BlackBerry Enterprise Server for IBM Lotus Domino

Version 4.0

Maintenance Guide

BlackBerry Enterprise Server Version 4.0 for IBM Lotus Domino Maintenance Guide

Last modified: 10 November 2004

Part number: SWD_X_BES(EN)-021.001

At the time of publication, this documentation complies with BlackBerry Enterprise Server Version 4.0 for IBM Lotus Domino.

Research In Motion Limited
295 Phillip Street
Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
Centrum House, 36 Station Road
Egham, Surrey TW20 9LF
United Kingdom

Published in Canada

Contents

1

Customizing the BlackBerry environment

Customizing the BlackBerry Controller configuration

The BlackBerry® Controller monitors the BlackBerry Messaging Agent component. In the case of a failed operation, the BlackBerry Controller detects and restarts the appropriate processes, which enables the BlackBerry Enterprise Server™ to continue to function in the event of non-responsive threads or inactive services.

The BlackBerry Controller does not attempt to restart the Messaging Agent when it is manually stopped by an administrator.

The BlackBerry Controller does not work with remote desktop applications.

Warnings: The BlackBerry Controller should not be manually restarted.

Performance monitoring cannot be running on the same server as the BlackBerry Controller.

Modify default settings using the Registry Editor

Warning: Use the Registry Editor with caution. Failure to do so might cause damage to computer programs or the Microsoft® Windows® operating system.

1. Open **regedit.exe**.
2. In the left pane, browse to HKEY_LOCAL_MACHINE\Software\Research In Motion\BlackBerry Enterprise Server.
3. Click **BlackBerry Controller**.
4. Modify the desired values.

Option	Default	Description
MaxRestartsPerDay	3	Defines the maximum number of times, for each server, that the BlackBerry Controller restarts the BlackBerry Enterprise Server on a daily basis.

Option	Default	Description
MaxUserDumpPerDay	3	Defines the maximum number of .dmp files generated, for each server on a daily basis, before the BlackBerry Controller restarts the BlackBerry Enterprise Server. These files are named DBES_*<yyyymmdd>*_*<hhmm>*.dmp where *<yyyymmdd>* is the log file creation date, and *<hhmm>* is the log file creation time. **Note:** To use this data collection option, download and install the User Mode Process Dump application included in the Microsoft Original Equipment Manufacturer (OEM) Support Tools. Visit http://support.microsoft.com/default.aspx?scid=kb;en-us;253066 for more information.
RestartOnCrash	1	Defines whether the BlackBerry Controller should restart the BlackBerry Enterprise Server if it stops responding. • 1: Restart the BlackBerry Enterprise Server. • 0: Do not restart the BlackBerry Enterprise Server.
SysLogPort	localhost:4070, localhost:4071	Specifies the port number on which the BlackBerry Controller listens to BlackBerry Enterprise Server log events.
WaitToRestartOnHung	0	Defines the number of missed health checks that occur before the BlackBerry Controller restarts the BlackBerry Enterprise Server. Health checks occur every 10 minutes. If the health check does not receive a response from the thread being monitored, this missed health check is tracked in the log file as the Wait Count. `[20148] (05/12 12:21:00):{0xC28} Thread: *** No Response *** Thread Id=0xB00, Handle=0x558, WaitCount=2,` When the Wait Count value reaches the WaitToRestartOnHung value, the BlackBerry Controller restarts the BlackBerry Enterprise Server. A value of **0** means that the BlackBerry Enterprise Server is not restarted because of non-responsive threads. **Warning:** If this feature is enabled, do not set the value any lower than **5**, so that the BlackBerry Controller has sufficient time to monitor thread health checks.
WaitToRestartOnSilentCrash	0	Defines the number of missed health checks that occur before the BlackBerry Controller assumes the BlackBerry Enterprise Server has stopped responding and restarts the BlackBerry Enterprise Server.

Customizing the database configuration

You can change the configuration database settings that were defined during the installation process.

Assign the server to another database

Warning: When you assign the BlackBerry Enterprise Server to use a different database, the data is not copied from the original database. If you want to move the database information, backup the information, restore it to the new location, and then assign the server to use the new database location. See " Restoring the configuration database" on page 36 for more information

You must use the same administrator account that was used during the installation process.

1. In the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. On the **Database Connectivity tab**, click **Change Database**.

3. Click **Yes** to proceed with the database change and to stop the BlackBerry Services.
4. Complete the configuration wizard, providing new database information.
5. If applicable, update the remote BlackBerry Manager(s) with new database information. See the *BlackBerry Enterprise Server Administration Guide* for more information.

Change the authentication method

Changing the authentication method changes how the BlackBerry Enterprise Server connects to the configuration database.

Note: You must use the same administrator account that was used during the installation process.

1. In the taskbar, click **Start** > **Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. On the **Database Connectivity** tab, in the **Authentication** section, modify the desired values.

Action	Procedure
Switch to Windows authentication.	▸ Select the **Windows (Trusted)** option.
Switch to SQL authentication.	1. Select the **SQL Authentication** option. 2. In the **User Name** field, type a name. 3. In the **Password** field, type a password.

3. Click **OK**.

Use database roles

Use predefined database roles to limit the access of remote and local BlackBerry Manager installations.

Members of the **rim_db_bes_server** role can read and write to the database, but cannot make any changes to the database schema.

Customizing logging configuration

You can change logging settings at either a global level (all log files on the BlackBerry Enterprise Server) or at a component level.

Change global logging settings

1. In the taskbar, click **Start > Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. On the **Logging** tab, modify the desired values.

Option	Description
Log Root	Defines the root folder in which all logs associated with BlackBerry Enterprise Server operations are stored. **Note:** This folder must be on a local drive.
Log file prefix	Specifies a custom prefix to add to all log file names.
Create daily log folder	Specifies whether daily folders are created for logs. If cleared, all logs are stored in the root folder.

3. Click **OK**.

Change component logging settings

1. In the taskbar, click **Start > Programs** > **BlackBerry Enterprise Server** > **BlackBerry Server Configuration**.
2. On the **Logging** tab, click a BlackBerry Enterprise Server component or service.
3. Modify the desired values.

Option	Default	Description
Debug log identifier		Defines the default 4-letter identifier of the component. See " File names" on page 21 for more information. **Note:** The identifier can be customized, up to 16 letters
Debug daily log file	Yes	Specifies whether a new log file is created every day. If set to **No**, the log files created do not contain the date as part of the name.
Debug log level		Defines the level of logging written to the log file, using one of the following: • 1: Error • 2: Warning • 3: Information • 4: Debug • 5: Verbose
Debug log size	0	Defines the maximum log file size in MB. When set to 0, there is no limit enforced. If Auto Log Rolling is enabled, a new file is created. If disabled, the existing file is overwritten.
Debug log auto-roll	No	Specifies whether a new log file is created when a component is restarted or the maximum file size is reached. If set to **Yes**, a new log file is created and the log number incremented.
Debug log maximum daily file age	0	Defines the maximum log age in days. If enabled, files are deleted after they exceed the age. When set to 0, there is no limit enforced.

4. Click **OK**.
5. Restart the component or service for the changes to take effect.

Configure Mobile Data Service logging

By default, the Mobile Data Service logs are stored in the same location as other component logs. See " Change global logging settings" on page 11 for more information.

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **Mobile Data Services** tab, click **Edit Properties**.
3. Click **Logs**.
4. Set the following options:

Option	Description
SRP logging enabled	Select **True** to record activity in the log files at the SRP network layer.
IPPP logging enabled	Select **True** to record activity in the log files at the IPPP network layer.
UDP logging enabled	Select **True** to record activity in the log files at the UDP network layer.
GME logging enabled	Select **True** to record activity in the log files at the GME network layer.

Option	Description
HTTP logging enabled	Select **True** to record the HTTP headers of the response message in the log files. Response messages are sent from the web server when users retrieve content from the Internet and corporate intranet.
Verbose HTTP logging enabled	Select **True** to record the HTTP headers and the body of the response message in the log files. Response messages are sent from the web server when users retrieve content from the Internet and corporate intranet.
TLS logging enabled	Select **True** to record activity in the log files when sending data that is encrypted to and from the origin web server using Transport Layer Security (TLS).
OCSP logging enabled	Select **True** to record activity in the log files when retrieving the certificate revocation status from the Online Certificate Status Protocol (OCSP) server.
LDAP logging enabled	Select **True** to record activity in the log files for requests to access a user profile or certificate from the LDAP directory.
CRL logging enabled	Select **True** to record activity in the log files when downloading certificate revocation lists from the CRL servers.

5. Double-click **Logs**.
6. Click **Destination**.
7. Specify the logging format and location.

Log location	Option	Description
File	Log Level	Defines the level of logging to write to the debug log file. • **Event**: Events defined as 0; indicates a critical error. • **Error**: Events defined as level 1; indicates an error that is lower priority than an event message. • **Warning**: Events defined as level 2 or lower; indicates an important event that is not an error. • **Information**: Events defined as level 3 or lower; used to monitor normal message flow. • **Debug**: All events; provides additional details for debugging. **Note:** Events that are written to the log begin with a five-digit number (for example, 30126). The first digit represents the logging level of the event.
	Location	The directory location of the Mobile Data Service log files.
	Log Timer Interval	Specifies the interval, in minutes, that messages are logged to the Mobile Data Service log files.
UDP	Log Level	Defines the level of logging to write to the debug log file. • **Event**: Events defined as 0; indicates a critical error. • **Error**: Events defined as level 1; indicates an error that is lower priority than an event message. • **Warning**: Events defined as level 2 or lower; indicates an important event that is not an error. • **Information**: Events defined as level 3 or lower; used to monitor normal message flow. • **Debug**: All events; provides additional details for debugging.
	Location	The BlackBerry Enterprise Server SNMP agent that the Mobile Data Service connects to send a UDP log message. The port used to connect to the SNMP agent is specified in the following registry path: HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BlackBerrySNMPAgent\Parameters\UDPPort. Change the location specified in the registry path by typing **hostname:port** in the **Location** field.

Log location	Option	Description
TCP	Log Level	Defines the level of logging to write to the debug log file. • **Event**: Events defined as 0; indicates a critical error. • **Error**: Events defined as level 1; indicates an error that is lower priority than an event message. • **Warning**: Events defined as level 2 or lower; indicates an important event that is not an error. • **Information**: Events defined as level 3 or lower; used to monitor normal message flow. • **Debug**: All events; provides additional details for debugging.
	Location	The location that the Mobile Data Service connects to send the TCP log message; use the format "hostname:port".
EventLog	Log Level	Defines the level of logging to write to the debug log file. • **Event**: Events defined as 0; indicates a critical error. • **Error**: Events defined as level 1; indicates an error that is lower priority than an event message. • **Warning**: Events defined as level 2 or lower; indicates an important event that is not an error. • **Information**: Events defined as level 3 or lower; used to monitor normal message flow. • **Debug**: All events; provides additional details for debugging.

8. Click **OK**.

Customizing Mobile Data Service statistics

Configure how often the Mobile Data Service calculates and stores statistics in the database.

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **Mobile Data Services** tab, click **Edit Properties**.
3. Click **Stats.**
4. Set the following options:

Option	Description
Size of History	The number of days that statistics are stored in the database.
Statistical Interval	The frequency, in minutes, that the Mobile Data Service calculates all statistics. See " View statistics" on page 17 for more information.
History Log Save Interval	The frequency, in minutes, that the Mobile Data Service saves statistics to the database.
History Log Size in Memory	The number of hours that statistics are stored in the database.
Backfill on Startup Enabled	Select **True** to access statistics from the last 24 hours after the Mobile Data Service is restarted.

2

Daily monitoring

Viewing statistics and settings

You can view statistics and settings on the server and user level, and for the Mobile Data Service.

View server statistics

These statistics are collected automatically when the BlackBerry Enterprise Server is first started, and are collected until the BlackBerry Enterprise Server is restarted, or the statistics are purged by an administrator.

1. In the BlackBerry Manager, in the left pane, click **BlackBerry Domain**.
2. On the **Server list** tab, click a server. A list of properties and statistics displays in the lower pane.

Option	Description
Service Name	The mail server monitored by the BlackBerry Enterprise Server, displayed in canonical format.
Number of Users	The number of users on the BlackBerry Enterprise Server.
Messages Forwarded	The total number of messages forwarded to BlackBerry Wireless Handhelds™. This total depends on the filters set at the user or administrator level.
Messages Sent	The total number of messages sent from handhelds.
Messages Pending	The total number of messages currently queued for delivery to handhelds.
Messages Filtered	The total number of messages to which the BlackBerry Enterprise Server applied filters and therefore did not forward to handhelds.
Messages Expired	The total number of messages that timed out without being forwarded to the user's handheld (for example, if the user is not in a wireless network coverage area). **Note:** Messages time out after 7 days of non-delivery to the handheld.
Messages Failed	The total number of messages that were not received by handhelds.
External Services (MDS) Enabled	Specifies whether the Mobile Data Service is enabled and running on the server.
Wireless Email Reconciliation Enabled	Specifies whether wireless email reconciliation is enabled on the server.
SRP Status	Specifies whether the BlackBerry Enterprise Server is connected successfully to the wireless network.
PID	The unique identifier of the BlackBerry Dispatcher.
Host Name	The name of the computer on which the BlackBerry Enterprise Server is installed.

View user statistics

1. In the BlackBerry Manager, in the left pane, click a server.

2. On the **User List** tab, click a user.

Option	Description
Status	The general status of email redirection for the user. • **Initializing**: Email redirection is starting. • **Running**: Email redirection is active. • **In-cradle**: email redirection is suspended while the handheld is connected to the desktop computer.
Messages Forwarded	The total number of messages forwarded to the user's handheld. This total depends on the filters that are set at the user or administrator level.
Messages Sent	The total number of messages that were sent from the user's handheld.
Messages Pending	The total number of messages that are currently queued for delivery to the user's handheld.
Messages Filtered	The total number of messages to which the BlackBerry Enterprise Server applied filters and therefore did not forward to the user's handheld.
Messages Expired	The total number of messages that timed out without being forwarded to the user's handheld (for example, if the user is not in a wireless network coverage area). **Note:** Messages time out after 7 days of non-delivery to the handheld.
Last Forward Time	The date and time that the last message (email or calendar) was forwarded to the user's handheld.
Last Sent Time	The date and time that the last message (email or calendar) was sent to the user's handheld.
Last Contact Time	The date and time that the server last made contact with the handheld.
Last Result	The last result that was returned for the user.

View Mobile Data Service statistics

1. In the BlackBerry Manager, in the left pane, click a server.
2. Click the **Mobile Data Services** tab. A list of properties and statistics displays.

Option	Description
Status	Specifies whether the Mobile Data Service is started.
Is push server	Specifies whether the BlackBerry Enterprise Server is enabled as the Mobile Data Service centralized push server.
Authorization exceptions	The number of requests that resulted in an error during authorization with the Mobile Data Service.
Authorization failures	The number of requests that the Mobile Data Service failed to authorize.
Authorization successes	The number of requests that the Mobile Data Service successfully authorized.
Connections truncated	The number of handheld-initiated connections requesting content that exceeded the maximum allowable size per connection.
Device authentication failures	The number of handheld-initiated connections that the Mobile Data Service failed to authenticate.
Max content size of device connections (KB)	The maximum size (in bytes) of Mobile Data Service data packets that were requested from handhelds.
Total content side of device connections (KB)	The total size (in bytes) of Mobile Data Service data packets that were requested from handhelds.
Number of packets from device connections	The number of packets that were sent from the handheld to the Mobile Data Service.
Device Connections	The number of handheld-initiated connections that the Mobile Data Service received.
Max content size of push connections (KB)	The maximum packet size, in bytes, that the Mobile Data Service received from push application servers.
Total content size of push connections (KB)	The total packet size, in bytes, that the Mobile Data Service received from push application servers.

Option	Description
Number of packets from push connections	The number of packets that are sent from the push application server to the Mobile Data Service.
Push connections	The number of push server connections that the Mobile Data Service received.

View Mobile Data Service statistics in a browser

View Mobile Data Service status, statistics and errors in a handheld or desktop browser application. If the Mobile Data Service is not running or is listening on a port that is different from the one specified, no results display.

View status

1. On your handheld or desktop, open a browser.
2. In the **Address** field, type http://*MDS computer*:*web server port*/admin/common where *web server port* is the port set in the Web Server Listen Port parameter in the Mobile Data Service general properties. The default value is 8080. A list of properties displays:

Option	Description
MDS name	The instance name of the Mobile Data Service.
Database connection status	The connection URL used to establish a connection to the database.
MDS started on	The date and time that the Mobile Data Service last started.
SRP connection status	The SRP ID for a successful connection to the BlackBerry Enterprise Server.
Last SRP connection attempt	The date and time that the Mobile Data Service last attempted to connect to the BlackBerry Enterprise Server.
MDS URL	The URL of the Mobile Data Service administration web page.

View statistics

1. On your handheld or desktop, open a browser.
2. In the **Address** field, type http://*MDS computer*:*web server port*/admin/statistics/Statistics where *web server port* is the port set in the Web Server Listen Port parameter in the Mobile Data Service general properties. The default value is 8080. A list of properties and statistics displays.

Note: The statistics and errors display in three columns: the first column displays results for the last hour, the second column displays results for the last 6 hours, and the third column displays results for the last 24 hours

Option	Description
Authorization exception	The number of requests that resulted in an error during authorization with the Mobile Data Service.
Authorization failure	The number of requests that the Mobile Data Service failed to authorize.
Authorization success	The number of requests that the Mobile Data Service successfully authorized.
Device Connections timed out	The number of handheld-initiated connections that were terminated when a connection timeout was reached.
Device Connections truncated	The number of handheld-initiated connections requesting content that exceed the maximum allowable size per connection.
Device authentication failure	The number of handheld-initiated connections that the Mobile Data Service failed to authenticate.
Max content size of device connections (KB)	The maximum size (in bytes) of Mobile Data Service data packets that were requested from handhelds.
Total content size of device connections (KB)	The total size (in bytes) of Mobile Data Service data packets that were requested from handhelds.

Option	Description
Device connections: MAX latency (msecs)	The maximum time, in milliseconds, that is required to send data packets from the handheld to the Mobile Data Service.
Device connections: AVG latency (msecs)	Average time, in milliseconds, that is required to send data packets from the handheld to the Mobile Data Service.
Number of packets from device connections	The number of packets that were sent from the handheld to the Mobile Data Service.
Device connections	The number of handheld-initiated connections that the Mobile Data Service received.
HTTP Errors: 400, 404, 500	The number of HTTP errors created when retrieving content from the Internet or intranet.
Max content size of push connections (KB)	The maximum packet size, in bytes, that the Mobile Data Service received from push application servers.
Total content size of push connections (KB)	The total packet size, in bytes, that the Mobile Data Service received from push application servers.
Number of packets from push connections	The number of packets that are sent from the push application server to the Mobile Data Service.
Push connections	The number of push server connections that the Mobile Data Service received.
Current device requests queue size	The total packet size, in bytes, for handheld-initiated connections.
SRP Connections failed	The number of connections from the origin web server or handheld to the BlackBerry Enterprise Server that failed.
SRP Connections succeeded	The number of connections from the origin web server or handheld to the BlackBerry Enterprise Server that succeeded.
SRP Invalid packet	The number of invalid packets that the Mobile Data Service received.
SRP Refused packet	Number of packets that the Mobile Data Service refused.

View custom statistics

1. On your handheld or desktop, open a browser.
2. In the **Address** field, type http://*MDS computer*.*web server port*/admin/statistics/Statistics, where *web server port* is the port set in the Web Server Listen Port parameter in the Mobile Data Service general properties. The default value is 8080.
3. Click **Customize statistics**.
4. In the **Select reference time** section, define the time to view statistics for. The current date and time is the default.
5. Select **From Date** to view the statistics from the specified date and time, and the set the hour, minute, and am/pm values.
6. In the **Select intervals** section, select the intervals before the reference time to view statistics for.
7. Click **Add interval(s)**. The intervals appear in the Current display intervals table.
8. In the **Select variables** section, select the statistics to view. See " View statistics" on page 17 for more information.
9. Perform one of the following actions:

Action	Procedure
View selected statistics.	▸ Click **Add selected statistic(s)**.
View all statistics.	▸ Click **Add all statistics**.

10. At the top of the page, click **Statistics**. The selected statistics and their corresponding interval values display.

Export user statistics to a text file

You can export Display Name, PIN, Enabled State, Forwarded, Sent from Handheld, Pending to Handheld, Expired, Filtered, and Mailbox statistics for a specific user.

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.

Tip: Press CTRL to select multiple users at the same time.

3. In the lower pane, click **Service Control and Customization**.
4. Click **Export Stats to File.**
5. Specify a location and file name.
6. Click **Save**.
7. Perform one of the following actions:

Action	Procedure
Retain user statistics after the export is complete.	▸ Click **No**.
Clear user statistics after the export is complete.	▸ Click **Yes**.

8. Click **OK.**

Clear statistics

1. In the BlackBerry Manager, in the left pane, click a server.
2. Perform one of the following actions:

Action	Procedure
Clear server statistics.	1. On the **Server Configuration** tab, click **Service Control and Customization**. 2. Click **Clear Statistics**. 3. Click **OK**.
Clear user statistics.	1. On the User List tab, click a user. 2. In the lower pane, click **Service Control and Customization.** 3. Click **Clear Statistics**. 4. Click **OK**.
Clear Mobile Data Service statistics.	▸ On the **Mobile Data Service** tab, click **Clear Statistics**.

Configuring notifications using BESAlert

BESAlert watches the Windows® NT Event log and sends defined users a copy of events whenever an error, warning, or information event is recorded. You must configure these settings on each BlackBerry Enterprise Server.

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **Server Configuration** tab, click **Edit Properties**.

3. Click **BESAlert**, and perform the following actions:

Action	Procedure
Define the SMTP computer through which notifications are sent.	▸ Type the SMTP Hostname of your gateway in DNS format (for example, smtp.CompanyName.com).
Define the SMTP account from which notifications are sent.	▸ If required by your SMTP server, type the SMTP account name (for example, the NT login name that you use to log into your computer).
Define the SMTP address from which notifications are sent.	▸ Type the SMTP Address from which to send and receive replies to alert messages (for example, BESAlerts@CompanyName.com).
Define the level at which events are monitored.	▸ From the **Event Level** drop-down list, select one of the following options: • **Error**: All level 1 events (error) • **Warning**: All level 2 events and lower (warning and error) • **Informational**: All level 3 events and lower (informational, warning, and error)

4. Double-click **User Notification**.
5. Click **New**.
6. Perform the following actions:

Action	Procedure
Define who to send the notifications to.	▸ Type the recipient's User name.
Define the level at which notifications are sent.	▸ From the **Event Level** drop-down list, select one of the following options: • **Default**: The event level defined for BESAlert. • **Error**: All level 1 events (error) • **Warning**: All level 2 events and lower (warning and error) • **Informational**: All level 3 events and lower (informational, warning, and error) **Note:** If you define a value other than **Default**, this setting overrides the default event level defined for BESAlert.
Define the SMTP address to which notifications are sent.	▸ Type the email address to which notifications are sent.
Define the computers on which console message notifications display.	▸ Type the console on which to display notifications.

7. Click **OK**.

Monitoring components using system logging

System logging (syslog) is a standard protocol for monitoring servers on a network. If events occur, they are transferred using User Datagram Protocol (UDP) to the syslog tool, where information is logged and console or user notifications can be sent.

Use syslog for additional monitoring of all BlackBerry Enterprise Server components, except for the BlackBerry Attachment Service and the Mobile Data Service. Syslog cannot be configured for the Attachment Service or the Mobile Data Service. Do not use syslog tools on the same computer that the BlackBerry Enterprise Server is installed on.

1. On an alternate machine, install your choice of third-party syslog tool.
2. On the BlackBerry Enterprise Server, open **regedit.exe**.

3. In the left pane, browse to **HKEY_LOCAL_MACHINE\Software\Research In Motion\BlackBerry Enterprise Server.**
4. Under **Logging Info**, select the component you want to monitor, and add or modify these values:

Value	Type	Action
<Default>	DWORD	▸ Define UDP port on which syslog will listen for events. Default is port 514. **Note:** This is an optional step. You can configure your syslog tool to listen on port 514 and bypass this step.
SysLogHost	String	▸ Type the IP address and port of the syslog tool (for example, 10.10.10.10:4070). If other sysloghost information is already configured for the component, add the syslog tool to the end of the string, separated by a comma.
EventLogLevel	DWORD	▸ Define the log level at which you want events to be communicated to the syslog tool, from these options: • 1 = error • 2 = warning • 3 = informational • 4 = debug • 5 = other **Note:** By default, EventLogLevel for each component is set to 2.

5. Repeat for remaining component(s).

Viewing logs

Log location

Logs are located in the root log directory that you defined during the installation process. The default location is C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs\. In the root log directory, files are then organized into daily folders. See “Change global logging settings” on page 11 for more information.

File names

Log file names are created using the default format of *<ServerName_Identifier_Instance_YYYYMMDD_Log#.txt>*. See " Customizing logging configuration" on page 11 for more information.

Component name	Identifier
BlackBerry Attachment Service	ASRV
BlackBerry Attachment Conversion	ACNV
BlackBerry Dispatcher	DISP
BlackBerry Alert	ALRT
BlackBerry Messaging Agent	MAGT
BlackBerry Synchronization Connector	CONN
BlackBerry Manager	MNGR
BlackBerry Router	ROUT

Component name	Identifier
BlackBerry Controller	CTRL
BlackBerry Policy Service	POLC
BlackBerry Mobile Data Service	MDAT
BlackBerry Synchronization Service	SYNC
Backup Connector	CBCK
Management Connector	CMNG
Notes Connector	CNTS

Default log levels

Log levels are defined automatically during the installation process. See " Customizing logging configuration" on page 11 for more information.

Component name	Default log level
BlackBerry Attachment Service	1
BlackBerry Attachment Conversion	1
BlackBerry Dispatcher	3
BlackBerry Messaging Agent	4
BlackBerry Manager	3
BlackBerry Router	3
BlackBerry Controller	4
BlackBerry Policy Service	4
BlackBerry Synchronization Service	4
Notes Connector	4
Backup Connector	4
Management Connector	4

Monitoring system performance

Monitoring system performance is key to understanding the impact of BlackBerry user growth and of specific BlackBerry components on hardware resources.

Setting performance monitoring counters

Use the counters included in the BlackBerry Enterprise Server software to monitor statistics for all active users with standard performance monitoring tools, such as the Windows Performance monitor. These statistics reflect server activity since the last time that the BlackBerry Enterprise Server restarted.

Warning: Performance monitoring tools cannot be running on the same server as the BlackBerry Controller.

Choose counters

1. On a remote server, in the taskbar, click **Start > Programs > Administrative Tools > Performance**.
2. In the left pane, click the **System Monitor** object.
3. Click the **+** icon.

4. In the **Select counters from this computer** drop-down list, set the name of the BlackBerry Enterprise Server to monitor.
5. From the drop-down list, select a performance object.
6. Modify the desired values.

Note: If the BlackBerry Enterprise Server is running, and the BlackBerry-specific counters are not visible in the list, you might need to re-install or repair the .dll file. See " Repairing the registration of the performance monitor file using the BBPerfmoninstall tool" on page 66 for more information.

Performance object	Counter	Action
BlackBerry Server	Connection State	1. Select the **All counters** option. 2. Click **Add**.
	Messages Expired	
	Messages Filtered	
	Messages Pending	
	Messages Forwarded	
	Messages Forwarded/min	
	Messages Sent	
	Messages Sent/min	
Process	%Processor Time	1. Select the **Select counters from list** option. 2. In the list, select **%Processor Time**. 3. Select the **Select instances from list** option. 4. In the list, select the following instances: • BBAttachServer • BBConvert(#1-3) • BlackBerryDispa • bmds • BlackBerrySyncS • NBES • Nserver 5. Click **Add**. 6. Repeat for the remaining recommended process counters. **Note:** These process instances are the ones most likely to impact resources. Other BlackBerry processes can be monitored if desired.
	Network usage	
	Memory usage	

7. Click **Close**.

Note: A session begins when the BlackBerry Enterprise Server starts.

The counters listed in the preceding table include only messages that are routed through the BlackBerry Enterprise Server. They do not include PIN, SMS, and other messages that are not routed through the server.

Enable logging

Enable logging on performance monitoring counters for one business day per week. Use this information to analyze the impact of additional users or the implementation of new features (for example, Mobile Data Service or Attachment Service) on hardware resources.

Viewing statistics using SNMP

You can use Simple Network Management Protocol (SNMP) to assess the configuration and status of your BlackBerry Enterprise Server and its users.

The Management Information Base (MIB) for the BlackBerry Enterprise Server is BlackBerryServer.mib, which is located in C:\Program Files\Research In Motion\BlackBerry Enterprise Server\ on the computer on which the BlackBerry Enterprise Server is installed.

Note: You must compile and register the .mib file to view descriptive names for MIB variables; otherwise, the SNMP monitor tool that you use displays the Object Identifiers (OIDs) only.

An OID is a sequence of integers that uniquely identifies a value by defining the path to that value through a registration tree. All BlackBerry Enterprise Server SNMP OIDs begin with `1.3.6.1.4.1.3530.5`, and all traps begin with `1.3.6.1.4.1.3530.5.9`. Each value integer is distinguished by a suffix, such as `25.1.1`.

Requirements

Viewing server redirection statistics in an SNMP browser requires the following:

- a running SNMP service
- an SNMP browser

Supported functions

Option	Description
Get	Retrieves a specified value that is stored in a table on the server. For example, a `Get` request for the MIB variable `besTotMsgsPending` returns the total number of messages that are queued for delivery to BlackBerry handhelds on the BlackBerry Enterprise Server.
Get Next	Fetches the next sequential MIB variable after the previous request.
Walk	Extracts all BlackBerry Enterprise Server and user information, with two exceptions: • To `WALK` the BlackBerry Enterprise Server Mail Server Health container, use its full root (`1.3.6.1.4.1.3530.5.26`) explicitly. • To `WALK` the BlackBerry Enterprise Server User Health container, use its full root (`1.3.6.1.4.1.3530.5.30`) explicitly.
Trap	Sends messages triggered by defined events; messages are sent from the BlackBerry Enterprise Server to the client computer.

Recommended values to monitor

To begin using SNMP monitoring, start with the following values. See " Appendix C: SNMP Values" on page 53 for more information on additional values.

Category	Value	Description	Object Identifier
System Health	besSysHealthSrpReconnects Fail	The number of times that the BlackBerry Enterprise Server has attempted, but failed, to connect to wireless network since startup.	1.3.6.1.4.1.3530.5.25.1.13
	besSysHealthSrpTotalSecNot Connected	The total number of seconds since startup that the BlackBerry Enterprise Server has not been connected to the wireless network.	1.3.6.1.4.1.3530.5.25.1.14
	besSysHealthSrpLastError Text	The error text associated with the last failed connection attempt.	1.3.6.1.4.1.3530.5.25.1.15
	besSysHealthMsgFilteredBy Global	The total number of messages to which the BlackBerry Enterprise Server applied global filters and did not forward to handhelds since startup.	1.3.6.1.4.1.3530.5.25.1.24
	besSysHealthMsgPending	The total number of messages that are pending to be delivered to handhelds.	1.3.6.1.4.1.3530.5.25.1.25
	besSysHealthMsgErrors	The total number of messages that were non-deliverable to handhelds because of an error.	1.3.6.1.4.1.3530.5.25.1.27

Category	Value	Description	Object Identifier
User Health	besUserHealthLastErrorText	The error text that was returned the last time an operation for this user failed.	1.3.6.1.4.1.3530.5.30.1.10
	besUserHealthLastErrorTime	The date and time of the last error for this user.	1.3.6.1.4.1.3530.5.30.1.11
	besUserHealthMsgPending	The total number of messages that are pending to be delivered to the user's handheld.	1.3.6.1.4.1.3530.5.30.1.44
BlackBerry Enterprise Server events	besSRPConnectEvent	Indicates whether the BlackBerry Enterprise Server is connected to the wireless network, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.1 (Connected) and 1.3.6.1.4.1.3530.9.2 (Disconnected)
	besHungThreadEvent	Indicates that a BlackBerry Enterprise Server non-responsive thread has been detected.	1.3.6.1.4.1.3530.9.3
	besMDStoBESConnectionEvent	Indicates whether the Mobile Data Service is connected to the BlackBerry Enterprise Server, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.7 (Connected) and 1.3.6.1.4.1.3530.9.8 (Disconnected)
	besMDSStartStopEvent	Indicates whether the Mobile Data Service is started, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.11 (Started) or 1.3.6.1.4.1.3530.9.12 (Stopped)
	besMDStoDBConnectionEvent	Indicates whether the Mobile Data Service is connected to the database, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.13 (Connected) or 1.3.6.1.4.1.3530.9.14 (Disconnected)
	besCriticalEvent	Indicates that an event has been logged with a 1*xxxx* or 5*xxxx* (critical) event ID.	1.3.6.1.4.1.3530.9.21

3

Preventive maintenance

Documenting the environment

Take the time to document your environment so that information is available in a disaster recovery scenario.

Data	Details
Server settings	• host names • Microsoft Windows Server™ names • IP addresses
Firewall settings	• connection details required by a BlackBerry Router in the DMZ • proxy configurations used by the BlackBerry Enterprise Server
BlackBerry wireless network connection credentials	• SRP address • SRP identifier • SRP authentication key
IBM® Lotus® Domino® environment	• names of all servers that contain BlackBerry users • approximate number of BlackBerry users on each mail server
BlackBerry Enterprise Server implementation	• whether the Attachment Service is on a separate server • which BlackBerry Enterprise Server is the Mobile Data Service Push server • customized registry settings (for example, BESAlert, BlackBerry Controller) • IT policy settings

Best practices

Manage log file storage

You should retain only seven days of log files, depending on the logging levels used. Store older log files on a different computer, or include them as part of your daily backup. Use the Debug Log Maximum Daily File Age setting to delete files older than seven days. See " Change component logging settings" on page 12 for more information.

Schedule regular database compaction

You should regularly compact all BlackBerry-related databases using the IBM Lotus Domino server Compact utility using the following settings:

Option	Description
"-B" option	• Recovers unused space. • Helps maintain database integrity. • Reduces on-disk file size. • Allows access to the database while the Compact program runs. **Note:** If the IBM Lotus Domino server is transaction logged, you should perform a full database backup soon after the Compact –B command is run.
"BES" parameter	• Compacts all databases in the Lotus/Domino/Data/BES directory.
Interval	• Once a day is ideal. • Preferably during low message traffic times. **Note:** If the full database backup required to support Transaction Logging (when the –B parameter is used) is too difficult to manage on a daily basis, Compact –B can be run weekly instead.

Remove old state databases

When a user is deleted from the BlackBerry Enterprise Server, you should also delete the user's state database. Failure to clean up these unneeded state databases increases the server resources needed for backup, routine maintenance, and server disk space.

Keep state database pruning enabled

The state database pruning feature keeps user state database size down, reducing server resource use. This feature is enabled by default in BlackBerry Enterprise Server version 4.0 and can be customized. See the *BlackBerry Enterprise Server Administration Guide* for more information.

Design a disaster recovery program

Method	Pros	Cons
Backup/Restore	• Can also be used to migrate the BlackBerry Enterprise Server onto new hardware.	• Very resource-intensive. • Data is only as current as the last backup. • Users might have some documents orphaned
Standby server	• Kept up-to-date using replication. • Allows for a more up-to-date restore than backup. • Useful for disaster recovery utilizing a remote site.	• Requires many steps to get up and running, and is dependent on the last replication time. • Essentially the same approach as clustering, without its advantages.
Clustering	• Minimal intervention needed to failover.	• Requires additional license(s) to create the cluster.

Backing up data

Backing up the BlackBerry Enterprise Server

You should regularly perform a full system backup so that you can recover data in the event of system failure on the computer on which the BlackBerry Enterprise Server Software is installed.

Note: To successfully back up the operational databases while the BlackBerry Enterprise Server add-in task is active and the IBM Lotus Domino server is running, an appropriate backup agent supporting the IBM Lotus Domino backup and recovery application program interface (API), or supported third-party open file management software is required. If this is not available in the environment, the BlackBerry Enterprise Server and IBM Lotus Domino server services must be stopped before the initiation of the backup, and then restarted upon completion to maintain the integrity of the database backup.

It is critical that you back up the following data:

Data	Location
NBES.exe	Lotus\Domino
notes.ini	Lotus\Domino
BlackBerry Enterprise Server database templates: • BBProfiles.ntf • BBSD.ntf	Lotus\Domino\Data\BES
BlackBerry Enterprise Server databases: • BlackBerryProfiles.nsf • State\...	Lotus\Domino\Data\BES
Server ID file	Lotus\Domino\Data
BlackBerry Enterprise Server registry settings	HKLM\SOFTWARE\Research In Motion
Log files	By default, C:\Program Files\Research In Motion\BlackBerry Enterprise Server\Logs\ **Note:** If the default location was not used, use the location defined in the following registry value: HKLM\SOFTWARE\Research In Motion\BlackBerry Enterprise Server\LoggingInfo\LogRoot
Attachment Service executables and supporting files	By default, C:\Program Files\Research In Motion\BlackBerry Enterprise Server\AttachServer

Backing up the configuration database

The configuration database is a critical part of BlackBerry Enterprise Server operations. Server and user administration, Mobile Data Service push, and PIM synchronization all depend on the information stored in the configuration database. See the *BlackBerry Enterprise Server Troubleshooting Guide* for more information on the impact of component failure.

You should regularly perform a full backup of the configuration database so that you can recover data in the event of a failure.

Backing up the configuration database using BlackBerry Database Backup tool

If you are using MSDE 2000 for your configuration database, you can use the BlackBerry Database Backup tool provided with the BlackBerry Enterprise Server software to perform a full backup of the database.

1. On the server where the configuration database is located, at the command prompt, switch to the Tools directory on the installation CD.

   Tip: You can copy this tool to your database server.

2. Type **BlackBerryDBBackup.exe**, followed by the parameters needed to configure the backup, in the following order:

   ```
   BlackBerryDBBackup.exe -d [-f] [-S] [-E | -U -P] [-p] [-?]
   ```

   See " Backing up the configuration database using the BlackBerry Database Backup tool" on page 61 for more information.

3. Press **Enter**.

By default, the backup file is named *<database name><YYYYMMDDHHMMSS>.bak*

Backing up the configuration database using SQL

If you are using SQL 2000 for your configuration database, you can use the tools provided with that software to perform backups.

Preparing to use alternate servers

You can minimize the impact of service or hardware failure by preparing alternate servers as failovers.

Create a server cluster

Note: IBM Lotus Domino clustering is not supported for load balancing.

Research In Motion recommend using the event-based replication of IBM Lotus Domino clustering to create the most up-to-date replicas of BlackBerry Profiles and user state databases on your standby server. This disaster recovery method can also be used to provide coverage during maintenance windows.

Action	Procedure
Create a cluster.	▸ Create an IBM Lotus Domino cluster, with the server already running the BlackBerry Enterprise Server configured as the primary cluster member.
Install the BlackBerry Enterprise Server.	1. Install the BlackBerry Enterprise Server on the secondary cluster member using the same version, including service pack and hot fix, as the primary cluster member. See the *BlackBerry Enterprise Server Installation Guide* for more information. 2. During configuration, use the same SRP identifier as the primary cluster member. 3. At the end of the configuration wizard, clear the **Start Services** check box. 4. If prompted, do not restart the server. **Warning:** Do not start this BlackBerry Enterprise Server. You cannot have two simultaneous connections to the wireless network using the same SRP identifier. Attempts to do so disable the SRP identifier.
Set the services to manual.	1. On the secondary cluster member, in the Windows Services pane, right-click **BlackBerry Alert**, and then click **Properties**. 2. Set the startup type to **Manual**, and then click **OK**. 3. Repeat steps 1 to 2 for all BlackBerry services.
Disable the BlackBerry Enterprise Server add-in task.	1. On the secondary cluster member, open the **notes.ini** file. 2. Remove "BES" from the server tasks entry (ServerTasks=). 3. Save and close the file.

Action	Procedure
Configure access.	▶ Deny users access to the secondary cluster member to prevent replication and, or save conflicts.
Create replicas.	1. Create replicas of the primary cluster member's BlackBerry-related databases on the secondary cluster member. These databases include the following: • BlackBerry Profiles database: Lotus\Domino\Data\BES\BBProfiles.nsf • BlackBerry state databases: Lotus\Domino\Data\BES\State\... 2. Enable the replicas for clustering 3. Configure a secondary replication cycle for all the databases listed in step 1, with an interval of 15 minutes to keep the databases current. **Note:** Replicas of BlackBerry state databases must be updated using a utility or agent, as users are added or removed.

Create a standby server

You can also use time-based replication to create replicas of the BlackBerry Profiles and user state databases on a standby server.

Action	Procedure
Install the BlackBerry Enterprise Server.	1. Install the BlackBerry Enterprise Server on the standby server using the same version, including service pack and hot fix, as the primary server. See the *BlackBerry Enterprise Server Installation Guide* for more information. 2. During configuration, use the same SRP identifier as the primary server. 3. At the end of the configuration wizard, clear the **Start Services** check box. 4. If prompted, do not restart the server. **Warning:** Do not start this BlackBerry Enterprise Server. You cannot have two simultaneous connections to the wireless network using the same SRP identifier. Attempts to do so disable the SRP identifier.
Set the services to manual.	1. On the standby server, in the Windows Services pane, right-click **BlackBerry Alert**, and then click **Properties**. 2. Set startup type to **Manual**, and then click **OK**. 3. Repeat steps 1 to 2 for all BlackBerry services.
Disable the BlackBerry Enterprise Server add-in task.	1. On the standby server, open the **notes.ini** file. 2. Remove "BES" from the server tasks entry (ServerTasks=). 3. Save and close the file.
Configure server access.	▶ Deny users access to the standby server to prevent replication and, or save conflicts.
Create replicas.	1. Create replicas of the primary server's BlackBerry-related databases on the secondary cluster member. These databases include the following: • BlackBerry Profiles database: Lotus\Domino\Data\BES\BBProfiles.nsf • BlackBerry state databases: Lotus\Domino\Data\BES\State\... 2. Configure a replication cycle for all the databases listed in step 1, with an interval of 15 minutes to keep the databases current. **Note:** Replicas of BlackBerry state databases must be updated using a utility or agent, as users are added or removed.
Copy server data.	▶ Copy the primary server.id to the standby server.

Create a database cluster and perform replication using SQL

Note: Database clustering is not supported for load balancing.

If you are using SQL 2000 for your configuration database, you can use the tools provided with the software to create a cluster or perform one-way replication to a standby server.

4

Restoring data and functionality

Moving users to another BlackBerry Enterprise Server

If one of your BlackBerry Enterprise Servers becomes unavailable, you can move users to another BlackBerry Enterprise Server before starting any recovery or failover process.

Perform a sourceless move

Under normal conditions, the Move User task replicates a copy of the user's state database from the source server to the destination server. When the source server is unavailable, users cannot be moved unless state database replicas are already present on the destination server. See " Preparing to use alternate servers" on page 30 for more information.

1. In a remote BlackBerry Manager, or the BlackBerry Manager on the destination server, in the left pane, click the source server.
2. On the **User List** tab, click a user.

Tip: Press CTRL to select multiple users at the same time.

3. In the lower pane, in **Common**, click **Move User**.

Tip: You can also drag-and-drop users into the destination server.

4. In the list, click the destination server.
5. Click **OK**.

After the user's state database is located on the destination server, the BlackBerry Profiles database is updated with a record for the user, which is created from data stored in the configuration database. New service books are sent to the user's handheld, so no reactivation is required.

Note: Handhelds must have Handheld Software version 4.0 for Java™-based handhelds or Handheld Software version 2.7 for C++-based handhelds installed to receive the new service books without reactivating the handheld. Users with earlier versioned handhelds must connect their handhelds to their computers for the changes to take effect.

Restoring the BlackBerry Enterprise Server

These recovery methods use data made available through backup or replication. See " Backing up data" on page 29 or " Preparing to use alternate servers" on page 30 for more information.

Switch to a secondary cluster member

Action	Procedure
Disable the BlackBerry Enterprise Server add-in task on the primary cluster member.	1. If possible, on the primary cluster member, open the **notes.ini** file. 2. Remove "BES" from the server tasks entry (ServerTasks=). 3. Save and close the file.
Configure access to cluster members.	1. Allow users access to the secondary cluster member. 2. If possible, deny users access to the primary cluster member to prevent replication and, or save conflicts.
Enable the BlackBerry Enterprise Server add-in task on the secondary cluster member.	1. On the secondary cluster member, the **notes.ini** file. 2. Add "BES" from the server tasks entry (ServerTasks=). 3. Save and close the file.
Set the services to automatic on the secondary cluster member.	1. On the secondary cluster member, in the Windows Services pane, right-click **BlackBerry Alert**, and then click **Properties**. 2. Set the startup type to **Automatic**, and then click **OK**. 3. Repeat steps 1 to 2 for all BlackBerry services.
Start the services on the secondary cluster member.	▸ Start the services in the following order: • BlackBerry Controller • BlackBerry Router • BlackBerry Dispatcher • All remaining services

Switch to standby server

Action	Procedure
Disable the BlackBerry Enterprise Server add-in task on the primary server.	1. If possible, on the primary server, open the **notes.ini** file. 2. Remove "BES" from the server tasks entry (ServerTasks=). 3. Save and close the file.
Configure access to the primary and standby servers.	1. Allow users access to the standby server. 2. If possible, deny users access to the primary server to prevent replication and, or save conflicts.
Switch the server identification of the standby server.	1. Change the Server.id to the standby server. 2. Verify that the server is resolvable. **Note:** If you do not change the server.id, the desktop clients must select the new BlackBerry Enterprise Server. If you do not use BlackBerry Desktop Manager in your environment, start the BlackBerry Enterprise Server add-in task.
Enable the BlackBerry Enterprise Server add-in task on the standby server.	1. On the standby server, open the **notes.ini** file. 2. Add "BES" from the server tasks entry (ServerTasks=). 3. Save and close the file.

Action	Procedure
Set the services to automatic on the standby server.	1. On the standby server, in the Windows Services pane, right-click **BlackBerry Alert**, and then click **Properties** 2. Set the startup type to **Automatic**, and then click **OK**. 3. Repeat steps 1 to 2 for all BlackBerry services.
Start the services on the standby server.	▸ On the standby server, start the services in the following order: • BlackBerry Controller • BlackBerry Router • BlackBerry Dispatcher • All remaining services
Start IBM Lotus Domino on the standby server.	▸ Start the IBM Lotus Domino server.

Restore the server from backup on a new server

Note: You can also use this procedure to migrate the BlackBerry Enterprise Server onto new hardware.

If the BlackBerry Enterprise Server that you are restoring was the Mobile Data Service push server, you can temporarily define another BlackBerry Enterprise Server as the push server. See the *BlackBerry Enterprise Server Administration Guide* for more information on defining a Mobile Data Service push server.

Action	Procedure
Create a new server that meets requirements.	▸ Restore the BlackBerry Enterprise Server on a computer that meets the following criteria: • meets the BlackBerry Enterprise Server hardware minimum requirements • has the same host name as the BlackBerry Enterprise Server that it is replacing • existing software has been removed
Restore the configuration database on the new server.	▸ If applicable, restore the configuration database from the backed up version. See " Restoring the configuration database" on page 36 for more information. **Note:** If the configuration database is on a remote server, the server must be availalble, and you must be able to connect to the server during the installation process.
Install the BlackBerry Enterprise Server on the new server.	1. Install the BlackBerry Enterprise Server on the new server using the same version, including service pack and hot fix, as the primary server. See the *BlackBerry Enterprise Server Installation Guide* for more information. 2. When completing the configuration wizard, use the same SRP identifier, SRP authentication key, and configuration database name as the primary server. 3. At the end of the configuration wizard, select the **Start Services** check box. **Warning:** If the backup BlackBerry Enterprise Server is still running, do not start the services on the new BlackBerry Enterprise Server. You cannot have two simultaneous connections to the wireless network using the same SRP identifier and key. Attempts to do so disable the SRP identifier.
Replace the IBM Lotus Domino data on the new server with the backed up version.	1. Replace the contents of the Lotus\Domino\Data\BES directory with the backed up version. See " Backing up the BlackBerry Enterprise Server" on page 29 for more information. 2. Run the following maintenance utilities: • Fixup • Updall • Compact

Action	Procedure
Start the services on the new server.	1. On the new server, start the services in the following order: • BlackBerry Controller • BlackBerry Router • BlackBerry Dispatcher • All remaining services 2. If applicable, define the sever as the Mobile Data Service push server. 3. Reconfigure any custom registry settings (for example, BESAlert or BlackBerry Controller).
Start IBM Lotus Domino on the new server.	▸ Start the IBM Lotus Domino server.

Restore BlackBerry Enterprise Server IBM Lotus Domino components

You might need to restore individual IBM Lotus Domino component databases, because of hardware failure or corruption.

Note: The BlackBerry Enterprise server users UNIDs created by the IBM Lotus Domino server to identify messages, calendar entries, and users. Existing UNIDs must be retained by using replicas or file system-level copies during backup and restore.

Action	Procedure
Restore user mail databases.	1. Restore replicas (or file system-level copies), instead of database copies. 2. After restoring the replica, ask the user to perform one of the following actions: • synchronize using the BlackBerry Desktop Manager • manually re-enable wireless calendaring **Warning:** If you fail to use a file system-level backup, users cannot reply-with-text, forward, or request more content on the handheld for messages that are in the restored mail database, and all calendar items on the handheld are no longer linked to the calendar items in IBM Lotus Notes®
Restore the IBM Lotus Domino Directory.	▸ Restore replicas (or file system-level copies), instead of database copies. **Warning:** If you fail to use a file system-level backup, users cannot send or receive messages on the handheld.

Restoring the configuration database

In the event of failure, you can recover data from a full database backup. You can also switch to a database replica or cluster member.

Restore the database using the BlackBerry Database Restore tool

If you are using MSDE 2000 for your configuration database, you can use the BlackBerry Database Restore tool provided with the BlackBerry Enterprise Server software.

1. On the server where the configuration database is being restored, at the command prompt, switch to the Tools directory on the installation CD.

   Tip: You can copy this tool to your database server.

2. Type **BlackBerryDBRestore**, followed by the parameters needed to configure the restore, in the following order:
   ```
   BlackBerryDBRestore.exe -d [-f] [-S] [-E | -U -P] [-p] [-?]
   ```
   See " Restoring the configuration database using the BlackBerry Database Restore tool" on page 62 for more information.
3. Press **Enter**.
4. After the restore is complete, use the BlackBerry Configuration Panel to connect the database to the BlackBerry Enterprise Server. See " Assign the server to another database" on page 10 for more information.

Restore the database using SQL Restore

If you are using SQL 2000 for your configuration database, you can use the tools provided with the software to perform a restore of the database.

- After the restore is complete, use the BlackBerry Configuration Panel to connect the database to the BlackBerry Enterprise Server. See " Assign the server to another database" on page 10 for more information.

Switch to a replica or alternate cluster member

If you are using SQL 2000 for your configuration database, you can use the tools provided with that software to switch to a database replica or cluster member.

Note: Database clustering is not supported for load balancing.

- Use the BlackBerry Configuration Panel to connect the configuration database to the BlackBerry Enterprise Server. See " Assign the server to another database" on page 10 for more information.

Restoring remote components

If a remote remote component fails, either connect your BlackBerry Enterprise Server to a standby server, or use the local component that is installed automatically with the BlackBerry Enterpriser Server.

Change the connection to the BlackBerry Router

When you change to a different BlackBerry Router, the BlackBerry Enterprise Server wirelessly sends updated service books, which include the routing information, to all handhelds.

Change the connection on the BlackBerry Enterprise Server

1. In the taskbar, click **Start** > **Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. On the **BlackBerry Server** tab, in the **Router Host** field, perform one of the following actions:

Action	Procedure
Connect the BlackBerry Enterprise Server to a standby remote BlackBerry Router.	▸ Type the standby server name.

Action	Procedure
Use the BlackBerry Router installed locally.	▸ Type **localhost**.

3. Click **OK**.

Change the connection using the BlackBerry Manager

Tip: Use this method to change connections on each BlackBerry Enterprise Server in a BlackBerry Domain from a single computer.

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **Server Configuration** tab, click **Edit Properties**.
3. On the **General** tab, in the **SRP Host** field, perform one of the following actions:

Action	Procedure
Connect the BlackBerry Enterprise Server to a standby remote BlackBerry Router.	▸ Type the standby server name.
Use the BlackBerry Router installed locally.	▸ Type **localhost**.

4. Click **OK**.
5. Repeat steps 1 to 4 for all BlackBerry Enterprise Servers in the BlackBerry Domain.

Change the connection to the Attachment Service

1. In the taskbar, click **Start** > **Programs > BlackBerry Enterprise Server > BlackBerry Server Configuration**.
2. On the **BlackBerry Server** tab, in the **Attachment Host** field, perform one of the following actions:

Action	Procedure
Connect the BlackBerry Enterprise Server to a standby remote Attachment Service.	▸ Type the standby server name.
Use the Attachment Service installed locally.	▸ Type **localhost**.

3. Click **OK**.

Restoring functionality to handhelds

Re-enabling a disabled handheld

If a user disables the handheld by typing an incorrect password the specified number of times, you can re-enable the handheld.

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, in the left pane, click **Ports**.
3. In the **Connection** list, click a connection.
4. Click **Load Handheld**.

Re-enabling a handheld when the password is unknown

1. In the BlackBerry Manager, in the left pane, click a server.
2. On the **User List** tab, click a user.
3. In the lower pane, click IT Admin, and then click **Set Password and Lock Handheld**.
4. In the **New Password** and **New Password Again** fields, type a password that is 4 to 14 characters long.

   Warning: Do not use special characters when you create the password. The BlackBerry handheld does not accept special characters.
5. Select the **Set Owner Information also** check box.
6. In the **Owner Name** and **Owner Information** fields, type the information.
7. Click **OK**. You must wait for the command to be delivered to the handheld.
8. Type the new password on the handheld to unlock it and restore functionality.

Returning handhelds to the factory default state

You can return a handheld to its original state by erasing all applications and data that might have been loaded on the handheld.

Warning: This procedure erases all data from the handheld. The data cannot be retrieved after the handheld is re-enabled.

1. Connect the handheld to the administration computer on which the BlackBerry Manager is installed.
2. In the BlackBerry Manager, in the left pane, click **Ports**.
3. In the **Connection** list, click a connection.
4. Click **Nuke Handheld**.
5. Click **Yes**.
6. In the left pane, click **Ports**.
7. From the **Connection** list, click a connection.
8. Click **Load Handheld**.

5

Security best practices

You can implement various security settings for the BlackBerry handheld using IT policy and wireless IT commands. See the *BlackBerry Enterprise Server Administration Guide* for more information on IT policy.

Enforcing handheld security using passwords

BlackBerry handhelds connecting to the computer using a USB port are designed to prevent replay attacks because the handheld password is not available across the USB connection. Instead, a challenge-response mechanism is used to convey the password from the BlackBerry Enterprise Server to the handheld and from the handheld to the server. In addition, the BlackBerry handheld only stores a SHA-1 hash of the password. A *hash* is a function that takes a variable-length input string and converts it into a fixed-length numerical representation of the original value. The hash is known as a one-way function because it cannot be reversed easily to reveal the password value.

Passwords that consist of a natural sequence (such as 12345) or identical characters are rejected by the handheld. By default, a user is limited to ten password attempts on the handheld. The data on the handheld is deleted after ten incorrect password attempts. If users have a current backup of the handheld data on the desktop, they can use the Backup and Restore tool in the BlackBerry Desktop Software to replace the data on the handheld. Alternatively, users can restore handheld data wirelessly. See "Restore handheld data wirelessly" on page 44 for more information.

Using an IT policy, you can force the use of a handheld password. See the *BlackBerry Enterprise Server Administration Guide* for more information on IT policies.

Set a handheld password

If a password is created and enabled on the handheld, users must type their password to view, load, and browse to data on the handheld.

- Perform the following actions:

Action	Procedure
Implement your corporate password policy on all handhelds.	▸ Set the following policy rules: • **Password Required**: set this to **TRUE**. • **Maximum Password Age**: set this to **30** (days). • **Minimum Password Length**: set this to **8** (characters). • **Password Pattern Checks**: set this to **2** (requires at least one alpha, one numeric, and one special character). • **Set Password Timeout**: set this to **5** (minutes). • **User Can Change Timeout**: set this to **FALSE**.
Erase all user data on the handheld if the user types the password incorrectly.	▸ Set the **Set Maximum Password Attempts** policy rule to **10** (incorrect passwords typed before the handheld data is erased).
Make sure that users do not use the same password repeatedly.	▸ Set the **Maximum Password History** policy rule to **10** (maximum number of previous passwords that the new password must be checked against).
Make sure that the email address specified is notified when a user types a password under duress. The user's duress password is the handheld password with the first character moved to the end (for example, "hello" for the handheld password translates into "elloh" for the duress password).	▸ In the **Duress Notification Address** policy rule, type the email address that receives notification.

Set handheld lock

- Perform the following actions:

Action	Procedure
Make sure that the handheld locks automatically (after 60 mins) regardless of user activity. Users must then type their password to access data on their handheld. **Note:** If the Periodic Challenge Time rule is set, the default 60 mins is replaced by the value specified in the Periodic Challenge Time rule.	▸ Set the **Enable Long Term Timeout** policy rule to **TRUE**.
Make sure that the user is prompted to type a password, regardless of whether the handheld is idle or is in use.	▸ Set the **Periodic Challenge Time** policy rule to **60** (minutes after which the user is prompted to enter a password).
Make sure that the handheld locks automatically when a user inserts it in the holster.	▸ Set the **Force Lock When Holstered** policy rule to **TRUE**.
Make sure that the handheld locks automatically after a period of user inactivity.	▸ Set the **Maximum Security Timeout** policy rule to **5** (mins of minutes of idle time allowed before the handheld locks).

Protecting lost or stolen handhelds

You can protect confidential enterprise information on BlackBerry handhelds remotely using the following wireless IT commands:

- **Erase Data and Disable Handheld**: This command erases all user and application data that is stored on the BlackBerry handheld. If a handheld is stolen or cannot be found, you can erase all information and application data remotely. See "Restore handheld data wirelessly" on page 44 for more information on restoring data.

- **Set Password and Lock Handheld**: Using this command, you create a new password and locks the handheld remotely. If the user is uncertain of the handheld location, you can set a password (if one has not been set) and lock the handheld. You can then verbally communicate the new password to the user when the handheld is found. If the user set a password in the past, the user is prompted on the handheld to accept or reject the new password change. If the user has forgotten the handheld password, you can reset the password remotely and communicate the new password to the user.

Note: If content protection is enabled, you cannot reset the user's password remotely.

You can protect confidential enterprise information on BlackBerry handhelds remotely using the following IT policy rule:

- **Allow Outgoing Call When Locked**: Set the policy rule to **False** to prevent users from placing outgoing calls until the handheld is recovered. Users are unable to place calls when the handheld is security locked.

Protecting handheld data

Enable content protection

Content protection encrypts data (including email fields, calendar entries, memos, tasks, contact information, and other information) that is stored on the BlackBerry handheld using 256-bit AES.

The handheld also encrypts email messages and meeting requests that it receives when it is locked using elliptic curve key pairs. Using an asymmetric key to protect data while the handheld is locked prevents other users from extracting the symmetric encryption key from the handheld's flash memory and decrypting the user's data.

- Set the content protection IT policy to specify the cryptographic strength of the key that encrypts data when the handheld is locked.

Note: If data is secured using the maximum encryption strength, decrypting the data on the handheld requires more time. For example, users require more time to open and view messages.

If data is secured using the maximum encryption strength, decrypting the data on the handheld will require more time. For example, users will require more time to open and view messages.

Research In Motion recommends that administrators enable content protection and select the encryption strength based on the length of the enforced password.

Strength	Public key length	Description
0	160-bit	Provides good security and performance. This setting is required in the majority of situations.
1	283-bit	Provides better security but slower performance. This setting is required if the handheld password is greater than 12 characters.
2	571-bit	Provides the best security but with the slowest performance. This setting is required if the handheld password is greater than 21 characters.

Prevent applications from persisting protected data

When content protection is enabled, user data is stored in an encrypted form. The original input of the user data is stored in unencrypted form as plaintext objects. Plaintext objects might contain information that the user considers sensitive and therefore should not be stored persistently in this unencrypted form.

If you require additional security for third-party applications, enable the Disable Persisted Plaintext IT policy to make sure that sensitive data cannot be persisted in plaintext form. Plaintext objects that are not stored persistently undergo secure garbage collection. When the handheld performs secure garbage collection, the collected objects are cleared by setting their memory to zero.

If Disable Persisted Plaintext IT policy is enabled, third-party applications attempting to persist plaintext objects causes the handheld to reset. When the handheld restarts, secure garbage collection of the plaintext objects occurs.

Warning: Setting the Disable Persisted Plaintext IT policy rule to **TRUE** might result in an unstable handheld in the presence of third-party applications. Research In Motion recommends setting this rule to **FALSE**.

Restrict handheld data backup

Using the Desktop Backup IT policy rules, you can control the handheld databases that are backed up by the desktop.

- Perform the following action:

Action	Procedure
Restrict the handheld from being backed up by a desktop.	▸ Set the **Desktop Backup** policy rule to one of the following values: • **0**: All handheld databases can be backed up by a desktop. **Note:** Research In Motion recommends setting this rule to 0. • **1**: Minimal subset of handheld databases can be backed up by a desktop. Generally, these are databases that some desktop components require access to for proper operation, such as CertSync. • **2**: No databases can be backed up by a desktop.

Restore handheld data wirelessly

If handheld data is lost or erased, user data can be restored to the handheld using wireless enterprise activation. Enterprise activation restores the latest version of the user's handheld databases that contain a wireless backup. You must enable **Wireless Synchronization** and **Automatic Wireless Backup** on the user's account in the BlackBerry Manager to perform wireless enterprise activation.

1. Authenticate the user, and then provide the user with the new handheld password.
2. Ask the user to perform the following actions:
   a) In the handheld options, click **Enterprise Activation**.
   b) Type the corporate email address and the shared secret password.
   c) Click **Activate**.

Securing communications

Data that is sent between the handheld and the BlackBerry Enterprise Server is encrypted using the Triple DES or the AES algorithm. In the BlackBerry Manager, you can enable data encryption using either a Triple DES encryption key or an AES encryption key. See the *BlackBerry Enterprise Server Administration Guide* for more information.

If you enable both Triple DES and AES on the BlackBerry Enterprise Server, and users are running a version of the BlackBerry Handheld Software, BlackBerry Desktop Software, or the BlackBerry Enterprise Server that is earlier than version 4.0, the BlackBerry Desktop Manager generates a Triple DES encryption key. When the user inserts the handheld into the cradle, its capabilities, including the encryption keys it uses, are transferred to the desktop manager.

If you enable the AES option on the BlackBerry Enterprise Server, and users are running a version of the BlackBerry Handheld Software, BlackBerry Desktop Software, or the BlackBerry Enterprise Server that is earlier than version 4.0, you must upgrade all components to version 4.0 to use AES encryption. See the *BlackBerry Security White Paper* for more information on encryption.

Enable AES for all handhelds

- Perform one of the following actions:

Action	Procedure
Enable AES encryption for an environment that is running version 4.0 BlackBerry Handheld Software, version 4.0 BlackBerry Desktop Software, and the version 4.0 BlackBerry Enterprise Server.	▸ Set the **Disable 3DES Transport Crypto** policy rule to **TRUE**. **Note:** If the rule is set to TRUE, the handheld does not accept Triple DES encrypted messages. Instead, communications for all handhelds are encrypted using AES
Disable AES encryption for an environment that is running a version of the BlackBerry Handheld Software, BlackBerry Desktop Software, or the BlackBerry Enterprise Server that is earlier than version 4.0.	▸ Set the **Disable 3DES Transport Crypto** policy rule to **FALSE**.

Encrypt network traffic between the IBM Lotus Notes client and the IBM Lotus Domino server

To protect master encryption keys in transit, it is recommended that BlackBerry users provisioning their handheld using the desktop and cradle, encrypt network data using the Ports panel in the User Preferences dialog box.

Restricting PIN, SMS, and email messaging

Some organizations might want to track all communications for security or other purposes. If you require all communication to travel through the enterprise-messaging environment, Research In Motion recommends using wireless IT policy to disable PIN and SMS communication for BlackBerry Enterprise Server version 3.5 or later. Disabling PIN and SMS communication disables the transmission of PIN messages from the handheld; however, users can still receive PIN and SMS messages. By default, users can send PIN and SMS messages.

- Perform one of the following actions:

Action	Procedure
Prevent users from sending PIN messages.	• Set the **Allow Peer-to-Peer Messages** policy rule to **FALSE**.
Prevent users from sending SMS messages.	• Set the **Allow SMS** policy rule to **FALSE**.
Prevent users from forwarding or replying to messages using a different BlackBerry Enterprise Server	• Set the **Disable Forwarding Between Services** policy rule to **TRUE**.
Set message sensitivity using different message background colors. **Note:** The background color of messages sent from the BlackBerry Enterprise Server that sent the IT policy is different from the background color of messages sent from other networks (and BlackBerry Enterprise Servers).	• In the **Security Service Colours** policy rule, type the colors of sensitive and non-sensitive messages in RGB (hexadecimal) format.

Note: PIN messages are encrypted with Triple DES, however the key to decrypt the message is available to everyone with a BlackBerry handheld. Therefore, PIN messages should be considered scrambled, but not encrypted.

Restricting access to third-party software applications

Use IT policies and application control policies to send third-party applications to handhelds wirelessly. You can also define and assign application control policies to software configurations for additional administrative control over third-party applications on handhelds.

Application control policies define the specific resources that third-party applications can access on the handheld and behind the corporate firewall. See the *BlackBerry Enterprise Server Handheld Management Guide* for more information on application control policies.

Note: You are solely responsible for the selection, implementation, and performance of any third-party applications that you use with the Handheld or Desktop Software. Research In Motion does not in any way endorse or guarantee the security, compatibility, performance, or trustworthiness of any third-party application and shall have no liability to you or any third-party for issues arising from such third-party applications.

Set IT policies to permit third-party applications to be loaded onto handhelds or prevent the applications from being loaded. Research In Motion recommends that you disable third-party access to handhelds users that require access to a particular third-party application.

- Perform one of the following actions:

Action	Procedure
Prevent third-party applications access to serial port, IrDA, or USB ports on the handheld.	• Set the **Allow Third Party Apps to Use Serial Port** policy rule to **FALSE**.
Prevent third-party applications access to the RIM persistent store API.	• Set the **Allow Third Party Apps to Use Persistent Store** policy rule to **FALSE**.
Prevent users from configuring and executing desktop add-ins (for example, third-party COM-based extensions that access the handheld databases during synchronization).	• Set the **Desktop Allow Desktop Add-Ins** policy rule to **FALSE**.
Prevent third-party applications from being downloaded to the handheld. **Note:** Use application control policies to specify the applications that are allowed to be downloaded to the handheld. See the *BlackBerry Enterprise Server Handheld Management Guide* for more information.	• Set the **Disallow Third Party Application Downloads** policy rules to **FALSE**.

Related resources

Guide	Information
BlackBerry Enterprise Server Administration Guide	• Changing and generating master encryption keys • IT policies
BlackBerry Security White Paper	• Bluetooth® support • Content protection • Application control • BlackBerry Encryption
BlackBerry Handheld Management Guide	• Controlling third-party software applications • Application control IT policies

Appendix A: BlackBerry Enterprise Server permissions

IBM Lotus Domino permissions and privileges

The following table lists the permissions and privileges associated with the BlackBerry Enterprise Server. The required settings for the IBM Lotus Domino databases are defined automatically when the databases are created. See the *BlackBerry Enterprise Server Installation Guide* for more information on creating the required permission settings.

Warning: You should retain the default settings. If you modify the permissions or privileges that are associated with the BlackBerry Enterprise Server, it might not operate in the expected manner.

Action	Permissions	Explanation
Install the BlackBerry Enterprise Server.	• **Windows:** Local administrator account that also has access to remote database server, if applicable. • **IBM Lotus Domino:** Local server ID.	Most BlackBerry services, and any applicable SQL authentication credentials, are installed using this administrator account.
Start the BlackBerry Manager on the same server.	• **Windows:** Local administrator account that also has access to the remote database server, if applicable. • **IBM Lotus Domino:** Local server ID.	By default, the BlackBerry Manager runs under the Local server ID.
Start the BlackBerry Manager on a remote server.	• **Windows:** Local administrator account that also has access to the remote database server, if applicable. • **IBM Lotus Domino:** Local administrator ID that is a member of the **BlackBerryAdmins** group.	The BlackBerry Manager prompts for the local administrator ID password on startup.

Use the BlackBerry state databases.	• **Windows:** Local administrator account.
	• **IBM Lotus Domino:** Local server ID, member of **BlackBerryAdmins** group, or LocalDomainServers with the following:
	  • manager-level access
	  • DeleteDocuments privilege
	  • [Admin] role
	• Note: The user to whom the database belongs also requires Editor access with Delete documents privileges.
		–

Use the BlackBerry Profiles database.	• **Windows:** Local administrator account.
	• **IBM Lotus Domino:** The **BlackBerryAdmins** group, Local server ID, and the LocalDomainServers group with the following:
	  • manager-level access
	  • DeleteDocuments privilege
	  • [Admin] role
		–

Action	Permissions	Explanation
BlackBerry Enterprise Server add-in task	• **Windows:** Local administrator account. • **IBM Lotus Domino:** Local server ID.	The BlackBerry Enterprise Server add-in task runs in the server context.

SQL permissions and privileges

The following table lists the permissions and privileges associated with the configuration database running on a SQL server. See the *BlackBerry Enterprise Server Installation Guide* for more information on creating the required permission settings.

Action	Permissions	Explanation
Create an empty database.	• **SQL Server role**: serveradmin • **Database role**: db_creator	A database administrator can create the database on a remote computer before the BlackBerry Enterprise Server installation process.
Populate a database during installation or upgrade.	• **SQL Server role**: serveradmin • **Database role**: db_owner	The administrator account under which you install the BlackBerry Enterprise Server must be explicitly assigned this permission on the remote computer if it is not a System Administrator/Local Admin account (which has this authority by default).
Read or write to a database using BlackBerry Manager.	• **SQL Server role**: public • **Database role**: rim_db_bes_server	The account under which you start the BlackBerry Manager must be assigned these permissions on the remote computer.
Update the database using the BlackBerry Configuration Panel.	• **SQL Server role**: serveradmin • **Database role**: db_owner	The BlackBerry Configuration Panel must be run after every installation or upgrade to complete database changes.

Appendix B: Default ports

Summary of default ports

Warning: Use of these default ports by another application could result in service interruption.

Component	Activity	Connection type	Default port
BlackBerry Attachment Service	Incoming document submissions from / Outgoing conversion results to: • Attachment connector to Attachment server	—	1900
	Incoming connections from / Outgoing connections to: • Attachment Service tab of BlackBerry Configuration Panel	—	1999
	Incoming document queries from / Outgoing conversion results of large attachments to: • Attachment connector to Attachment server	—	2000
BlackBerry Controller	Incoming syslog connections from: • BlackBerry Messaging Agent	UDP	4070, 4071
	Outgoing logger connections to: • BlackBerry Messaging Agent	UDP	Port provided by the BlackBerry Messaging Agent
BlackBerry Dispatcher	Incoming data connections, using BIPP, from: • BlackBerry Messaging Agent	TCP	5096
	Incoming data connections, using WART, from: • BlackBerry Mobile Data Service • BlackBerry Synchronization Service • BlackBerry Policy Service	TCP	3200
	Outgoing data connection, using SRP, to: • BlackBerry Router	TCP	3101
BlackBerry Messaging Agent	Outgoing data connection, using SRP, to: • BlackBerry Dispatcher	TCP	5096
	Incoming logger connections from: • BlackBerry Controller • CalHelpers	UDP	first unused in the range of 4085-4499
	Outgoing syslog connection to: • BlackBerry Controller	UDP	4070
	Outgoing syslog connection to: • SNMP Agent	UDP	4071

Component	Activity	Connection type	Default port
BlackBerry Mobile Data Service	Incoming HTTP listener ports for: • http • https, if access control is enabled for push		 • 8080 • 8443
	Outgoing data connection to: • BlackBerry Dispatcher	TCP	3200
	Outgoing syslog connection to: • SNMP Agent	UDP	4071
BlackBerry Mobile Policy Service	Incoming data connection from / Outgoing data connection to: • BlackBerry Dispatcher		3200
BlackBerry Router	Incoming data connection from: • BlackBerry Dispatcher	TCP	3101
	Outgoing data connection to: • BlackBerry Messaging Agent	TCP	3101
	Incoming data connections from: • Handhelds using BlackBerry Handheld Manager for serial bypass	TCP	4101
BlackBerry Synchronization Service	Incoming data connection from / Outgoing data connection to: • BlackBerry Dispatcher		3200
SNMP Agent	Incoming syslog connections from: • BlackBerry Messaging Agent	UDP	4071

Appendix C: SNMP Values

Version 1

The values in the following table represent global statistics counters from the first BlackBerry Enterprise Server session started on the system and are maintained for backward compatibility with MIB version 1.

Notes: The values in the table are persistent (they do not reset at startup).

The statistics in the table only include messages that are routed through the BlackBerry Enterprise Server (for example, they do not include PIN or SMS messages).

Value	Description	Object Identifier
besSysHealthV1MsgsPending	The total number of messages that are queued for delivery to handhelds.	1.3.6.1.4.1.3530.5.25.1.202
besSysHealthV1TotalMsgsSent	The total number of messages that were sent from handhelds.	1.3.6.1.4.1.3530.5.25.1.203
besSysHealthV1TotalMsgsReceived	The total number of messages that were delivered to handhelds.	1.3.6.1.4.1.3530.5.25.1.204
besSysHealthV1TotalMsgsExpired	The total number of messages that have expired without being delivered to handhelds.	1.3.6.1.4.1.3530.5.25.1.205
besSysHealthV1TotalMsgsFiltered	The total number of messages that have been filtered.	1.3.6.1.4.1.3530.5.25.1.206
besSysHealthV1MsgsSentPerMin	The total number of messages that were sent from handhelds each minute.	1.3.6.1.4.1.3530.5.25.1.207
besSysHealthV1MsgsRecvdPerMin	The total number of messages that were delivered to handhelds each minute.	1.3.6.1.4.1.3530.5.25.1.208
besSysHealthV1SRPConnectState	The state of the BlackBerry Enterprise Server's connection to the wireless network.	1.3.6.1.4.1.3530.5.25.1.209
version	The version number of the BlackBerryServer.mib file.	1.3.6.1.4.1.3530.5.1.0
besTotMsgsPending	The total number of messages that are queued for delivery to handhelds.	1.3.6.1.4.1.3530.5.2.0
besTotMsgsSent	The total number of messages that were sent from handhelds.	1.3.6.1.4.1.3530.5.3.0
besTotMsgsRecvd	The total number of messages that were delivered to handhelds.	1.3.6.1.4.1.3530.5.4.0
besTotMsgsXpired	The total number of messages that have expired without being forwarded to handhelds.	1.3.6.1.4.1.3530.5.5.0
besTotMsgsFiltered	The total number of messages that have been filtered.	1.3.6.1.4.1.3530.5.6.0
besTotMsgsSentPerMin	The total number of messages that were sent from handhelds each minute. This value is averaged from the last 10 minutes of processing.	1.3.6.1.4.1.3530.5.7.0

Value	Description	Object Identifier
besTotMsgsRecvdPerMin	The total number of messages that were delivered to handhelds each minute. This value is averaged from the last 10 minutes of processing.	1.3.6.1.4.1.3530.5.8.0
besNumServerInfoAvailable	The number of BlackBerry Enterprise Servers that are installed on this system, and for which information is exposed and currently available using SNMP.	1.3.6.1.4.1.3530.5.15.0

Configuration

The values in the following table represent the Configuration container for BlackBerry Enterprise Servers that are running on the system.

Note: The statistics in the table only include messages that are routed through the BlackBerry Enterprise Server (for example, they do not include PIN or SMS messages).

Value	Description	Object Identifier
besConfigServerInstance	The BlackBerry Enterprise Server instance number (1...n).	1.3.6.1.4.1.3530.5.20.1.1
besConfigServerName	The BlackBerry Enterprise Server name.	1.3.6.1.4.1.3530.5.20.1.2
besConfigVersionString	The BlackBerry Enterprise Server version information.	1.3.6.1.4.1.3530.5.20.1.10
besConfigReleaseMaj	Indicates whether this is a major release.	1.3.6.1.4.1.3530.5.20.1.11
besConfigReleaseMin	Indicates whether this is a minor release.	1.3.6.1.4.1.3530.5.20.1.12
besConfigReleaseServicePack	Indicates whether this is a Service Pack release.	1.3.6.1.4.1.3530.5.20.1.13
besConfigReleaseBuild	The build number.	1.3.6.1.4.1.3530.5.20.1.14
besConfigLicenceTotal	The total number of end-user licenses that are installed on the BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.20.1.20
besConfigLicenceUsed	The total number of end-user licenses that are currently in use on the BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.20.1.21
besConfigLicenceRemaining	The total number of available end-user licenses that are not currently in use.	1.3.6.1.4.1.3530.5.20.1.22
besConfigServerUID	The UID (also SRP Identifier) of this BlackBerry Enterprise Server instance; the UID uniquely identifies the BlackBerry Enterprise Server to the wireless network.	1.3.6.1.4.1.3530.5.20.1.30
besConfigSystemAttendant	The email address that was defined to send and receive notifications that are sent from the BlackBerry Enterprise Server administration application.	1.3.6.1.4.1.3530.5.20.1.40
besConfigSRPHost	The SRP host (also SRP address) that is configured for the BlackBerry Enterprise Server; the SRP host is the BlackBerry Enterprise Server connection to the wireless network.	1.3.6.1.4.1.3530.5.20.1.50
besConfigSRPPort	The port that the BlackBerry Enterprise Server uses to establish outbound connectivity to the wireless network.	1.3.6.1.4.1.3530.5.20.1.51
besConfigAutoBCCEnabled	Indicates whether messages that are sent from handhelds are automatically blind carbon copied (AutoBCC) to an email address; 1 means that the option is enabled, 0 means that the option is not enabled.	1.3.6.1.4.1.3530.5.20.1.60
besConfigAutoBCCAddress	If the AutoBCC feature is enabled, indicates the address that is configured to receive blind carbon copies; an empty value is returned if AutoBCC is not enabled on the BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.20.1.61

Value	Description	Object Identifier
besConfigForceSaveInSentEnabled	Indicates whether, regardless of users' desktop software settings, all messages that are sent from handhelds are saved in their email client's Sent folder.	1.3.6.1.4.1.3530.5.20.1.70
besConfigWirelessEmailRecoEnabled	Indicates whether wireless email reconciliation support is enabled on the BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.20.1.80.

System health

The values in the following table represent the System Health container for BlackBerry Enterprise Servers that are running on the system.

Note: The statistics in the table only include messages that are routed through the BlackBerry Enterprise Server (for example, they do not include PIN or SMS messages).

Value	Description	Object Identifier
besSysHealthServerInstance	The BlackBerry Enterprise Server's instance number (`1..n`).	1.3.6.1.4.1.3530.5.25.1.1
besSysHealthSrpConnectedState	Indicates whether the BlackBerry Enterprise Server is connected to the wireless network.	1.3.6.1.4.1.3530.5.25.1.10
besSysHealthSrpLastConnectDate	The date and time that the BlackBerry Enterprise Server last connected to the wireless network successfully.	1.3.6.1.4.1.3530.5.25.1.11
besSysHealthSrpReconnectSuccess	The number of times that the BlackBerry Enterprise Server has reconnected successfully to the wireless network since startup.	1.3.6.1.4.1.3530.5.25.1.12
besSysHealthSrpReconnectsFail	The number of times that the BlackBerry Enterprise Server has attempted, but failed, to connect to the wireless network since startup.	1.3.6.1.4.1.3530.5.25.1.13
besSysHealthSrpTotalSecNot Connected	The total number of seconds since startup that the BlackBerry Enterprise Server has not been connected to the wireless network.	1.3.6.1.4.1.3530.5.25.1.14
besSysHealthSrpLastErrorText	The error text associated with the last failed connection attempt.	1.3.6.1.4.1.3530.5.25.1.15
besSysHealthSrpLastErrorTime	The date and time of the last connection error.	1.3.6.1.4.1.3530.5.25.1.16
besSysHealthMsgTotalProc	The total number of messages that the BlackBerry Enterprise Server has processed since startup; this total includes messages that were sent to the handheld, sent from the handheld, or not forwarded to the handheld because they were filtered.	1.3.6.1.4.1.3530.5.25.1.20
besSysHealthMsgToHandheld	The total number of messages that passed the filter criteria and were forwarded to handhelds; this total does not include calendar items.	1.3.6.1.4.1.3530.5.25.1.21
besSysHealthMsgFromHandheld	The total number of messages that were sent from handhelds since startup; this total does not include calendar items.	1.3.6.1.4.1.3530.5.25.1.22
besSysHealthMsgFilteredByUser	The total number of messages to which the BlackBerry Enterprise Server applied user-defined filters and did not forward to handhelds since startup.	1.3.6.1.4.1.3530.5.25.1.23
besSysHealthMsgFilteredByGlobal	The total number of messages to which the BlackBerry Enterprise Server applied global filters and did not forward to handhelds since startup.	1.3.6.1.4.1.3530.5.25.1.24

Value	Description	Object Identifier
besSysHealthMsgPending	The total number of messages that are pending to be delivered to handhelds.	1.3.6.1.4.1.3530.5.25.1.25
besSysHealthMsgExpired	The total number of messages that expired without being delivered to handhelds since startup.	1.3.6.1.4.1.3530.5.25.1.26
besSysHealthMsgErrors	The total number of messages that were non-deliverable to handhelds because of an error.	1.3.6.1.4.1.3530.5.25.1.27
besSysHealthMsgMoreRequests	The total number of MORE requests that were issued from handhelds since startup.	1.3.6.1.4.1.3530.5.25.1.28
besSysHealthCalUsersOTACEnabled	The total number of users for whom wireless calendar synchronization is enabled.	1.3.6.1.4.1.3530.5.25.1.40
besSysHealthCalEventToHandheld	The total number of calendar events that were sent to handhelds.	1.3.6.1.4.1.3530.5.25.1.41
besSysHealthCalEventFrom Handheld	The total number of calendar events that were sent from handhelds.	1.3.6.1.4.1.3530.5.25.1.42
besSysHealthWERUsersEnabled	The total number of users that are enabled for wireless email reconciliation.	1.3.6.1.4.1.3530.5.25.1.50
besSysHealthWERRequestsTo Handheld	The total number of wireless email reconciliation events that were sent to handhelds.	1.3.6.1.4.1.3530.5.25.1.51
besSysHealthWERRequestsFrom Handheld	The total number of wireless email reconciliation events that were sent from handhelds.	1.3.6.1.4.1.3530.5.25.1.52
besSysHealthMdsDevice Connections	The number of handheld-initiated Mobile Data Service connections that were made since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.60
besSysHealthMdsPush Connections	The number of push server connections that were made since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.61
besSysHealthMdsTotalBytes FromDevices	The total size (in bytes) of Mobile Data Service data that was sent from all handhelds since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.62
besSysHealthMdsMaxPacket SizeFromDevice	The largest packet size of Mobile Data Service data (in bytes) that was sent from a handheld since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.63
besSysHealthMdsAvgPacketSize FromDevice	The average packet size (in bytes) of Mobile Data Service data that was sent from handhelds since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.64
besSysHealthMdsTotalBytesTo Device	The total size (in bytes) of push data that was sent from the Mobile Data Service to handhelds since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.65
besSysHealthMdsMaxPacketSize ToDevice	The largest packet size (in bytes) of push data that was sent from the Mobile Data Service to handhelds since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.66
besSysHealthMdsAvgPacketSize ToDevice	The average packet size (in bytes) of push data that was sent from the Mobile Data Service to handhelds since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.67
besSysHealthMdsRefused Packets	The number of packets that the wireless network refused that were sent from the Mobile Data Service (using the BlackBerry Enterprise Server) since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.68
besSysHealthMdsInvalid Packets	The number of invalid packets that were received by the Mobile Data Service since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.69

Value	Description	Object Identifier
besSysHealthMdsConnection Success	The number of successful connections that were initiated by the Mobile Data Service to another address or service since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.70
besSysHealthMdsConnection Failure	The number of unsuccessful connections that were initiated by the Mobile Data Service to another address and, or service in this BlackBerry Enterprise Server session.	1.3.6.1.4.1.3530.5.25.1.71
besSysHealthMdsConnection Truncated	The number of truncated connections that were encountered by the Mobile Data Service since BlackBerry Enterprise Server startup.	1.3.6.1.4.1.3530.5.25.1.72

Mail server health

The values in the following table represent the list of mail servers, and statistics and performance values related to each particular mail server.

Value	Description	Object Identifier
besMailServerHealthServerInstance	The server instance ID of the BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.26.1.1
besMailServerHealthServerId	The server instance ID of the mail server.	1.3.6.1.4.1.3530.5.26.1.2
besMailServerHealthServerName	The Mail server name.	1.3.6.1.4.1.3530.5.26.1.3
besMailServerHealthTotalUsers	The number of users that have accounts on this mail server.	1.3.6.1.4.1.3530.5.26.1.10
besMailServerHealthAvgResponse Time10min	The average response time (in milliseconds) for operations for users on this mail server in the last 10 minutes.	1.3.6.1.4.1.3530.5.26.1.11
besMailServerHealthFailedConn 10min	The number of failed connection attempts that the BlackBerry Enterprise Server made to this mail server in the last 10 minutes.	1.3.6.1.4.1.3530.5.26.1.12

User health

The values in the following table represent the list of user configuration, statistics and performance values related to each user and handheld on a BlackBerry Enterprise Server.

Note: The statistics in the table only include messages that are routed through the BlackBerry Enterprise Server (for example, they do not include PIN or SMS messages).

Value	Description	Object Identifier
besUserHealthServerInstance	The instance ID of the user's associated BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.30.1.1
besUserHealthUserId	The user's instance ID.	1.3.6.1.4.1.3530.5.30.1.2
besUserHealthUserName	The user name.	1.3.6.1.4.1.3530.5.30.1.3
besUserHealthLastErrorText	The error text that was returned the last time that an operation for this user failed.	1.3.6.1.4.1.3530.5.30.1.10
besUserHealthLastErrorTime	The date and time of the last error for this user.	1.3.6.1.4.1.3530.5.30.1.11
besUserHealthDeviceNetwork	The wireless network on which the user's handheld operates.	1.3.6.1.4.1.3530.5.30.1.20
besUserHealthDevicePIN	The PIN that is associated with the user's handheld.	1.3.6.1.4.1.3530.5.30.1.21

Value	Description	Object Identifier
besUserHealthDeviceInCradle	Indicates whether the user's handheld is connected to the Desktop Software.	1.3.6.1.4.1.3530.5.30.1.22
besUserHealthNumRedirected Folders	The number of redirected folders that the user has configured.	1.3.6.1.4.1.3530.5.30.1.30
besUserHealthSaveInSent	Indicates whether the user has enabled the **Save in Sent** option in the Desktop Software.	1.3.6.1.4.1.3530.5.30.1.31
besUserHealthRedirectEnabledOn Desktop	Indicates whether the user has selected the desktop software option to redirect incoming messages to the handheld.	1.3.6.1.4.1.3530.5.30.1.32
besUserHealthDisableWhileInCradle	Indicates whether the user has selected the desktop software option to disable redirection while the handheld is connected to the computer.	1.3.6.1.4.1.3530.5.30.1.33
besUserHealthFullyConfigured	Indicates whether the user's handheld is fully configured with a PIN and encryption key.	1.3.6.1.4.1.3530.5.30.1.34
besUserHealthEnabled	Indicates whether the user is currently enabled on the BlackBerry Enterprise Server.	1.3.6.1.4.1.3530.5.30.1.35
besUserHealthMsgTotalProc	The total number of messages that the BlackBerry Enterprise Server has processed for this user since startup; includes messages that were sent to the handheld, sent from the handheld, or not forwarded to the handheld because they were filtered.	1.3.6.1.4.1.3530.5.30.1.40
besUserHealthMsgToHandheld	The total number of messages that passed the filter criteria and were forwarded to the user's handheld. This total does not include calendar items.	1.3.6.1.4.1.3530.5.30.1.41
besUserHealthMsgFromHandheld	The total number of messages that were sent from the user's handheld in this session; this value does not include calendar items.	1.3.6.1.4.1.3530.5.30.1.42
besUserHealthMsgFiltered	The total number of messages to which the BlackBerry Enterprise Server applied filters and did not forward to the user's handheld in this session.	1.3.6.1.4.1.3530.5.30.1.43
besUserHealthMsgPending	The total number of messages that are pending delivery to the user's handheld.	1.3.6.1.4.1.3530.5.30.1.44
besUserHealthMsgExpired	The total number of messages that expired without being delivered to the user's handheld in this session.	1.3.6.1.4.1.3530.5.30.1.45
besUserHealthMsgErrors	The total number of messages that were non-deliverable to the user's handheld because of an error.	1.3.6.1.4.1.3530.5.30.1.46
besUserHealthMsgMoreRequests	The total number of MORE requests that were issued from the user's handheld.	1.3.6.1.4.1.3530.5.30.1.47
besUserHealthMsgForwardedFrom Device	The total number of messages that the user has forwarded from the handheld.	1.3.6.1.4.1.3530.5.40.1.48
besUserHealthMsgRepliedToWith Text	The total number of messages that were replies with-text from the user's handheld.	1.3.6.1.4.1.3530.5.30.1.49
besUserHealthLastTimeInCradle	The date and time that the user last connected the handheld to the computer.	1.3.6.1.4.1.3530.5.30.1.60
besUserHealthLastInteractionWith Device	The date that the BlackBerry Enterprise Server and the user's handheld last interacted.	1.3.6.1.4.1.3530.5.30.1.61
besUserHealthLastMessage Forwarded	The date and time that the last message (email or calendar) was sent to the user's handheld.	1.3.6.1.4.1.3530.5.30.1.62
besUserHealthLastKeyDate Generated	The date and time that the user last generated an encryption key.	1.3.6.1.4.1.3530.5.30.1.63

Value	Description	Object Identifier
besUserHealthAvgKBForwarded	The average size of messages that the user forwarded from the handheld (in KB); for example, if the user receives a message with a 5 MB attachment and forwards it from the handheld, the value is 5120 KB.	1.3.6.1.4.1.3530.5.30.1.70
besUserHealthAvgKBReplyWithText	The average size of messages that the user replied to with text from the handheld (in KB); for example, if the user receives a message with a 5 MB attachment and replies to it with text on the handheld, the value is 5120 KB.	1.3.6.1.4.1.3530.5.30.1.71
besUserHealthAvgLatencyInSecLast 10Msg	For the last 10 messages sent to the user's handheld, the average length of time (in seconds) between the message arriving on the mail server and the DELIVERED message appearing on the user's handheld.	1.3.6.1.4.1.3530.5.30.1.72
besUserHealthCalOTAEnabled	Indicates whether wireless calendar synchronization is enabled for the user.	1.3.6.1.4.1.3530.5.30.1.80
besUserHealthCalEventToHandheld	The total number of calendar items that were sent to the user's handheld.	1.3.6.1.4.1.3530.5.30.1.81
besUserHealthCalEventFrom Handheld	The total number of calendar events that the user sent from the handheld.	1.3.6.1.4.1.3530.5.30.1.82
besUserHealthWirelessEmailReco Enabled	Indicates whether the user is enabled for wireless email reconciliation.	1.3.6.1.4.1.3530.5.30.1.90
besUserHealthWERRequests ToHandheld	The total number of wireless email reconciliation events that were sent to the user's handheld.	1.3.6.1.4.1.3530.5.30.1.91
besUserHealthWERRequests FromHandheld	The total number of wireless email reconciliation events that were sent from the user's handheld.	1.3.6.1.4.1.3530.5.30.1.92

BlackBerry Enterprise Server events

The values in the following table represent event-driven traps which notify the server management application that an event has taken place on the system.

Value	Description	Object Identifier
besSRPConnectEvent	Indicates whether the BlackBerry Enterprise Server is connected to the wireless network, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.1 (Connected) and 1.3.6.1.4.1.3530.9.2 (Disconnected)
besHungThreadEvent	Indicates that a BlackBerry Enterprise Server non-responsive thread has been detected.	1.3.6.1.4.1.3530.9.3
besMailServerDownEvent	Indicates whether the mail server is running, as indicated by the last integer in the OID; this event occurs if more than one user (or one user if there is only one) on the mail server receives more than one non-access control error while connecting to the mail server.	1.3.6.1.4.1.3530.9.5 (Server is down) or 1.3.6.1.4.1.3530.9.6 (Server is up)
besMDStoBESConnectionEvent	Indicates whether the Mobile Data Service is connected to the BlackBerry Enterprise Server, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.7 (Connected) and 1.3.6.1.4.1.3530.9.8 (Disconnected)
besMDSStartStopEvent	Indicates whether the Mobile Data Service is started, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.11 (Started) or 1.3.6.1.4.1.3530.9.12 (Stopped)

Value	Description	Object Identifier
besMDStoDBConnectionEvent	Indicates whether the Mobile Data Service is connected to the database, as indicated by the last integer in the OID.	1.3.6.1.4.1.3530.9.13 (Connected) or 1.3.6.1.4.1.3530.9.14 (Disconnected)
besCriticalEvent	Indicates that an event has been logged with a 1*xxxx* or 5*xxxx* (critical) event ID.	1.3.6.1.4.1.3530.9.21

Appendix D: Command line tools

Backing up the configuration database using the BlackBerry Database Backup tool

If you are using MSDE 2000 for your configuration database, you can use the BlackBerry Database Backup tool provided with the BlackBerry Enterprise Server software to perform a full backup of the database. By default, this backup file is named *<database name><YYYYMMDDHHMMSS>.bak*.

Run the BlackBerry Database Backup tool

1. On the server where the configuration database is located, at the command prompt, switch to the Tools directory on the installation CD.
2. Type **BlackBerryDBBackup.exe,** followed by the parameters needed to configure the backup, in the following order:

   ```
   BlackBerryDBBackup -d [-f] [-S] [-E | -U -P] [-p]
   ```

3. Configure BlackBerryDBBackup using the following parameters:

Parameter	Procedure
-d	▸ Type the database name.
-f	▸ Type the folder in which the backup file is saved. By default, this is set to the current location. **Note:** If you specify a different location, the folder must already exist.
-S	▸ Type the name of the server where the database is located. By default, this is set to local server.
-E	▸ Specify if Windows authentication is used to connect to the database. By default, this is set to **False**. **Note:** If you want to use SQL authentication, omit this parameter from the statement and provide the SQL credentials.
-U	▸ Type the SQL authentication user name. By default, this is set to System Administrator. **Note:** If you do not want to use the System Administrator account, you must use an account with SQL Server Administrator and Database Owner permissions.
-P	▸ Type the SQL authentication password. By default, this is blank.

Parameter	Procedure
-p	▸ Type the interval at which you want progress reported. By default, this is set to 10%.

4. Press **Enter**.

Example

```
C:\Documents and Settings\Desktop\CDLayout\tools>BlackBerryDbBackup -d BESMgmt -f
c:\DB_backup_folder -U sqlusername -P sqlpassword
Connecting to SQLServer...
Connected.

Backing up to file [c:\DB_backup_folder\BESMgmt_20040512122125.bak]

Percent done:  31 @ Mon May 12 12:21:25 2004
Percent done:  62 @ Mon May 12 12:21:25 2004
Percent done:  93 @ Mon May 12 12:21:25 2004
Percent done: 100 @ Mon May 12 12:21:25 2004

Backup Completed @ Mon May 12 12:21:25 2004
[Microsoft][ODBC SQL Server Driver][SQL Server]BACKUP DATABASE successfully proc
essed 385 pages in 0.743 seconds (4.238 MB/sec).
```

Restoring the configuration database using the BlackBerry Database Restore tool

If you are using MSDE 2000 for your configuration database, you can use the BlackBerry Database Restore tool provided with the BlackBerry Enterprise Server software.

Run the BlackBerry Database Restore tool

1. On the server where the configuration database is located, at the command prompt, switch to the Tools directory on the installation CD.
2. Type **BlackBerryDBRestore**, followed by the parameters needed to configure the restore, in the following order:

   ```
   BlackBerryDBRestore -d [-f] [-S] [-E | -U -P] [-p]
   ```

3. Configure BlackBerryDBRestore.exe using the following parameters:

Parameter	Procedure
-d	▸ Type the database name. **Note:** You must use the same database name for restore that you used for backup. You cannot use this tool to change a database name.
-f	▸ Type the name of the backup file.
-S	▸ Type the name of the server where the database is located. By default, this is set to local server.
-E	▸ Specify if Windows authentication is used to connect to the database. By default, this is set to **False**. **Note:** If you want to use SQL authentication, omit this parameter from the statement and provide the SQL credentials.

Parameter	Procedure
-U	▸ Type the SQL authentication user name. By default, this is set to System Administrator. **Note:** If you do not want to use the System Administrator account, you must use an account with SQL Server Administrator and Database Owner permissions.
-P	▸ Type the SQL authentication password. By default, this is blank.
-p	▸ Type the interval at which you want progress reported. By default, this is set to 10%.

4. Press **Enter**.

Example

```
C:\Documents and Settings\Desktop\CDLayout\tools>BlackBerryDbRestore -d BESMgmt -f
c:\DB_backup_folder\BESMgmt_20040512122125.bak -U sqlusername -P sqlpassword
Connecting to SQLServer...
Connected.

Restore starting...
Percent done:  10 @ Wed May 12 12:21:26 2004
Percent done:  20 @ Mon May 12 12:21:26 2004
Percent done:  31 @ Mon May 12 12:21:26 2004
Percent done:  41 @ Mon May 12 12:21:26 2004
Percent done:  52 @ Mon May 12 12:21:26 2004
Percent done:  60 @ Mon May 12 12:21:26 2004
Percent done:  70 @ Mon May 12 12:21:26 2004
Percent done:  81 @ Mon May 12 12:21:26 2004
Percent done:  91 @ Mon May 12 12:21:26 2004
Percent done: 100 @ Mon May 12 12:21:26 2004

Restore Completed @ Mon May 12 12:21:26 2004
[Microsoft][ODBC SQL Server Driver][SQL Server]RESTORE DATABASE successfully
processed 385 pages in 0.536 seconds (5.875 MB/sec).
```

Creating the configuration database using the CreateDB.exe tool

Use the CreateDB tool to create the configuration database. The details of the installation are written to a log file. By default, this log file is named DBInstallV*<YYMMDDHHMMSS>*.log.

Configure the database using the BESMgmt.cfg file

1. On any server, at the command prompt, switch to the Database directory on the installation CD.
2. Open the **BESMgmt.cfg** file, and then configure the file using the following parameters:

Command	Procedure
Database_name	▸ Type the database name.
CMD	▸ Specify type of database action to perform, using one of the following: • Install • Migrate • Restore By default, the database action is set to **Install**.

Command	Procedure
Verbose	▸ Set to **True** to include information and error messages in log file. By default, this is set to **False**.
Version	▸ Specify the database version to create and, or migrate to, using one of the following: • 3.5 • 3.6 • 4.0 By default, the version is set to **4.0**.
Create	▸ Set to **False** if no database should be created. By default, this is set to **True**. **Note:** This setting is ignored in a database migration.
Backup	▸ Set to **True** to back up the existing database. By default, this is set to **False**.
Drop	▸ Set to **True** to drop the existing database. By default, this is set to **False**. **Note:** This setting is ignored in a database migration.
Server	▸ Specify the server on which to install the database. By default, this is **Local**.
Stop	▸ Specify if the process should stop if an error is encountered. By default, this is set to **True**.
Script_root	▸ Specify the path to the DBInstallScripts directory. By default, this is the same root as createdb.exe.
Log_dir	▸ Specify the path to the directory where log files should be created. By default, this is the same root as createdb.exe.
Timestamp	▸ Set to **False** to remove timestamp (HHMMSS) from log files. By default, this is set to **True**.
DBMS	▸ Specify which database management system is used. By default, this is set to **SQL**.
Db_file_dir	▸ Specify the directory in which to save the database files. This directory must already exist. By default, this is the same root as createdb.exe.
Backup_dir	▸ Specify the directory in which to save the database backup. This directory must already exist. By default, this is the same root as createdb.exe.
Restore_filename	▸ Specify the file to use for a database restore. By default, this is *<database location>*\DatabaseNameBKUP.dat **Note:** If more than one backup file exists, the most current version is used.
Generate_execute	▸ Set to **False** to generate, but not execute, the SQL files. By default, this is set to **True**.

3. Save and close the file.

Run the CreateDB.exe tool

1. On any server, at the command prompt, switch to the Database directory on the installation CD.
2. Type **CreateDB.exe BESMgmt.cfg**.
3. Press **Enter**.

Migrating users using the NBESMigration tool

If you are upgrading from BlackBerry Enterprise Server version 2.2 to version 4.0, and have more than 200 users, Research In Motion recommends that you use this tool to migrate users after the BlackBerry Enterprise Server upgrade is complete.

Run the NBESMigration.exe

1. On the server where the upgraded BlackBerry Enterprise Server is located, at the command prompt, switch to the Database directory on the installation CD.
2. Type **nbesmigration.exe**, followed by the parameters needed to configure the migration, in the following order:
   ```
   nbesmigration -d [-l] [-t] [-w] [-u]
   ```
3. Use these parameters to configure NBESMigration:.

Command	Procedure
- d *<DB server name> <DB name>*	▸ Type the server name and the database name of the configuration database.
-l	▸ Type the name and path for the log file. If the migration fails for any reason, refer to this file for error messages.
-t	▸ Type the name and path of the status file used to track the progress of the migration. On subsequent migration attempts, this file prevents duplicate user records from being created.
-w	▸ Include this parameter at the command prompt to write status and progress information to the registry
-u *<username> <password>*	▸ If applicable, type the user name and password needed for SQL authentication.

Example

```
C:\Documents and Settings\Desktop\CDLayout\database>nbesmigration.exe -d
"sqlserver1" "besmgmt" -l migrate.log -t status.tmp
```

Testing the BlackBerry Enterprise Server SRP connection using the BBSRPTest tool

Use the BBSRPTest tool to test the connection of the BlackBerry Enterprise Server—using the BlackBerry Router—to the SRP address.

Run the BBSRPTest tool

1. On the server where the BlackBerry Enterprise Server is located, at the command prompt, switch to the Utility directory created during the installation process.
2. Type **BBSRPTest.exe -?** to view the list of commands that can be used with BBSRPTest.

Command	Description
-server "*Servername*"	This command enables you to specify the BlackBerry Enterprise Server instance to be tested, if multiple instances have been installed.
-host *<hostname>*	This command enables you to specify a host to be tested. If no host name is specified, the host name is retrieved from the registry.
-port *<port>*	This command enables you to specify a port to be tested. If no port is specified, the port is retrieved from the registry.
-quiet	This command prevents output to the screen.
-wait	This command returns the SRP connection information and then prompts you to click Enter to continue.

3. At the command prompt, type **BBSRPTest.exe -flag <optional arguments>**.

   The utility checks the BlackBerry Enterprise Server network access node (for example, srp.na.blackberry.net) and confirms whether the SRP connection to the wireless network exists.

Repairing the registration of the performance monitor file using the BBPerfmoninstall tool

If problems with performance monitor counters occur, use the BBPerfmoninstall tool to repair the registration of the performance monitor tool .dll file.

Run the BBPerfmoninstall tool

1. On the server where the BlackBerry Enterprise Server is located, at the command prompt, switch to the Utility directory created during the installation process.
2. Type **BBPerfmoninstall.exe -uninstall**.
3. Type **BBPerfmoninstall.exe -install**. The utility repairs the registration of the performance monitor .dll file.

Appendix E: Notes.ini settings

Reviewing the notes.ini file

notes.ini value	Description	Default
RIMDataPath	Defines the directory in Domino\Data that contains the BlackBerry Enterprise Server databases (profiles, outgoing queue, state databases, BlackBerry directory, and BlackBerry stats).	BES
RIMForceSaveInSent	Defines whether the BlackBerry Enterprise Server forces all messages that are sent from handhelds to be copied in the user's Sent folder in the client software. If the value is **0** or is not present, the user's settings are read. If the value is **1**, the **Don't save a copy to the Sent Items folder** setting in users' Redirector Settings is ignored and all messages that are sent from handhelds are copied in their sent folder.	0
RIMSRPPortDispatcher	Defines the port that is used for the BlackBerry Messaging Agent connections to the BlackBerry Dispatcher.	5096
ServerTask	Defines the BlackBerry Enterprise Server IBM Lotus Domino add-in task.	BES
RIMUID, RIMPolling, RIMSRPHost, RIMSystemAttendant, RIMAuthKey, RIMNumLicenses, RIMRescanRange, RIMRescanInterval, RIMRpcServerPort	These value are no longer stored in the notes.ini file.	–

Published in Canada.