or to only the Master operators:

```
<MinimumRefreshSeconds>15</MinimumRefreshSeconds>
<DefaultFixletVisibility>Visible</DefaultFixletVisibility>
```

4. Upload the modified file by running the following command:

   ```
   ./iem post /appo/options.xml admin/options
   ```

Extending the IBM Endpoint Manager License

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

1. Notify your IBM representative (if you have not paid for the extended license, you must talk to your sales person or reseller to buy an extended license).
2. Your server checks daily for a new version of your license. If you want to force your server to check immediately, in the console, go to the **BigFix Management** domain, click **License Overview** node, and click the **Check for license update**.

For additional information about how to manage licenses see the *Managing licenses* chapter of the *Administration Guide*.

Re-creating Site Credentials

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

- **Do not lose the certificate (license.crt)** and **the private key for your site (license.pvk)**. Follow standard procedures for backing up and securing critical confidential information.
- **Do not change the IP address and hostname or port number of the server**, because it is the primary identifier for your site certificate. Any change to the IP address or port number that was specified when the license was requested negates the license and necessitates a fresh installation of the IBM Endpoint Manager system. If you plan to decommission a server, be sure to apply the same IP address and port number to the replacement server.
- **Do not forget your password.** Follow your corporate standards for noting and storing your password.

Note: The IBM Endpoint Manager Site Administrator can change the password of the site-level key, if they know the current password.

Chapter 3. Maintenance and Troubleshooting

If you are subscribed to the Patches for Windows site, you can ensure that you have the latest upgrades and patches to your SQL server database servers. This means that you must install the client on all your computers, including the server and console computers. In addition, you might want to take advantage of these other tools and procedures:

- If you have the SQL Server installed, you should become familiar with the **MS SQL Server Tools**, which can help you keep the database running smoothly.
- It is standard practice to back up your database on a regular schedule, and the IBM Endpoint Manager database is no exception. It is also wise to run the occasional error-check to validate the data.
- If you start to notice any performance degradation, check for fragmentation. IBM Endpoint Manager writes out many temporary files, which might create a lot of disk fragmentation, so defragment your drive when necessary. Regular maintenance also involves running the occasional error-check on your disk drives.
- The IBM Endpoint Manager **Diagnostics Tool** performs a complete test on the server components and can be run any time you experience problems. For additional information see the *IBM Endpoint Manager Installation Guide*.
- Check the **BigFix Management** domain often. There are a number of Fixlets available that can detect problems with any of your IBM Endpoint Manager components. This can often prevent problems before they ever affect your network.
- Check the IBM Endpoint Manager Knowledge Base at Tivoli Endpoint Manager Support site. This site is continually updated, and if you cannot find an existing knowledge-base article about your question, you can find information about how to submit a question to IBM Software Support.
- Add relays to improve the overall system performance and pay close attention to them. Healthy relays are important for a healthy deployment.
- Review the **Deployment Health Checks** dashboard in the **BigFix Management** domain for optimizations and failures.
- Set up monitoring activities on the servers to notify you in the event of a software or hardware failure, including:
  - Server powered off or unavailable
  - Disk failure
  - Event log errors about server applications
  - Server services states
  - FillDB buffer directory data back-up situations

Chapter 4. Upload and archive manager settings

You can collect multiple files from Endpoint Manager clients into an archive and move them through the relay system to the server. This allows the Endpoint Manager Administrator to automatically log data from specific managed computers.

To do this, a new component called the **Archive Manager** has been added to the Endpoint Manager Client which can collect files periodically or on command. It passes the resultant compressed tar-ball to the **Upload Manager** on the Endpoint Manager Client. The Upload Manager has an input directory that queues the files for uploading.

The Upload Manager performs one upload operation at a time, moving the data in manageable chunks to reduce network traffic. It sends these chunks to the nearest Endpoint Manager relay or server, where the **PostFile** program reassembles the chunks back into the original file.

PostFile then passes the file up the chain, to the next Endpoint Manager relay or to its ultimate destination at the Endpoint Manager server. It again uses the Upload Manager to slice the file into chunks and send them on to the next PostFile program in the hierarchy. When the file finally arrives at the Endpoint Manager server, it is saved in a special directory location based on the ID of the client computer.

Along the way, both the Upload Manager and the PostFile program can alter the chunk size or throttle the upload speed to smooth out network traffic.

Note: When it encounters an unregistered Endpoint Manager Client, the Upload Manager pauses. This can happen for a variety of reasons, including a downed network, a busy server, or a disconnected client. As soon as the Endpoint Manager client can register with the Endpoint Manager system again, it restarts the Upload Manager and continues from where it stopped.

Editing the archive manager settings

A typical archive is a collection of logs and configuration files that are compiled regularly and posted to the server. There are many settings available to help you customize your logging needs.

To initialize the various archive settings, follow these steps:

1. Start the Endpoint Manager Console.
2. Select the **Computers** tab.
3. From the filter/list, select the set of computers that you want to start archiving.
4. Select **Edit Computer Settings** from the **Edit** menu. Typically, you select multiple computers, so you see a tabbed dialog box.
5. Select the **Settings** tab.
6. Check the **Custom Setting** box.
7. Enter the **Names** and corresponding **Values** of the desired settings.

Creating a Custom Action

You can create custom actions that can post attributes about the Endpoint Manager client to an archive file.

To create a custom action:

1. Start the Endpoint Manager Console.
2. Select the **Computers** tab.
3. From the filter/list, select the set of computers that you want to target for the action.
4. Select **Take Custom Action** from the **Tools** menu.
5. Select the **Action Script** tab.
6. Enter the desired **Action Script** in the text box provided.

Archive Manager

Archive Manager is a component of the Endpoint Manager Client that can collect files periodically or on command. It passes the resultant compressed tar-ball to the Upload Manager on the Endpoint Manager Client.

Archive Manager Settings

These are the settings of the Archive Manager component:

_BESClient_ArchiveManager_OperatingMode

The OperatingMode dictates the style of archiving, allowing periodic or triggered archiving. The following modes are available:

0: Disable all archival operations (default value).

1: Automatic, with a period = BESClient_ArchiveManager_IntervalSeconds.

2: Enables the **archive now** action command.

To allow a custom action to post client attributes to an archive file, make sure the OperatingMode is set to 2.

The default value of 0 disables archiving.

_BESClient_ArchiveManager_FileSet-<tag>

This setting (actually a group of settings with optional tags) specifies the files to be archived. This technique lets you specify multiple named batches of files. Each setting starts with "_BESClient_ArchiveManager_FileSet-" and ends with a batch name (the <tag> part).

The value of each setting is a path on the client file system. It can be a single file, in which case that file is part of the archive; a single directory, in which case all files in the directory will be part of the archive; or a directory path ending with wild cards, in which case all files in the directory matching the wild cards will be part of the archive.

For example, the setting _BESClient_ArchiveManager_FileSet-(log), representing all the log files in a temporary log folder, could have a value like c:\temp\log.

Everything after the dash (-) is used as the default prefix of the files as they are unpacked on the root server. Therefore a file named x.log in the c:\temp\log folder would be unpacked as (Log)x.log.

_BESClient_ArchiveManager_SendAll

This setting allows you to send just the archives that have changed, avoiding redundant uploads. There are two possible values for this setting:

0: Only send files that have changed since the last archive operation (default).

1: Send all files, even if they have not changed.

The default value of 0 is recommended for most applications.

_BESClient_ArchiveManager_MaxArchiveSize

This setting limits the size (in bytes) of the uploaded archive. Because a typical archive might be composed of several files, the archive size corresponds to the sum of the file sizes.

If the limit is exceeded, an archive that contains only the index file is created and uploaded by the Archive Manager. The index contains the following header line:

```
MaxArchiveSize: Exceeded
```

The default value is 1000000 (one million bytes), however, since IBM Endpoint Manager V8.0, the file system is 64-bit. This means that the actual maximum file size is 2^64 – 1, sufficient for any reasonably sized file.

Note: For additional information about the index file see “Archive Manager Settings” on page 58.

_BESClient_ArchiveManager_IntervalSeconds

When the OperatingMode is set to 1, this setting determines the interval at which the client triggers an archive.

The default value is 86400 seconds (24 hours).

Archive Manager internal variables

These are the internal variables of the Archive Manager component:

__BESClient_ArchiveManager_LastArchive

The Archive Manager updates this setting whenever it posts an archive. The value of the setting is the secure hash algorithm (sha1) of the file that was posted.

__BESClient_ArchiveManager_LastIntervalNumber

The Endpoint Manager Client updates this setting whenever it posts an archive. It represents the interval number from 1970 to the time when the archive was last collected. If the interval is a day long (the default), then the setting indicates the number of days from 1970 to the day when it created the last archive. It is calculated such that when the interval number changes, it is time to create a new archive.

The value is also offset by a time corresponding to the computer id, to stagger the collecting of archives.

Archive Manager Index File Format

During the building of the archive, the Archive Manager creates an index containing metadata about the archive. This is a sample index from an archive with a single file:

```
MIME-Version: 1.0
Content-Type: multipart/x-directory2; boundary="==="
Unique-ID: 1077307147
Archive-Size: 105
SendAll: 0
Date: Wed, 17 Mar 2004 02:23:01 +0000
FileSet-(LOG): c:\temp\log\newfile.log

--===

URL: file:///c:/temp/log/newfile.log
NAME: (LOG)newfile.log
SIZE: 105
TYPE: FILE
HASH: 3a2952e0db8b1e31683f801c6384943aae7fb273
MODIFIED: Sun, 14 Mar 2004 18:32:58 +0000

--===--
```

Upload Manager

The Upload Manager coordinates the sending of files in chunks to the Post File program. You can throttle the upload dataflow to conserve bandwidth. Since IBM Endpoint Manager version 8.0, the file system uses 64 bits, sufficient for file sizes of up to 2^64 – 1 bytes in length.

Upload Manager Settings

These are the settings of the Upload Manager component:

_BESClient_UploadManager_BufferDirectory
The Archive Manager always sets the Upload Manager input Buffer Directory to `__BESData/__Global/Upload`. This directory is on the client computer, in the Endpoint Manager Client folder.

_BESClient_UploadManager_ChunkSize
Uploads are done one chunk at a time. In a conflict between this computer and the upstream computer, the size of the chunk is set to the smaller of the two.

A value of 0 for the chunk size indicates that the upload is done in a single chunk. The local chunk size setting is specified in bytes. The default value is 131072 that corresponds to 128 KB.

This setting does not apply to Windows systems. There is no need of a restart to update the value of this setting.

_BESClient_UploadManager_ThrottleKBPS
After each chunk is uploaded, the Upload Manager calculates the amount of time to sleep to maintain the throttle speed in kilobytes per second (ThrottleKBPS). This allows you to compensate for network bottlenecks. For example, a Endpoint Manager client that is connected over a slow VPN to the relay might have a low upload throttle rate to minimize the bandwidth on that network segment.

In a conflict between this computer and the upstream relay (or server), the throttle KBPS is set to the smaller of the two.

The default value is 0, which disables throttling.

_BESRelay_UploadManager_BufferDirectory

Like the Endpoint Manager Client, the Endpoint Manager Relay also has an Upload Manager, and it also has a buffer directory, whose path is specified by this setting. The Upload Manager uploads the files in the sha1 subdirectory of the specified directory. It sorts the files by modification time and then, just like the Endpoint Manager Client, it uploads them in chunks to smooth out the bandwidth requirements.

_BESRelay_UploadManager_BufferDirectoryMaxSize

This setting denotes the maximum amount of space on disk that the server is allowed to take from the client using the Upload Manager. You can set the maximum file size to be as large as 2^64 – 1 bytes. Its default is 1GB.

_BESRelay_Uploadmanager_BufferDirectoryMaxCount

This setting denotes the number of files that the buffer directory is allowed to hold. Its default is 10,000.

_BESRelay_UploadManager_CompressedFileMaxSize

This setting denotes the amount of space of the largest compressed file the Upload Manager will be allowed to handle. You can set the maximum file size to be as large as 2^64 – 1 bytes. It applies only to the server and it is evaluated during the decompression of the uploaded archive.

_BESRelay_UploadManager_ChunkSize

Uploads are done one chunk at a time. In a conflict between this computer and the upstream computer, the size of the chunk is set to the smaller of the two.

A value of 0 for the chunk size indicates that the upload is done in a single chunk. The local chunk size setting is specified in bytes. The default value is 131072 that corresponds to 128 KB.

This setting does not apply to Windows systems. There is no need of a restart to update the value of this setting.

_BESRelay_UploadManager_ThrottleKBPS

After each chunk has been uploaded, the Upload Manager calculates the amount of time to sleep to maintain the throttle speed in kilobytes per second (ThrottleKBPS). This allows you to compensate for network bottlenecks. For example, a Endpoint Manager relay connected over a slow VPN to the server might have a low upload throttle rate to minimize the bandwidth on that network segment.

In case of a conflict between this computer and the upstream server (or relay), the throttle KBPS is set to the smaller of the two.

The default value is 0, which disables throttling.

_BESRelay_UploadManager_CleanupHours

Sometimes archived files accumulate but do not get uploaded. This could happen with a network outage, a downed server or other communication problem. To avoid overloading the system, these old files are deleted or cleaned up. This setting determines how old a file can get before it is deleted.

The default value is 72 hours (3 days).

PostFile

The PostFile program receives the chunks of files posted by the Upload Manager and appends them to its own copy of the file. The Upload Manager specifies the range of bytes being posted and the sha1 of the file, which is used as the filename. These parameters are appended to the URL as in the following example:

```
postfile.exe?sha1=51ee4cf2196c4cb73abc6c6698944cd321593007&range=1000,1999,20000
```

Here the sha1 value identifies the file, and the range in this case specifies the second 1,000 byte chunk of a 20,000 byte file.

When PostFile receives a chunk of the file it first checks to make sure it is the correct segment. If so, it appends the posted data to its local copy of the file. It returns the size of this file, as well as the current chunk size and throttle BPS settings.

PostFile has to handle several Endpoint Manager clients feeding into it at the same time. To balance that load, it adjusts the throttle rate. The effective throttling rate is determined by dividing the limiting PostFile rate by the number of concurrently uploading files.

For example, if PostFile has a throttle setting of 100 KBPS and 50 clients are simultaneously uploading files, the throttle value returned to each client would be adjusted to 2 KBPS. By setting custom throttle values to specific Endpoint Manager relays, you can efficiently deal with any bottlenecks in your network.

PostFile stores the partially uploaded files in the Upload Manager's buffer directory with an underscore in front of them (the Upload Manager does not upload files that begin with underscore). When PostFile receives the last chunk of the file, it calculates the sha1 of the file and checks that it matches the sha1 parameter in the URL. If so, it removes the leading underscore.

The Upload Manager can then upload the file to the next relay up the hierarchy (or any other server, if so specified).

PostFile determines whether or not the Upload Manager is running. If not, PostFile assumes that it has reached its root server destination. It renames the uploaded file, extracts the files from the archive, and deposits them in a subfolder of the Upload Manager's buffer directory.

The program calculates the subfolder path using a modulus of the computer ID. This has the effect of spreading out file directory accesses and preventing an overpopulation of any single directory.

For example, the path to file "log" from computer ID1076028615 is converted to the path "BufferDir/sha1/**15**/1076028615/log" where 15 is the remainder modulo 100 (the lower two digits) of the id.

If the uploaded file is a valid Endpoint Manager archive and is successfully extracted, then the original uploaded file is deleted.

PostFile Settings

PostFile uses the **_BESRelay_PostFile_ChunkSize** and **_BESRelay_PostFile_ThrottleKBPS** settings for the chunk size and throttle values for incoming data. These values can be adjusted for varying connection speeds or other network anomalies.

When PostFile communicates with the upload manager, it passes along these values. As mentioned before, if there is a conflict between any two computers over these settings, it favors the smaller value.

The default values are 128K for ChunkSize and 0 for ThrottleKBPS (disable throttling).

Resource Examples

Example 1

In this example, we want to collect all the files in the `c:\log` folder and all the .ini files in the `c:\myapp` folder once an hour. Send up only the differences and don't send the archive if it exceeds 1,000,000 bytes in size. To set this up, create the following settings in the Endpoint Manager Console:

```
_BESClient_ArchiveManager_FileSet-(Log) = c:\log
_BESClient_ArchiveManager_FileSet-(Ini) = c:\myapp\*.ini
_BESClient_ArchiveManager_OperatingMode = 1
_BESClient_ArchiveManager_Interval_Seconds = 3600
_BESClient_ArchiveManager_SendAll = 0
_BESClient_ArchiveManager_MaxArchiveSize = 1000000
```

Example 2

In this example, we want the same set of files as above, but we also want to collect some useful attributes (retrieved properties) from the client computer. A custom action can generate these attributes and trigger an archive when it completes. It uses the same settings as above, but sets the operating mode to 2 to enable the **archive now** action command:

```
_BESClient_ArchiveManager_OperatingMode = 2
```

You can then create a custom action, specifying the attributes you want to collect. For example, to append the operating system, computer name, and DNS name to the log file, create a custom action like this:

```
appendfile {"System:" & name of operating system}
appendfile {"Computer:" & computer name}
appendfile {"DNS name:" & dns name}
delete "c:\log\properties.log"
copy __appendfile "c:\log\properties.log"
archive now
```

The **appendfile** command creates a temporary text file named **__appendfile** . Each time you invoke the command, it appends the text you specify to the end of this temporary file.

The **delete** and **copy** commands clear out the old log file (if any) and copy the __appendfile to the log. This has the effect of creating a new properties.log file. The **archive now** command immediately creates an archive, as long as the OperatingMode is set to 2.

You can then target this action to any subset of Endpoint Manager Clients, using whatever scheduling you choose. Using variations on this scheme, you could perform a full archive once a week, in addition to nightly differences.

Chapter 5. Command-Line Interface

The Endpoint Manager Command-Line Interface (CLI) is a utility that facilitates programmatic control of an Endpoint Manager Server using the server RESTAPI. It is a lightweight wrapper for user authentication, session management, HTTP request and response generation, and parsing. The utility is packaged as `iem.exe` on Windows systems and `iem` on Linux Red Hat Enterprise V.5.0 (or later) systems and is installed with the server installer.

Location

On a Linux server, the Endpoint Manager command line is deployed at the following path:

```
/opt/BESServer/bin/iem
```

On Windows server, the Endpoint Manager command line is deployed at the following path:

```
C:\Program Files (x86)\BigFix Enterprise\BES Server\IEM CLI\iem.exe
```

Conventions and usage

Conventions:

```
<> = required argument
[] = optional argument
* = 0 or more instances supported
| = OR
```

Usage:

```
iem <GET|DELETE> <Resource> [-q] [--param value]*
```

OR

```
iem <POST|PUT> [inputFile] <Resource> [-q] [--param value]*
```

OR

```
iem admin <COMMAND> [-q] <--pkey=KEYFILE>
                   [--pkeypwd=PASS][--param value]*\n
```

OR

```
iem LOGIN [-q] [--server=SERVER] [--user=USER]
[--password=PASS] [--masthead=PATH_TO_TRUSTED_MASTHEAD]
```

```
-q : Quiet mode. Input prompts disabled.
```

User Authentication and Session Management

To start the command line interface, log in to the server with the following command from a command prompt:

```
iem LOGIN
```

Three arguments are required, `SERVER`, `USER`, and `PASSWORD`. Provide these arguments in one of the following three ways:

Environment variables
Use IEM_SERVER, IEM_USER, and IEM_PASSWORD to specify the values of the arguments.

Command line
Use --server, --user, and --password to specify the variables on the command line.

Standard Input
If any arguments are not provided by either of the first two methods, the CLI utility prompts you to provide them.

If the server uses a self-signed certificate for HTTPS interactions, the utility prompts you to accept or decline the certificate. If you choose to trust it, the certificate is cached and used to validate all future interactions with the server.

The --masthead command line argument can be used to specify a local file to trust when communicating with the server, removing the need for this prompt. The masthead file is copied into the CLI cache directory and used for all future interactions with the server.

When login is successful, the utility receives a session token from the server, which it saves to a local config file and uses for future communication. This token is currently invalidated after 5 minutes of inactivity by the server. You can configure this time with the setting _BESDataServer_APIAuthenticationTimeoutMinutes.

Local Data Directory

The CLI stores a config file and a directory tree of cached server certificates locally. By default, this is located in a .iem folder in the user profile directory /usr/{user}) on Linux systems or in %LOCALAPPDATA%\BigFix on Windows systems. If a console is installed on the local Windows machine, any server certificates that have been trusted by the console are implicitly trusted by the CLI as well.

The directory used for local caching can be overridden with the environment variable IEM_DATADIR.

FIPS Deployments

The Endpoint Manager CLI tool is provided as a convenient wrapper for HTTP requests to the REST API on the root server. The CLI is currently **NOT** capable of using the Endpoint Manager FIPS-compliant cryptography library. To have this capability in a REST API HTTP environemnt, access REST API endpoints from another FIPS-capable client application.

Making Requests

The CLI is a lightweight abstraction of HTTP requests to the Endpoint Manager Server RESTAPI. The basic syntax for constructing requests using the CLI is:

```
iem <METHOD> <RESOURCE>
```

where:

<METHOD>

Refers to the HTTP method of the request and can be: `GET`, `POST`, `PUT`, and `DELETE`

<RESOURCE>

Refers to the RESTAPI resource that is being requested. See RESTAPI.

Query Parameters

If the request requires query parameters (such as, the RESTAPI resource `/api/query` requires the parameter `relevance=<expression>`), you can specify them by using the command line in the following format:

```
--param value
```

or

```
--param=value
```

Some examples:

```
iem GET query --relevance "names of bes computers"
iem GET query --relevance=now
```

POST and PUT Input

POST and PUT requests require a body in their HTTP Requests. You can specify the body either as an input file on the command line, such as:

```
iem POST inputfile.xml operator/bigfix
```

By running this command you post the file `inputfile.xml` to the location `operator/bigfix` and update the operator `bigfix` with the information provided in the `inputfile.xml` file or, you can enter it manually when prompted (if no input file is specified on the command line, the utility prompts for input:

```
iem POST query
Input: relevance=now
```

The input must be of the format expected by the specified RESTAPI resource, the CLI does not do any pre-parsing or sanity checking.

Portability

The Endpoint Manager executable can be run on any machine. To run it from a location other than the one in which it was installed, copy the executable and the `libBEScrypto_1_0_0_4` library into the same directory on the target machine. The Endpoint Manager tool runs only in non-FIPS mode so the `libBEScrypto_1_0_0_1` library is not required.

Note: On Linux systems, you must run the tool from the directory containing the `libBEScrypto_1_0_0_4` library, otherwise, the environment variable `BES_LIBPATH` must be set to a directory containing that executable.

IEM CLI Examples

The following links contain relevant examples of the syntax used in the Endpoint Manager commands:

- Login
- Operators
- Advanced Options
- System Options
- Export masthead
- Actions
- Fixlet
- LDAP
- Role

Actions

To submit the Fixlet ID 42 in the Master Action Site, on the computer `nc926036.romelab.it.ibm.com`, create an XML file as follows:

```
<BES xmlns:xsi="http://www.w3.org/2001
             /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
      <SourcedFixletAction>
        <SourceFixlet>
            <Sitename>ActionSite</Sitename>
            <FixletID>42</FixletID>
            <Action>Action1</Action>
        </SourceFixlet>
        <Target>
            <ComputerName>nc926036.romelab.it.ibm.com</ComputerName>
        </Target>
      </SourcedFixletAction>
</BES>
```

Use the following command to post the action of submitting the Fixlet on a specific computer:

```
./iem post /TEM/take_action_site.xml actions
```

Advanced Options

To get the list of advanced options, run the following command:

```
./iem get admin/fields
```

The command returns the list of fields in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="BESAPI.xsd">
            <AdminField Resource="https://nc926065:52311/api/admin
                                    /field/usePre70ClientCompatibleMIME">
                 <Name>usePre70ClientCompatibleMIME</Name>
                 <Value>false</Value>
           </AdminField>
```

To set the admin key `disableNmoSiteManagementDialog`, create an XML file (`besadmin.xml`) as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:noNamespaceSchemaLocation="BESAPI.xsd">
          <AdminField Resource="https:/nc926065:52311/api/admin
                                     /field/disableNmoSiteManagementDialog">
                <Name>disableNmoSiteManagementDialog</Name>
                <Value>1</Value>
          </AdminField>
</BESAPI>
```

Use the following command to set the appropriate attribute:

```
./iem post /TEM/besadmin.xml admin/fields
```

Export masthead

Use the following command to export the masthead to standard output:

```
./iem get admin/masthead
```

Use the following command to retrieve masthead parameters:

```
./iem get admin/masthead/parameters
```

The command returns the list of parameters in XML format as follows:

```
<BESAPI xmlns:xsi="http://www.w3.org/2001
          /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
            <MastheadParameters Resource="https://nc926065:52311
                                          /api/admin/masthead/parameters">
                <PortNumber>52311</PortNumber>
                <GatherInterval>Day</GatherInterval>
                <Controller>nobody</Controller>
                <InitialLockState>on</InitialLockState>
                <RequireFIPSCompliantCrypto>false</RequireFIPSCompliantCrypto>
           </MastheadParameters>
</BESAPI>
```

Fixlet

To get the list of Fixlets in the custom site `myfixes`, use the following command:

```
./iem get fixlets/custom/myfixes
```

The command returns the list of Fixlets in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001
         /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
      <Fixlet Resource="https://nc926065:52311/api/fixlet/custom/myfixes/34?"
        LastModified="Mon, 10 Dec 2012 14:33:36 +0000">
              <Name>myfixes Custom Fixlet</Name>
              <ID>34</ID>
      </Fixlet>
      <Fixlet Resource="https://nc926065:52311/api/fixlet/custom/myfixes/40?"
        LastModified="Mon, 10 Dec 2012 16:05:30 +0000">
              <Name>MyFixlet</Name>
              <ID>40</ID>
      </Fixlet>
</BESAPI>
```

LDAP

To get the list of defined LDAPs, use the following command:

```
./iem get ldapdirectories
```

The command returns the list of LDAP in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="BESAPI.xsd">
    <LDAPDirectory Resource=" https://nc125058.romelab.it.ibm.com:52311
                                    /ldapdirectory/34">
          <ID>34</ID>
          <Name>AD</Name>
          <IsActiveDirectory>true</IsActiveDirectory>
          <IsGlobalCatalog>true</IsGlobalCatalog>
          <UseSSL>false</UseSSL>
          <BaseDN>DC=tem,DC=test,DC=com</BaseDN>
          <UIDAttribute>userPrincipalName</UIDAttribute>
          <UserFilter>(objectCategory=user)</UserFilter>
          <GroupFilter><![CDATA[(&(objectCategory=group)
                (groupType:1.2.840.113556.1.4.803:=2147483648))]]></GroupFilter>
          <User>TEM\Administrator</User>
          <Servers>
            <Server>
                <Host>10.43.5.20</Host>
                <Port>3268</Port>
                <Priority>0</Priority>
            </Server>
          </Servers>
    </LDAPDirectory>
```

To create a new LDAP, use the same XML syntax as `./iem get ldapdirectories` and add the following row after the `User` row in the XML file:

```
<Password>MyLDAP-Password</Password>
```

Then create the new LDAP with the following command:

```
./iem post MyLDAP.xml ldapdirectories
```

To get the configuration data of a specific LDAP having its ID (in the current example `ID=34`) run the following command:

```
./iem get ldapdirectory/34
```

The command returns the LDAP configuration in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xsi:noNamespaceSchemaLocation="BESAPI.xsd">
      <LDAPDirectory Resource="https://nc125058.romelab.it.ibm.com:52311
                                    /ldapdirectory/34">
             <ID>34</ID>
             <Name>AD</Name>
             <IsActiveDirectory>true</IsActiveDirectory>
             <IsGlobalCatalog>true</IsGlobalCatalog>
             <UseSSL>false</UseSSL>
             <BaseDN>DC=tem,DC=test,DC=com</BaseDN>
             <UIDAttribute>userPrincipalName</UIDAttribute>
             <UserFilter>(objectCategory=user)</UserFilter>
             <GroupFilter><![CDATA[(&(objectCategory=group)
                (groupType:1.2.840.113556.1.4.803:=2147483648))]]></GroupFilter>
             <User>TEM\Administrator</User>
             <Servers>
                     <Server>
                            <Host>10.43.5.20</Host>
                            <Port>3268</Port>
                            <Priority>0</Priority>
                    </Server>
             </Servers>
      </LDAPDirectory>
```

To remove a specific LDAP having its ID (in the current example ID=34) run the following command:

```
./iem delete ldapdirectory/34
```

To convert a local operator into an LDAP operator, run the following command:

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

where <file> is the mapping file containing the matching between Windows local operators and LDAP operators. Each line of the file must contain the name of the user to convert, followed by a tab and the name of the user in LDAP or Active Directory. The LDAP name must have the same format used to log into the console, such as domain\user, user@domain, or user. If the file is not available, BESAdmin converts all local users assuming their name in LDAP or Active Directory is the same as their local user name.

Login

To log in:

```
./iem login --server=ServerName:ServerPort --user=master --password=Mypassword
```

To perform an https login:

```
./iem login --server=https://TEMServer:52311 --user=master
      --password=Mypassword
```

Operators

To display a list of operators (local and LDAP), run the following command:

```
./iem get operators
```

To get roles associated to an operator, run the following command:

```
./iem get operator/OperatorName/roles
```

To add an operator, use the XML syntax example from ./iem get operators, remove the row <LastLoginTime>. For a local operator, add the row <Password>, and then run the following command:

```
./iem post MyOperator.xml operators
```

To modify an operator, use the XML syntax example from ./iem get operators, and then run the following command:

```
./iem post /tmp/Operator.xml operator/MyOperatorName
```

To remove an operator (local and LDAP), run the following command:

```
./iem delete operator/OperatorName
```

Replication

You can change the replication interval and the master server of your replication servers using the command line.

Replication interval changes

To change the replication interval, perform the following steps:

1. Start the command line:

   On Windows systems:

```
iem login --server=servername:serverport --user=username
--password=password
```

On Linux systems:

```
./iem login --server=servername:serverport --user=username
--password=password
```

2. Retrieve the replication server settings by running the following command:

   On Windows systems:

   ```
   iem get replication/server/0 > c:\temp\replicationServer0.xml
   ```

   On Linux systems:

   ```
   ./iem get replication/server/0 > /appo/replicationServer0.xml
   ```

3. Edit the following keyword of the `replicationServer0.xml` file:

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

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

   This is an example of the `replicationServer0.xml` file:

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <BESAPI xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                               xsi:noNamespaceSchemaLocation="BESAPI.xsd">
      <ReplicationServer Resource="http://9.87.126.68:52311/api/replication
                                                               /server/0">
              <ServerID>0</ServerID>
              <URL>http://nc926068.romelab.it.ibm.com:52311</URL>
              <DNS>nc926068.romelab.it.ibm.com</DNS>
         <ReplicationIntervalSeconds>300</ReplicationIntervalSeconds>
         <ReplicationLink Resource="http://9.87.126.68:52311/api/replication
          /server/0/link/3">
                 <SourceServerID>0</SourceServerID>
                 <DestinationServerID>3</DestinationServerID>
                 <Weight>1</Weight>
                 <IsConnected>0</IsConnected>
                 <LastReplication>Fri, 01 Mar 2013 11:17:12 +0000
                 </LastReplication>
                 <LastError>19NoMatchingRecipient - Fri, 01 Mar 2013 11:17:12 +0000
                 </LastError>
         </ReplicationLink>
         <ReplicationLink Resource="http://9.87.126.68:52311/api/replication/server/
                                           3/link/0">
                      <SourceServerID>3</SourceServerID>
                      <DestinationServerID>0</DestinationServerID>
                      <Weight>1</Weight>
                      <IsConnected>1</IsConnected>
                      <LastReplication>Fri, 01 Mar 2013 11:17:18 +0000
                      </LastReplication>
         </ReplicationLink>
      </ReplicationServer>
   </BESAPI>
   ```

4. Upload the modified file by running the following command:

   On Windows:

   ```
   iem post c:\temp\replicationServer0.xml  replication/server/0
   ```

   On Linux:

   ```
   ./iem post /appo/replicationServer0.xml  replication/server/0
   ```

Master server switch

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

1. Start the command line:

   On Windows systems:

   ```
   iem login --server=servername:serverport --user=username
   --password=password
   ```

   On Linux systems:

   ```
   ./iem login --server=servername:serverport --user=username
   --password=password
   ```

2. Retrieve the settings to switch the master server:

   On Windows systems:

   ```
   iem get admin/fields > c:\temp\switchmaster.xml
   ```

   On Linux systems:

   ```
    ./iem get admin/fields > /appo/switchmaster.xml
   ```

3. In the `switchmaster.xml` file, add or edit the following keyword and its value:

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

   to switch the master server to another master server:

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

4. Upload the modified file by running the following command:

   On Windows systems:

   ```
   iem post c:\temp\switchmaster.xml admin/fields
   ```

   On Linux systems:

   ```
    ./iem post /appo/switchmaster.xml admin/fields
   ```

After the value has successfully replicated to the new server, it become the master server. If a server has a failure while it is the master, another server must be made the master server by direct manipulation of the ADMINFIELDS table in the database.

Role

To get the role configuration, run the following command:

```
./iem get roles
```

The command returns the role configuration in XML format.

To create a new role, run the following command:

```
./iem post Example.xml roles
```

Where `Example.xml` contains role configuration data in a XML format.

System Options

To display `MinimumRefreshSeconds` (seconds), and `DefaultFixletVisibility` (Visible, Hidden) run the following command:

```
./iem get admin/options
```

The command returns the list of options in XML format as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001
     /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
        <SystemOptions Resource="https://nc926065:52311/api/admin/options">
             <MinimumRefreshSeconds>15</MinimumRefreshSeconds>
             <DefaultFixletVisibility>Visible</DefaultFixletVisibility>
       </SystemOptions>
</BESAPI>
```

To set the system option `MinimumRefreshSeconds` create an XML file (`SystemOptions.xml`) as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<BESAPI xmlns:xsi="http://www.w3.org/2001
     /XMLSchema-instance" xsi:noNamespaceSchemaLocation="BESAPI.xsd">
        <SystemOptions Resource="https://nc926065:52311/api/admin/options">
             <MinimumRefreshSeconds>20</MinimumRefreshSeconds>
             <DefaultFixletVisibility>Hidden</DefaultFixletVisibility>
        </SystemOptions>
</BESAPI>
```

Use the following command to set the appropriate attribute:

```
./iem post /TEM/SystemOptions.xml admin/options
```

Appendix. Support

For more information about this product, see the following resources:

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services that are offered in the USA.

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

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

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

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

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

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

Programming interface information

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

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

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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM® Corp. and Quantum in the U.S. and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA