



BlackBerry Enterprise Server for Microsoft Exchange

Version 4.0

Feature and Technical Overview

BlackBerry Enterprise Server for Microsoft Exchange Version 4.0 Feature and Technical Overview

Last modified: 10 November 2004

Part number: SWD_X_BES(EN)-029.001

MAT-08562-001

ASY-08564-002

© 2004 Research In Motion Limited. All rights reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, BlackBerry and 'Always On, Always Connected' are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

CDMA2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA). Global System for Mobile Communications™ and GSM™ are registered trademarks of the GSM Association. Java and JavaScript are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. or other countries. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other brands, product names, company names, trademarks, and service marks are the properties of their respective owners.

The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

This document is provided "as is" and Research In Motion Limited (RIM) assumes no responsibility for any typographical, technical, or other inaccuracies in this document. RIM reserves the right to periodically change information that is contained in this document; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this document to you in a timely manner or at all. RIM MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS, OR COVENANTS, EITHER EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, MERCHANTABILITY, DURABILITY, TITLE, OR RELATED TO THE PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE REFERENCED HEREIN, OR PERFORMANCE OF ANY SERVICES REFERENCED HEREIN). IN CONNECTION WITH YOUR USE OF THIS DOCUMENTATION, NEITHER RIM NOR ITS AFFILIATED COMPANIES AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, OR CONSULTANTS SHALL BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER BE THEY DIRECT, ECONOMIC, COMMERCIAL, SPECIAL, CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, OR INDIRECT DAMAGES, EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA, DAMAGES CAUSED BY DELAYS, LOST PROFITS, OR A FAILURE TO REALIZE EXPECTED SAVINGS.

This document might contain references to third-party sources of information and/or third-party web sites ("Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation, the content, accuracy, copyright compliance, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the third party in any way. Any dealings with third parties, including, without limitation, compliance with applicable licenses, and terms and conditions are solely between you and the third party. RIM shall not be responsible or liable for any part of such dealings.

Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server Software, BlackBerry Desktop Software, and/or BlackBerry Handheld Software and may require additional development or third-party products and/or services for access to corporate applications. Prior to subscribing to or implementing any third-party products and services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third-party products and services. Installation and use of third-party products and services with RIM's products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. You are solely responsible for acquiring any such licenses. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use these products until all such applicable licenses have been acquired by you or on your behalf. Your use of third-party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third-party products and services that are provided with RIM's products and services are provided "as is." RIM makes no representation, warranty, or guarantee whatsoever in relation to the third-party products or services and RIM assumes no liability whatsoever in relation to the third-party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>) and/or licensed pursuant to Apache License, Version 2.0 (<http://www.apache.org/licenses/>). For more information, see the NOTICE.txt file included with the software.

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

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

The BlackBerry Wireless Solution	7
Features	11
New in this release	11
BlackBerry software requirements for new features and enhancements.....	15
Messaging.....	18
Email	18
PIM data	19
Attachments.....	20
Remote address lookup	21
BlackBerry Mobile Data Service.....	21
BlackBerry Enterprise Server management tools	23
IT Policy.....	23
Handheld management.....	24
Deployment.....	24
Maintenance and upgrades	26
Security	26
Encryption	26
Confidentiality.....	27
Integrity and authenticity.....	27
Content protection.....	28
Third-party application control.....	29
IT policies and IT commands	29
Architecture	31
Components.....	32
Remote components	33
Workflows.....	35
Email.....	35
Email sent to a handheld.....	35
Email sent from a handheld.....	36

Attachments.....	37
Address lookup.....	39
PIM data.....	40
Initial synchronization.....	40
PIM synchronization.....	41
Mobile data.....	42
Wireless enterprise activation.....	45
BlackBerry Router.....	46

Index.....	47
-------------------	-----------

The BlackBerry Wireless Solution

The BlackBerry® Wireless Solution, including innovative software, advanced wireless handhelds, and wireless network service, provides a unified framework for mobile access to enterprise applications, and wireless email communication. Benefits include

- streamlining deployment
- enabling end-to-end connectivity
- supporting multiple devices, applications, and networks
- simplifying management
- pushing important information to mobile users
- keeping data confidential
- extending existing infrastructure
- staying connected

Benefit	Description
Streamlining deployment	To reduce the administrative tasks associated with handheld deployment, the BlackBerry Wireless Solution includes features that streamline deployment tasks. Wireless enterprise activation enables users to activate their BlackBerry Wireless Handhelds™ wirelessly, while administrators retain control over assets, third-party application distribution, and deployment attributes.
Enabling end-to-end connectivity	The BlackBerry Wireless Solution provides a robust infrastructure that supports communication with handhelds. It does this over many wireless networks through a secure connection from behind the firewall. It monitors BlackBerry user mailboxes for email, pushes data to end users, and manages data requests, messages, and organizer items that are submitted from the handheld.
Supporting multiple devices, applications, and networks	A single BlackBerry Enterprise Server™ supports multiple devices, applications, and networks. The BlackBerry Enterprise Server supports all BlackBerry handhelds, regardless of network technology or service provider. The BlackBerry platform integrates with enterprise application servers and messaging platforms and supports major global networks, which currently include GSM™/GPRS, iDEN, CDMA2000® 1X, Mobitex, and DataTAC. Through the BlackBerry Connect Licensing Program™, the server also supports a variety of other mobile devices from participating manufacturers. (Note: Any reference to handhelds in this document refer to the BlackBerry Wireless Handheld.)

Feature and Technical Overview

Benefit	Description
Simplifying management	<p>The BlackBerry solution simplifies management and provides centralized control of the wireless environment with administration tools and performance monitoring tools. You can customize corporate-wide and workgroup-specific policies, such as enforced handheld software upgrades and periodic handheld backups.</p>
Pushing important information to mobile users	<p>Through BlackBerry push technology, users equipped with BlackBerry handhelds can immediately receive up-to-date communications and information, including email and organizer data that are synchronized wirelessly with corporate messaging and collaboration servers. The BlackBerry push model eliminates the need to actively retrieve information from corporate servers. Mobile users can maintain a virtual presence in the workplace, gaining access to important corporate information, email, attachments, address book data, and calendar appointments while away from their desks.</p> <p>The BlackBerry Mobile Data Service feature of the BlackBerry Enterprise Server efficiently distributes information consolidated on application servers wirelessly to a community of handheld users. You can customize software and services to meet the needs of your mobile workforce and improve the efficiency of business operations. Through a fully integrated end-to-end system, mobile users receive data as it is needed. The BlackBerry Enterprise Server is scalable and reliable enough to support global enterprise operations in industries such as legal, financial services, government, healthcare, manufacturing, and international commodities trading.</p>
Keeping data confidential	<p>Maintaining the integrity of enterprise applications requires rigorous attention to security. The BlackBerry solution incorporates some of the most stringent security measures in the industry for maintaining information integrity and confidentiality. BlackBerry handhelds have received the FIPS 140 validation, signifying their adherence to strict government security standards. Using end-to-end AES or Triple DES encryption, data remains encrypted at all points between the handheld and the BlackBerry Enterprise Server. For organizations that already use Secure Multipurpose Internet Mail Extensions (S/MIME) to protect their data, the BlackBerry solution offers optional support for this security standard.</p> <p>To help further protect the confidentiality of the information stored on the handheld, all user data (for example, messages, contacts, memos, and tasks) can be encrypted locally on the handheld using password protection. You can control local encryption and set and enforce other security policies, such as mandatory passwords and password configuration. If the handheld is lost or stolen, you can also lock the handheld wirelessly or erase its information.</p> <p>All aspects of the BlackBerry security model have been audited and verified by @stake Inc., a premier digital security-consulting firm. This independent audit and analysis indicated that "...the BlackBerry security model provides the same level of security as a traditional VPN connection." Visit the Technical Knowledge Center at www.blackberry.com to read the complete results of the audit and analysis.</p>
Extending existing infrastructure	<p>The BlackBerry solution integrates well with existing enterprise components, extending and enhancing them. The BlackBerry Enterprise Server supports a variety of corporate messaging systems and supports corporate data stores and applications through the Mobile Data Service. The BlackBerry architecture routes all communication between the BlackBerry Enterprise Server and the handheld through an authenticated, outbound-only initiated connection in the corporate firewall. No additional configuration is required to handle application data instead of email data communication.</p>

Benefit	Description
Staying connected	The BlackBerry solution uses an Always On, Always Connected® model to provide the mobile workforce with access to vital information. Within the work facility and outside the enterprise walls, the BlackBerry solution creates an extended collaborative environment in which employees, partners, and suppliers can routinely conduct business transactions and maintain contact with each other. Enterprises experience greater productivity, heightened efficiency, and improved communication through wireless access to information.

Feature and Technical Overview

Features

-
- **New in this release**
 - **Messaging**
 - **BlackBerry Mobile Data Service**
 - **BlackBerry Enterprise Server management tools**
 - **Handheld management**
 - **Security**
-

New in this release

Feature	Description
Wireless PIM synchronization	This feature synchronizes personal information management (PIM) application data wirelessly between user handhelds and desktops. When users modify address book entries, tasks, or notes, the changes are wirelessly synchronized. Users can configure wireless PIM synchronization for each related component. You can use the administration tools to configure wireless PIM synchronization for multiple or individual users. The settings that you define override user settings.
Attachment viewing enhancements	The BlackBerry Attachment Service now supports <ul style="list-style-type: none">• viewing .jpg, .bmp, .gif, .png, and .tif image formats• panning, zooming, and rotating images• viewing images embedded in Microsoft® Word .doc files• viewing document information (if available)• viewing footnotes• viewing tracked changes• using the table of contents to jump to document content instead of retrieving content sequentially from the server.• searching through a document on the server if the search query is not found in the attachment content that is already available on the handheld.• the identification of messages with attachments by a unique message icon in the handheld messages list
BlackBerry Handheld Manager	You can push the BlackBerry Handheld Manager to user desktops so that when users connect the handheld to their computer and run the Handheld Manager (which can be configured to start automatically at startup), the Handheld Manager connects to the BlackBerry Router on the BlackBerry Enterprise Server. The BlackBerry Router uses this connection to route data to the handheld instead of through the wireless network.

Feature and Technical Overview

Feature	Description
Wireless enterprise activation	Users can activate a handheld on the BlackBerry Enterprise Server without a physical network connection. For example, users who are away from the office can purchase a replacement for a lost or stolen handheld, contact the administrator to receive a shared secret password, and then activate the handheld wirelessly by starting the Enterprise Activation application and providing the password and their corporate email address.
BlackBerry Handheld Configuration Tool	This tool enables you to load handheld software on multiple handhelds and configure them for deployment. Using the tool, you can <ul data-bbox="489 526 1086 638" style="list-style-type: none">• create and assign software configurations• assign application control policies to third-party applications• configure third-party applications for wireless deployment to handhelds• activate handhelds
Automatic wireless backup	You can automatically back up the following user handheld settings and preferences to the BlackBerry Enterprise Server: <ul data-bbox="489 708 665 821" style="list-style-type: none">• browser bookmarks• autotext entries• font settings• icon positions If a handheld is lost or stolen, and the user has a backup, the backup of their settings and preferences is restored when a new handheld is activated for the user. This feature, combined with wireless handheld activation, enables you to restore BlackBerry functionality for users whose handheld is lost or stolen while they are away from the office.
BlackBerry Application Loader	You can place this configurable upgrade wizard in a central location on the network to provide upgrades for handheld software (for example, the operating system, radio code, BlackBerry applications such as email, and third-party applications) to user computers.
Wireless email settings	Users can now define email settings on their handhelds. This feature, combined with wireless PIM synchronization, eliminates the need for BlackBerry Desktop Software. Users can define the following email settings: <ul data-bbox="489 1124 782 1298" style="list-style-type: none">• email filters• BlackBerry auto-signature• redirection settings• saving sent items in the Sent view• out of office messages• folder redirection

Feature	Description
Handheld management reporting	<p>You can view user handheld information in the administration application to manage handhelds and track assets. The information available in the administration application includes hardware, device configuration, and software attributes, such as</p> <ul style="list-style-type: none"> • model name and number • flash memory size • phone number (if applicable) • password state • BlackBerry application version numbers • third-party applications
Third-party application control	<p>You can define which third-party applications are required on the handheld, permitted on the handheld, or not permitted on the handheld.</p> <ul style="list-style-type: none"> • If an application is required, it is sent automatically to the handheld. • If an application is permitted on the handheld, users can optionally load the application. • If an application is not permitted on the handheld, users cannot load the application. <p>You can also specify which handheld resources a specific third-party application can access (for example, which databases and APIs).</p>
Seamless moves between BlackBerry Enterprise Servers	<p>If multiple BlackBerry Enterprise Servers share a configuration database, you can move users between the BlackBerry Enterprise Servers without requiring users to connect their handheld to their desktop and generate an encryption key. This feature enables you to move users to load balance, consolidate servers, or deploy a new architecture, with minimal disruption to users. You can also use this feature to restore BlackBerry functionality to users if the BlackBerry Enterprise Server on which they reside is unavailable.</p>
Improved fault tolerance	<p>Key BlackBerry Enterprise Server components are now monitored by an independent component called the BlackBerry Controller. If the Controller detects that a component or process has failed, it restarts the component or process automatically. Changes to the product architecture and processing workflow also reduce the impact on system functionality if an individual service stops responding.</p>
Enhanced failover support	<p>Expanded monitoring and troubleshooting documentation describes how to monitor the system, detect issues, and identify recovery strategies that minimize the impact on users (for example, how to move users to a new BlackBerry Enterprise Server if hardware failure occurs).</p>

Feature and Technical Overview

Feature	Description
BlackBerry Mobile Data Service enhancements	<p>Enhancements to the Mobile Data service include</p> <ul style="list-style-type: none"><li data-bbox="491 361 1236 439">• Proxy URL exclusion list: If the Mobile Data Service is connected to a corporate proxy server, Proxy Auto-Configuration (PAC) files are no longer required to permit direct internal URL routing or intranet access support and web filtering rules for external URLs.<li data-bbox="491 444 1236 494">• Increased access control: You can now specify which application servers can push content to handhelds and which application servers BlackBerry users can access.<li data-bbox="491 499 1236 578">• Enhanced XML support: XML parser/generator optimizations on the handheld help application developers create applications that generate less XML-based wireless data traffic with less effort required.<li data-bbox="491 583 1236 661">• Enhanced wireless application transport: Application developers can define how long push data persists being delivered to the handheld. The push application can also query the Mobile Data Service for status updates on pushed content.

BlackBerry software requirements for new features and enhancements

End user features

Feature	BlackBerry Enterprise Server version 4.0	BlackBerry Handheld Software version 2.7	BlackBerry Handheld Software version 4.0
Wireless PIM synchronization	required	required	required
Wireless email settings	required	required	required
Automatic wireless backup	required	required	required
On-handheld help	not applicable	not supported	required
Attachment viewing enhancements			
Image viewing	required	not supported	color only
Document information	required	not supported	required
Footnotes	required	not supported	required
Track changes	required	not supported	required
Document jump	required	not supported	required
Server find	required	not supported	required
Unique message icon for email with an attachment	not applicable	not supported	required
BlackBerry Browser enhancements			
JavaScript™ v1.3 support	required	not supported	required
Offline improvements	not applicable	not supported	required
Usability enhancements	not applicable	not supported	required
Enhanced HTML tables support	required	not supported	required
Ability to email a URL	not applicable	not supported	required
Animated GIF support	not applicable	not supported	required
Partial support for cascading style sheets (WAP 2.0 CSS)	required	not supported	required
Calendar enhancements			
Tentative acceptance	version 2.1 or later	not supported	required
Conflict and adjacent notification	version 2.1 or later	not supported	required
Private flag support	required	not supported	required
Phone enhancements			
Improved call handling when locked	not applicable	not supported	required
Allow outgoing calls when locked	required	not supported	required
Task enhancements			

Feature and Technical Overview

Feature	BlackBerry Enterprise Server version 4.0	BlackBerry Handheld Software version 2.7	BlackBerry Handheld Software version 4.0
Task reminders and recurrences	not applicable	version 2.5 or later	required
Security enhancements			
Content protection	not applicable	not supported	required
Content compression	not applicable	not supported	required
Password keeper	not applicable	not supported	optional feature
Handheld wipe	not applicable	required	required
Wireless encryption key regeneration	required	required	required
AES transport encryption	required	required	required
General user experience improvements			
PIM categories	not applicable	not supported	required
Sent item synchronization	required	required	required
Remote address lookup returns PIN	required	not applicable	not applicable
Support for more address book fields	required	not supported	required
Reconcile now (always present)	version 3.6 or later	required	required
Improved profiles usability	not applicable	not supported	required
Ability to delete BlackBerry applications from the handheld	not applicable	not supported	required



Note: BlackBerry Handheld Software version 4.0 applies to all Java™-based BlackBerry handhelds. BlackBerry Handheld Software version 2.7 applies to the RIM 950 Wireless Handheld™, the RIM 957 Wireless Handheld™, the RIM 850 Wireless Handheld™, and the RIM 857 Wireless Handheld™.

Administration features

Feature	BlackBerry Enterprise Server version 4.0	BlackBerry Desktop Software version 4.0 (optional)	BlackBerry Handheld Software version 2.7	BlackBerry Handheld Software version 4.0
BlackBerry Router and Handheld Manager	required	required	required	required
Wireless enterprise activation	required	not applicable	required	required
Handheld Configuration Tool	required	not applicable	not applicable	not applicable
Remote Application Loader	not applicable	required	not applicable	not applicable
Optional BlackBerry Desktop Manager	not applicable	required	not applicable	not applicable
Handheld management reporting	required	not applicable	required	required
Third-party application control	required	not applicable	not supported	required
Seamless user moves between BlackBerry Enterprise Servers	required	not applicable	required	required
Improved fault tolerance	required	not applicable	not applicable	not applicable
Consolidation of multiple BlackBerry Enterprise Server instances	required	not applicable	not applicable	not applicable
Mobile Data Service improvements				
Proxy URL exclusion list	required	not applicable	not applicable	not applicable
Increased access control	required	not applicable	not applicable	not applicable
Enhanced XML support	required	not applicable	not supported	required
Enhanced wireless application transport	required	not applicable	required	required

i Note: BlackBerry Handheld Software version 4.0 applies to all Java-enabled BlackBerry handhelds. BlackBerry Handheld Software version 2.7 applies to the RIM 950™, the RIM 957™, the RIM 850™, and the RIM 857™.

Software Development Kit features

Feature	BlackBerry Enterprise Server version 4.0	BlackBerry Handheld Software version 4.0
Enhanced Java Technology for the Wireless Industry (JTWI) support	not applicable	required
Enhanced BlackBerry APIs	not applicable	required
XML parser/generator	required	required
Attachment viewing SDK	required	not applicable
Synchronization SDK	required	required

Messaging

The BlackBerry solution provides a secure wireless extension of the corporate messaging environment.

Email

The BlackBerry Enterprise Server integrates seamlessly with existing email accounts. If users configure identical signatures on their handheld and their computer, recipients cannot distinguish between email sent from the handheld or the desktop email program. Email is pushed to handhelds automatically, so users can receive email on their handheld with the same speed and reliability as that of their desktop email program.

Wireless email reconciliation

When users move or delete email messages from their handheld or their desktop email program, or mark messages read or unread, the changes are reconciled wirelessly between their handheld and their computer. Wireless email reconciliation is enabled by default on both the handheld and the BlackBerry Enterprise Server.

Wireless email settings

Users can modify the following settings on the handheld:

Setting	Description
Email filters	Users can create, edit, and modify filters that define an action to perform if an incoming email message matches the filter criteria. For example, users can specify that messages from a particular sender are forwarded to the handheld with high importance.
Save copy in Sent folder	Users can define whether messages sent from the handheld are copied to the Sent Items folder in their desktop email program.
Redirection settings	Users can specify whether messages are redirected to the handheld.
Auto-signature	Users can modify the auto-signature that is appended to messages sent from the handheld.
Out of office reply	Users can create and activate an out of office message.

PIM data

Users can synchronize personal information management (PIM) items such as calendar entries, tasks, memos, and contacts wirelessly so that the entries on their handheld and their desktop email program are consistent. If wireless PIM synchronization is enabled, PIM items are synchronized over the wireless network automatically. With wireless PIM synchronization and wireless email reconciliation, users no longer have to connect their handheld to their computer to synchronize and reconcile messaging and PIM data.

Users can create or edit meeting invitations or accept or decline invitations on their handheld or their desktop email program. Any changes are synchronized wirelessly between the handheld and the computer.

When wireless PIM synchronization is enabled, an initial data synchronization between the handheld and the server to fully synchronize both sides is performed in a way that avoids data loss on either side and is optimized for wireless transmission. After the initial synchronization is complete, incremental changes are synchronized bidirectionally between the handheld and the server.

You configure wireless PIM synchronization in the BlackBerry Manager. The settings can apply to all users on the BlackBerry Enterprise Server or to individual users. Configuration settings include whether wireless PIM synchronization is enabled on the server or a user account, which databases can be synchronized, their synchronization type, their conflict resolution settings, and their address book field mappings. You can also configure wireless PIM synchronization settings using IT policies.

See the *BlackBerry Enterprise Server Administration Guide* for more information on configuring wireless PIM synchronization.

Automatic wireless backup

Automatic wireless backup is enabled on the BlackBerry Enterprise Server by default. Settings and data that are not stored on the server are backed up on the BlackBerry Enterprise Server automatically. The following handheld settings can be backed up using automatic wireless backup:

Application	Settings
Browser	<ul style="list-style-type: none"> • bookmarks • channels • folders • options
Email	<ul style="list-style-type: none"> • attachment viewer options • filters • message list options • searches • settings

Application	Settings
Handheld	<ul style="list-style-type: none"> • auto text • content store • default service selector • device agent • device options • firewall options • font settings • help options • profiles • profiles options • ribbon positions • WAP push options
Phone	<ul style="list-style-type: none"> • hotlist • logs • options
PIM	<ul style="list-style-type: none"> • address book options • calendar options • categories • memo pad options • task options

Automatic wireless backup enables you to make sure that user settings are backed up without requiring users to do so manually. This feature, combined with wireless handheld activation and wireless PIM synchronization, enables you to provide a replacement handheld to users with the same user experience as the missing or stolen handheld, all without a physical network connection.

Attachments

The BlackBerry Attachment Service enables users to view supported email attachments on their handheld in a format that retains the original layout, appearance, and navigation of the attachment. The handheld attachment viewer is fully integrated with the handheld mail application and the BlackBerry Enterprise Server; the Attachment Service uses the existing Messaging Agent link to the user mail server to access attachments directly on the server.

Because the Attachment Service interprets and converts email attachments in binary format, the applications that are associated with the attachment format are not required on the BlackBerry Enterprise Server, and there is no risk of infection on the handheld by macro viruses that operate within those applications.

The attachment viewer is installed automatically with the BlackBerry Enterprise Server Software and supports many formats.

Attachment type	Supported formats
Document	<ul style="list-style-type: none"> • .doc, .dot • .xls • .ppt • .pdf • .txt • .html, .htm • .wpd • .zip
Graphic	<ul style="list-style-type: none"> • .jpg • .bmp • .gif • .png • .tif

Remote address lookup

Remote address lookup enables users to search for a recipient in their corporate directory when they compose an email message on their handheld.

Users can search using letters from the entry's first name, last name, or both. The BlackBerry Enterprise Server searches the corporate directory and returns (up to) the 20 closest matches. If the desired name does not appear in the list, users can request the next 20 search results. When users select a match, they can add the match to their personal address book.

BlackBerry Mobile Data Service

The BlackBerry Mobile Data Service provides the BlackBerry Browser and third-party Java applications with secure access to the Internet and online corporate data and applications. The Mobile Data Service can provide a link to standard servers on the corporate intranet or Internet using standard Internet protocol, such as HTTP or TCP/IP, and encrypts content using the same encryption standard used to encrypt email and other BlackBerry data.

The BlackBerry Enterprise Server and the Mobile Data Service perform the following functions:

Function	Description
Manage handheld requests	<ul style="list-style-type: none"> The Mobile Data Service manages BlackBerry Browser and Java application requests to provide handheld applications with secure access to HTTP, HTTPS, or TCP content on the Internet and intranet using the same channel that is used for BlackBerry email.
Manage push requests	<ul style="list-style-type: none"> The Mobile Data Service accepts and responds to push requests from server-side push applications, provided that the application server is behind the corporate firewall. The Mobile Data Service permits applications to <ul style="list-style-type: none"> push data based on the recipient email address push data to custom handheld applications or to the BlackBerry Browser, browser cache, or message list define the length of time that push data persists The Mobile Data Service responds to application queries for the status of push data.
Provide authentication	<ul style="list-style-type: none"> The Mobile Data Service fits in a corporate sign-on authentication scheme; it provides support for Basic Authentication, NT LAN Manager (NTLM), Lightweight Third-Party Authentication (LTPA), and Kerberos. The Mobile Data Service optionally proxies user credentials for the period that you define. The Mobile Data Service optionally caches cookies for the period that you define.
Provide access control	<ul style="list-style-type: none"> You can assign roles to handhelds and push initiators that control their activity using the Mobile Data Service. You can <ul style="list-style-type: none"> limit push requests from push initiators to specific BlackBerry users restrict the servers that users can access

Feature and Technical Overview

Function	Description
Work with corporate proxy servers	<ul style="list-style-type: none">• Many corporate proxy servers do not permit internal traffic. The Mobile Data Service enables you to provide access to internal content by supporting<ul style="list-style-type: none">• a proxy exclusion list, which defines internal URLs that the Mobile Data Service routes directly instead of going through the corporate proxy server• a Proxy Auto-Configuration (PAC) file
Transcode data	<ul style="list-style-type: none">• The Mobile Data Service converts data to a format that can be interpreted and displayed by the handheld.
Optimize data	<ul style="list-style-type: none">• The Mobile Data Service optimizes and compresses content for viewing in the BlackBerry Browser. The Mobile Data Service can change the data format or remove extraneous information to reduce network traffic and support a simplified application on the handheld.• The Mobile Data Service compresses, for more efficient wireless delivery, XML application data for applications that use the handheld XML parser/generator and the Mobile Data Service.

BlackBerry Enterprise Server management tools

Tool	Description
BlackBerry Manager	Use the BlackBerry Manager to perform the following server and user management tasks: <ul style="list-style-type: none"> • manage user accounts • apply IT policies and IT administration commands • define user and global filters • monitor user and server statistics • modify settings for BlackBerry Enterprise Server services such as the Mobile Data Service or wireless PIM synchronization • manage multiple servers in a single window • send email or PIN messages to users on the BlackBerry Enterprise Server • configure email or console message recipients for notification when BlackBerry Enterprise Server events are logged at a specified level
BlackBerry Configuration Panel	Use the BlackBerry Configuration Panel to modify the BlackBerry Enterprise Server configuration after the server is installed.
Log files	BlackBerry Enterprise Server components write to component-specific log files that are located in a common directory.

IT Policy

Wireless IT policy

Wireless IT policy enables you to define settings and push them wirelessly to users' handhelds. A policy consists of rules that define handheld security, PIM synchronization settings, or other behaviors for the group of users that you define. For example, you can define rules and add them to a custom policy designed for sales personnel and then add the personnel to the policy. Because the policies are pushed wirelessly, they are effective immediately.

When you install the BlackBerry Enterprise Server and add users, the users are added to the Default policy by default. You can also define custom policies and add users to them. IT policies enable you to define consistent behavior to simplify managing BlackBerry in your organization.

Rule	Description
Allow BCC Recipients	Specify whether users can include BCC recipients on email messages.
Allow Peer-to-Peer Messages	Specify whether users can send and receive PIN messages on the handheld.
Allow Phone	Specify whether users can use phone capabilities on the handheld.

Rule	Description
Allow SMS	Specify whether users can use Short Message Service (SMS) messaging on the handheld.
Attachment Viewing	Specify whether users can view attachments on the handheld.
Auto Signature	Specify the signature that is appended automatically to messages sent from the handheld.
Disallow Third Party Application Downloads	Restrict handheld application downloads to those authored by Research In Motion.
Duress Notification Address	Specify an email address that receives notification when users type a handheld password while under duress.
Password Required	Specify whether a password is required on the handheld.
Maximum Security Timeout	Specify the maximum time before a handheld locks if it is unused.

Wireless IT commands

You can send commands to the handheld wirelessly and securely. Wireless IT commands include

Command	Description
Kill handheld	If a handheld is stolen or lost, you can send the Kill handheld command to erase all information and application data on the handheld and disable it.
Set password and lock the handheld	If a handheld is misplaced but likely not stolen or lost, you can send the Set password and lock the handheld command to set a password and lock the handheld to protect the data until the handheld is located. You can also use this feature if a user forgets their handheld password.
Set owner information	If a handheld is stolen or lost, you can send the Set owner information command to make owner information appear when the handheld is locked. The owner information can include contact information that the finder can use to return the handheld.

Handheld management

Deployment

Deploying handhelds wirelessly

Users can receive a new handheld in the office or purchase a new or replacement handheld on the road and activate the handheld without a physical connection to the corporate network. This wireless enterprise activation, combined with automatic wireless backup, enables users who have lost their handheld to get up and running quickly with a replacement handheld that looks and feels like the handheld they lost.

To initiate the wireless activation process, users contact the administrator for a shared secret password, open the handheld Enterprise Activation application, and type their corporate email address and the shared secret password. See "Wireless enterprise activation" on page 45 for more information on the wireless enterprise activation workflow.

Deploying handhelds from a central location

You can use the Handheld Configuration Tool to create standard handheld configurations and apply them simultaneously to multiple handhelds. This enables you to define a consistent handheld configuration for simplified handheld management. When users receive the configured handhelds, they are operational and require no user intervention.

You can use the Handheld Configuration Tool to perform the following actions simultaneously for multiple users:

- load appropriate handheld software from a central location
- load the appropriate user data, including
 - service books
 - calendar items
 - address book entries
 - tasks
 - memos
 - email messages
 - existing handheld options (if present)

Redistributing handhelds wirelessly

You can provide an existing replacement handheld to a user and activate the handheld on user accounts without a physical connection to the corporate network. You can send the **Kill Handheld** command to a handheld that was associated with a different user account, provide the handheld to a new user, and deploy it wirelessly. See "Deploying handhelds wirelessly" on page 24 for more information.

Maintenance and upgrades

Upgrading handheld software using the administration computer

You can upgrade handheld software using the administration computer by collecting handhelds that require software upgrades and using the Handheld Configuration Tool to upgrade the handheld software through a connection to the administration computer.

Sending upgrades to handhelds using the Application Loader

You can send handheld software upgrades to user computers that have the Handheld Manager installed by sending an email with a link or posting a link on a web site to the network location from which users can run the BlackBerry Application Loader. To upgrade, users connect the handheld to the computer, start the Handheld Manager, and then run the Application Loader from the link.

Forcing handheld software upgrades using the Desktop Manager

You can push handheld software upgrades to user computers that have the optional BlackBerry Desktop Manager software (which includes the Handheld Manager and Application Loader) installed. When the user runs the Desktop Manager, the user is prompted and forced to upgrade the handheld.

Security

The BlackBerry solution enables users to send and receive email and access corporate data wirelessly, while seamlessly protecting data against attack. The BlackBerry Enterprise Solution uses Triple Data Encryption Standard (Triple DES) or Advanced Encryption Standard (AES) encryption to encrypt data in transit. Data remains encrypted during transit and is never decrypted between the BlackBerry Enterprise Server and the handheld.

Encryption

Encryption is the scrambling of data based on a key. An encryption algorithm is designed so that only the parties that know the secret key can decrypt the encrypted data or ciphertext.

Triple-DES

BlackBerry uses three iterations of the Data Encryption Standard (DES) algorithm with three 56-bit keys, in cipher block chaining (CBC) mode for an overall key length of 168 bits. The encryption procedure is the same as regular DES, but it is repeated three times. With Triple DES, the data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the first key.

Advanced Encryption Standard

AES was developed to replace DES. AES provides a better combination of security and performance than DES or Triple DES. AES provides greater security against brute-force attacks by offering a larger key size. BlackBerry uses 256 bit keys in CBC mode to encrypt data that is sent between the BlackBerry Enterprise Server and the handheld.

Confidentiality

Confidentiality makes sure that only the intended recipient can view the contents of a message. Confidentiality is typically achieved using encryption.

BlackBerry uses a symmetric key algorithm to encrypt and decrypt data. The symmetric key algorithm provides strong security and complete confidentiality of sensitive user information. The BlackBerry Wireless Handheld compresses and encrypts the message using a key that is unique to that handheld. When the BlackBerry Enterprise Server receives a message from the handheld, it decrypts the message using the handheld's unique key. The BlackBerry Enterprise Server and the handheld are the only parties that know the value of the master encryption key, thus providing confidentiality to the recipients.

Integrity and authenticity

Integrity enables a recipient to detect if a message has been tampered with in transit. *Authenticity* makes sure that the recipient can identify the sender and trust that the sender actually did send the message.

The BlackBerry solution relies on its encryption mechanism to provide integrity and authenticity based on a known message format. The decrypted and decompressed message must conform to a known message format. If it does not conform, the recipient knows that the message has been altered in transit because only the BlackBerry Enterprise Server and the handheld know the value of the symmetric encryption key. The handheld automatically rejects any messages that do not produce the known message format upon decryption.

Content protection

Content protection encrypts data that is stored on the handheld using 256 bit AES. The handheld also encrypts email messages and meeting requests that it receives when it is locked.



Tip: You can use the Content Protection Strength IT policy to define the cryptographic strength of the key that encrypts data when the handheld is locked.

If the user enables content protection on the handheld, the following items are secured:

Handheld application	User data
Email	<ul style="list-style-type: none">• subject• email addresses• message body• attachments
Calendar	<ul style="list-style-type: none">• subject• location• organizer• attendees• notes included in the appointment or meeting request
MemoPad	<ul style="list-style-type: none">• title• information in the note body
Tasks	<ul style="list-style-type: none">• subject• information in the task body
Contacts	<ul style="list-style-type: none">• all information except for title and category
Auto Text	<ul style="list-style-type: none">• all entries that the original text is replaced with
BlackBerry Browser	<ul style="list-style-type: none">• content that is pushed to the handheld• web sites that are saved on the handheld• browser cache

Third-party application control

You can use the BlackBerry Handheld Configuration Tool to control third-party applications in the following ways:

- allow or disallow third-party applications from being downloaded to handhelds
- create application control policies that define which resources (for example, email, phone, and handheld keystore) third-party applications can access on the handheld.
- create policies that define the type of connections that a third-party application deployed on the handheld can establish (for example, opening network connections inside the firewall)
- assign application control policies, which specify the third-party applications that can be downloaded to a handheld
- send third-party applications to handhelds wirelessly (applications that are required for a particular user are pushed wirelessly to the handheld and are automatically installed)

IT policies and IT commands

Wireless IT commands

Wireless IT commands enable you to send commands wirelessly and securely to handhelds to manage handheld security. They enable you to respond immediately to a lost or stolen handheld and protect confidential enterprise information. Use wireless IT commands to perform the following actions:

- delete handheld application data
- set or reset a password and lock the handheld
- disable a handheld and delete stored data
- disable a handheld and delete all applications and stored data

See the *BlackBerry Enterprise Server Handheld Management Guide* for more information on Wireless IT commands.

Wireless IT policies for security settings

You can set IT policies that are sent wirelessly to user handhelds and override user-defined security settings.

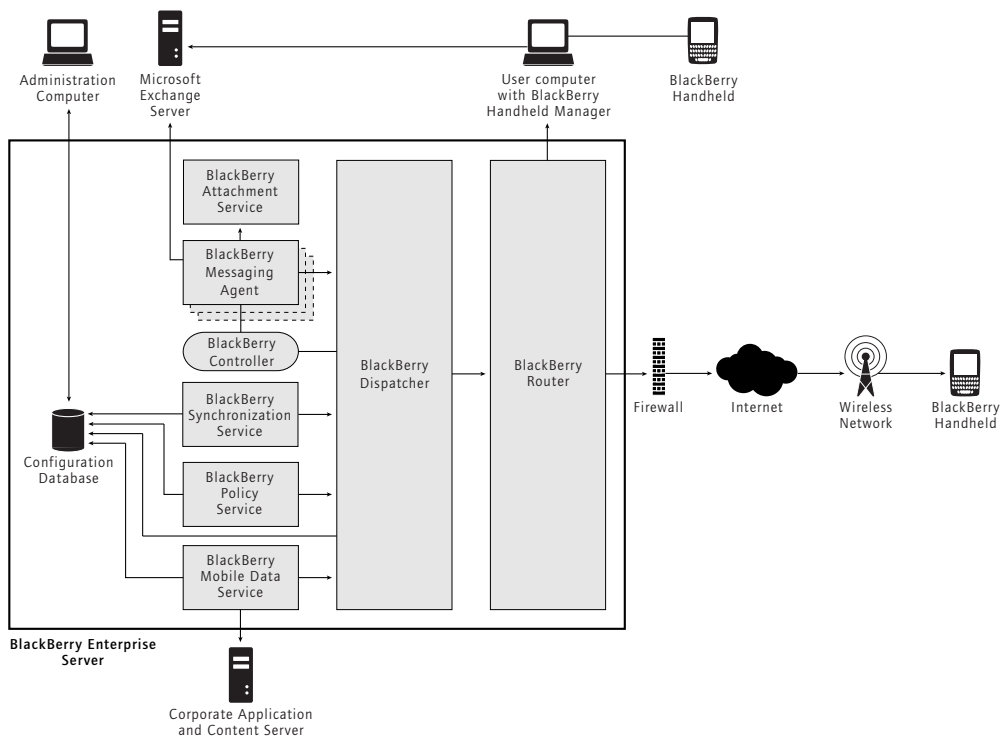
IT policy	Description
IT policies for security	Set IT policies that define security settings for the BlackBerry handheld and BlackBerry Desktop Manager. For example, you can specify whether a handheld password is required, the length of time that a password can exist before it becomes invalid, and the length and composition of a password. You can also specify encryption key details using IT policies.
Wireless policy deployment	All IT policies, including security settings, can be applied wirelessly when the settings are defined. To provide wireless delivery of new policies and immediate user adoption, IT policy settings are written automatically to the user configurations. To make sure that the settings are always current, the BlackBerry Enterprise Server periodically transmits handheld settings to the handheld wirelessly.
Group policies	The IT policy feature enables you to define a policy for a group of users and apply it to all users in the group instead of creating a policy for each user. For example, you can create a policy for executives, and assign each executive to the group policy.

See the *BlackBerry Enterprise Server Administration Guide* for information on managing IT policies.

Architecture

- Components
- Remote components

The BlackBerry Enterprise Server consists of services that provide functionality and components that monitor services and process, route, compress, and encrypt data, and communicate with the wireless network.



BlackBerry Enterprise Server for Microsoft Exchange architecture

Components

Component	Description
Administration computer	The administration computer runs the BlackBerry Enterprise Server administration software. The computer connects to the configuration database for remote administration.
BlackBerry Attachment Service	The BlackBerry Attachment Service converts supported attachments into a format that can be viewed on the handheld. The Attachment Service can also be installed on a computer separate from the BlackBerry Enterprise Server.
BlackBerry Dispatcher	The BlackBerry Dispatcher performs data encryption and compression services for all BlackBerry data, and routes the data through the BlackBerry Router to and from the wireless network.
BlackBerry Messaging Agent	The BlackBerry Messaging Agent connects to the mail server to provide email, calendar, address lookup, attachment, and wireless encryption key generation services. The BlackBerry Messaging Agent consists of a number of agents. It also acts as a gateway for the Mobile Synchronization Service to access PIM data on the mail server and synchronizes configuration data between the SQL configuration database and user mailboxes.
BlackBerry Synchronization Service	The BlackBerry Synchronization Service synchronizes PIM application data wirelessly between the handheld and the mail server
BlackBerry Mobile Data Service	The BlackBerry Mobile Data Service provides access to online content and applications on the corporate intranet or Internet.
BlackBerry Policy Service	The BlackBerry Policy Service performs administration services such as wireless IT policy, wireless IT commands, and wireless service book provisioning.
BlackBerry Router	The BlackBerry Router connects to the wireless network. It also routes data to handhelds that are connected using the BlackBerry Handheld Manager.
Configuration database	The configuration database is a SQL database that contains configuration information, which is used by the BlackBerry Enterprise Server services that do not connect to the mail server directly. The configuration database includes the following information: <ul style="list-style-type: none"> • details about the connection to the wireless network • user list • PIN to email mapping for Mobile Data Service push functionality • a read-only copy of each user security key
BlackBerry Controller	The BlackBerry Controller monitors the Messaging Agent and the BlackBerry Dispatcher and restarts them if they stop responding.
Corporate application and content server	The corporate application and content server provides push application and intranet content for the Mobile Data Service.
Microsoft® Exchange Server	The Microsoft Exchange Server is the server on which user mailboxes reside.

Component	Description
User computer with BlackBerry Handheld Manager	The user computer with the BlackBerry Handheld Manager enables users to connect their handhelds using a serial or USB connection and use the connection to route all BlackBerry data. Handheld traffic bypasses the wireless network while the handheld is connected to the computer. The Handheld Manager connects to the BlackBerry Router, which routes data directly to the handheld through this connection. The Handheld Manager can be installed separately or as part of an optional full BlackBerry Desktop Manager installation. The Handheld Manager is an optional component, but it is required to support a bypass connection to the BlackBerry Router.

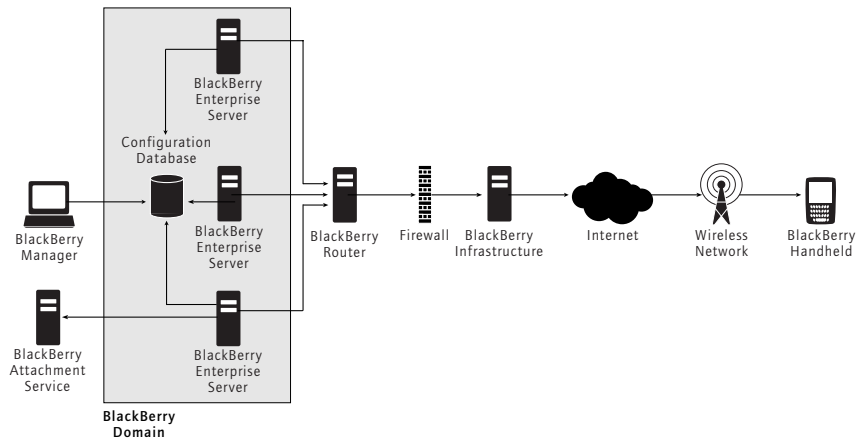
Remote components

The following components are installed with the BlackBerry Enterprise Server installation, but they can also be installed optionally on a remote computer.

Component	Description
BlackBerry Manager	The BlackBerry Manager administration program can be installed on a remote computer to manage one or more BlackBerry Enterprise Servers.
BlackBerry Attachment Service	The BlackBerry Attachment Service can be installed on a remote computer to convert attachments for one or more BlackBerry Enterprise Servers. While the Attachment Service does not have a large impact on performance, if you expect high usage of the attachment viewing feature in your environment, you can monitor the impact, and then install the Attachment Service on a remote computer at a later time.
BlackBerry Router	The BlackBerry Router can be installed on a remote computer to route BlackBerry traffic to and from the BlackBerry Infrastructure for one or more BlackBerry Enterprise Servers. The BlackBerry Router does not have a large impact on performance, so most organizations choose this configuration for network topology reasons. If you install the BlackBerry Router on a remote computer, consider the following: <ul style="list-style-type: none"> the BlackBerry Router can only connect to a single SRP address (for example, <code>srp.na.blackberry.net</code>) if your users use the BlackBerry Desktop Software or the Handheld Manager, make sure that those applications can connect to the BlackBerry Router
Configuration database	When you install the BlackBerry Enterprise Server, you can specify a remote computer on which to install the SQL database and configure multiple servers to use the remote configuration database. BlackBerry Enterprise Servers that share a database belong to the same BlackBerry Domain. Users can be moved easily between servers in the same BlackBerry Domain for load balancing or to restore BlackBerry functionality if the BlackBerry Enterprise Server on which they reside is unavailable.

Feature and Technical Overview

The following sample distributed architecture shows three BlackBerry Enterprise Servers sharing a single configuration database, which resides on a separate computer. Users can be moved to any server in the BlackBerry Domain using the BlackBerry Manager that connects to the shared configuration database. The servers connect to the BlackBerry Infrastructure using the same BlackBerry Router. A single BlackBerry Enterprise Server is configured to connect to the remote BlackBerry Attachment Service.

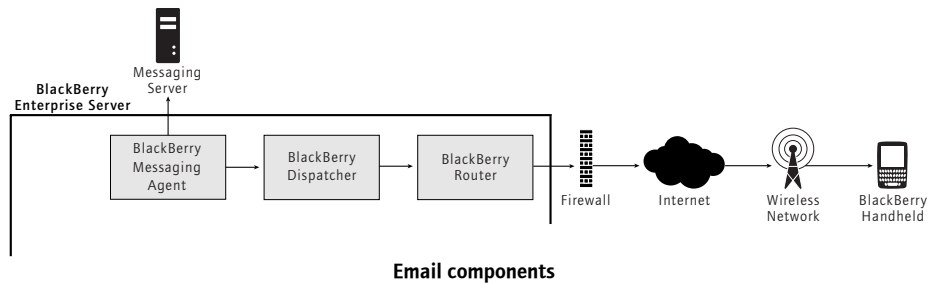


Sample BlackBerry Enterprise Server architecture with remote components

Workflows



- Email
- PIM data
- Mobile data
- Wireless enterprise activation
- BlackBerry Router

Email




Email sent to a handheld

1. **New message arrives:** A message arrives in the user's Microsoft Exchange Mailbox. Microsoft Exchange notifies the BlackBerry Messaging Agent that a new message has arrived for the user.
2. **Applies filters:** The Messaging Agent checks the message fields against global filter rules and filters the messages that meet the filter criteria. After it applies the global filter rules, the BlackBerry Enterprise Server applies any user-defined filters to messages that meet the filter criteria.
3. **Sends to the BlackBerry Dispatcher:** The Messaging Agent sends the first 2 KB portion of the message to the BlackBerry Dispatcher.
4. **Compresses and encrypts:** The BlackBerry Dispatcher compresses the first portion of the message, encrypts it with the user encryption key, and then passes it to the BlackBerry Router for delivery to the handheld.

5. **Sends to the wireless network:** The BlackBerry Router sends the first portion of the message over port 3101 to the wireless network, which verifies that the PIN belongs to a valid handheld that is registered on the wireless network.
6. **Returns confirmation:** The wireless network locates the BlackBerry handheld and delivers the message. The handheld sends delivery confirmation to the BlackBerry Dispatcher, which passes it to the Messaging Agent. If the BlackBerry Enterprise Server does not receive confirmation within four hours, it resubmits the message to the wireless network.
 -  **Note:** The confirmation is a radio-level confirmation. It confirms that the message was delivered to the handheld, but it does not confirm that the user received or read the message.
7. **Arrives on the handheld:** The handheld decrypts and decompresses the message so that the user can view it, and notifies the user of its arrival.
 -  **Note:** The workflow for wireless calendar or email reconciliation items is the same as the preceding workflow; however, the Messaging Agent detects that the item is a calendar entry or a moved, deleted, or read/unread message.

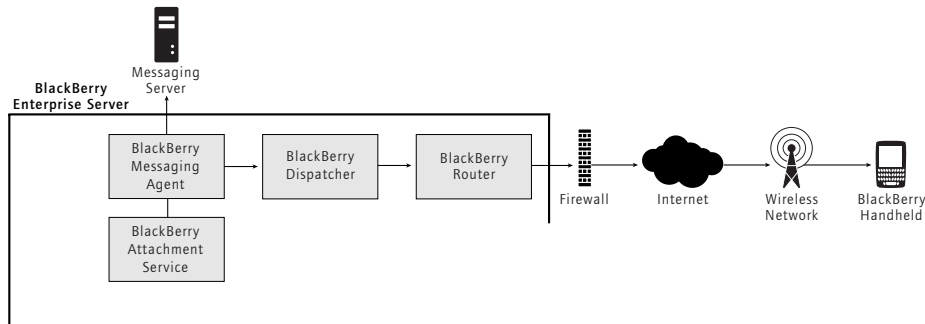
Email sent from a handheld

1. **Message is sent from handheld:** The user sends a message from the handheld. On the handheld, the message is assigned the RefId. If the message is a meeting invitation or calendar item, the handheld appends the calendar information to the message.
2. **Compresses and encrypts:** The handheld compresses and encrypts the entire message.
3. **Sends to the BlackBerry Enterprise Server:** The message is sent to port 3101 over the wireless network to the BlackBerry Enterprise Server.
 -  **Note:** The BlackBerry Enterprise Server accepts only encrypted messages from the handheld. If the message is not encrypted, the BlackBerry Enterprise Server rejects it.
4. **Decrypts and decompresses:** The BlackBerry Dispatcher uses the user encryption key to decrypt and decompress the message. If the message cannot be decrypted using the unique encryption key, the BlackBerry Enterprise Server ignores the message and sends an error to the handheld.
5. **Delivers to mailbox:** The Messaging Agent places the message in the user's Microsoft Exchange mailbox.
6. **Copied in Sent folder:** The Messaging Agent places a copy of the message in the Sent Items folder in the desktop email program. This step does not take place if the **Don't save a copy to the Sent Items folder** option is enabled in the user settings and that setting is permitted on the BlackBerry Enterprise Server.

7. **Routes to recipients:** The Microsoft Exchange Server routes the message to the recipients. As a result, a message that is sent from the handheld is the same as a message that is sent from the desktop; messages originate from the user corporate email address, and, if necessary, a copy is placed in the Sent Items folder.

Note: The workflow for wireless calendar or email reconciliation items is the same as the preceding workflow; however, the Messaging Agent detects that the item is a calendar entry or a moved, deleted, or read/unread message.

Attachments



Attachment components

1. **Message with attachment arrives:** A user receives a message with an attachment on the handheld.
2. **Verifies attachment:** The Messaging Agent verifies that the attachment is a valid format for conversion. If the format is not valid, and the handheld is a Java-based handheld, the Open Attachment menu item does not appear on the recipient's handheld
3. **Attachment request:** The handheld user clicks Open Attachment to view the attachment on the BlackBerry handheld.
4. **Sends request:** The request is sent from the handheld Attachment Viewer to the Messaging Agent, which invokes the Attachment Service using port 1900.
5. **Retrieves document:** The Attachment Service retrieves the document in binary format from the user mail file using the Messaging Agent link to the mail server.
6. **Distills document:** The Attachment Service distills the document.
7. **Extracts and stores document information:** The Attachment Service extracts the document content, layout and appearance, and navigation information. The information is organized, stored, and linked

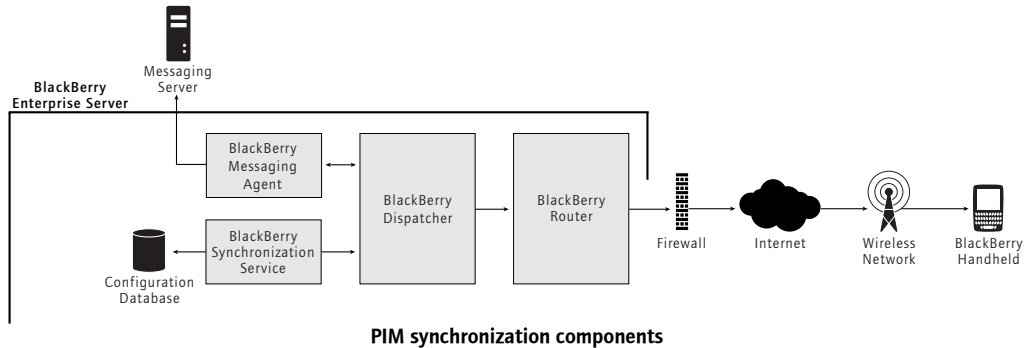
in an efficient, proprietary Document Object Model (DOM) in a binary Extensible Markup Language (XML) style.

8. **Formats document for the handheld:** The Attachment Service conversion process formats the document for the handheld and converts it to Universal Content Stream (UCS) format. The formatting is based on the request for content (for example, page and paragraph information or search words) and the available handheld information (for example, screen size, display, or available space).
9. **Sent to the Messaging Agent:** The Attachment Service sends the UCS data to the Messaging Agent using a TCP/IP connection to port 1900.
10. **Sends to the BlackBerry Dispatcher:** The Messaging Agent sends the converted attachment to the BlackBerry Dispatcher.
11. **Compresses and encrypts:** The BlackBerry Dispatcher compresses the first portion of the attachment, encrypts it with the user encryption key, and then passes it to the BlackBerry Router for delivery to the handheld.
12. **Sends to the wireless network:** The BlackBerry Router sends the first portion of the attachment over port 3101 to the wireless network, which verifies that the PIN belongs to a valid handheld that is registered on the wireless network.
13. **Returns confirmation:** The wireless network locates the BlackBerry handheld and delivers the attachment. The handheld sends delivery confirmation to the BlackBerry Dispatcher, which passes it to the Messaging Agent. If the BlackBerry Enterprise Server does not receive confirmation within four hours, it resubmits the attachment data to the wireless network.
14. **Decrypts and decompresses:** The handheld uses the user encryption key to decrypt and decompress the attachment so that the user can view it.
15. **Viewed on the handheld:** The user can view the attachment on the handheld by selecting a section from the table of contents or viewing the full attachment. The original formatting of the attachment, including indents, tables, fonts, font formatting, and bullets is reflected on the handheld.

Address lookup

1. **Lookup on handheld:** The user performs an address lookup on the handheld. On the handheld, the request is assigned a RefId.
2. **Compresses and encrypts:** The handheld compresses and encrypts the request using Triple DES or AES encryption.
3. **Sent to the BlackBerry Enterprise Server:** The request is sent over the wireless network, using port 3101, to the BlackBerry Enterprise Server.
4. **Decrypts and decompresses:** The BlackBerry Dispatcher uses the encryption key to decrypt and decompress the request, and then passes it to the Messaging Agent.
5. **Retrieves matches from the Global Address Book:** The Messaging Agent queries the Global Address Book on the Microsoft Exchange server and retrieves the 20 closest matches to the lookup request.
6. **Sends to the BlackBerry Dispatcher:** The Messaging Agent sends the lookup results to the BlackBerry Dispatcher.
7. **Compresses and encrypts:** The BlackBerry Dispatcher encrypts the results with the user encryption key, compresses them, and passes the results to the BlackBerry Router for delivery to the handheld.
8. **Sends to the wireless network:** The BlackBerry Router sends the results over port 3101 to the wireless network, which verifies that the PIN belongs to a valid handheld that is registered on the wireless network.
9. **Returns confirmation:** The wireless network locates the BlackBerry handheld and delivers the results. The handheld sends delivery confirmation to the BlackBerry Dispatcher, which passes it to the Messaging Agent. If the BlackBerry Enterprise Server does not receive confirmation within four hours, it resubmits the lookup results to the wireless network.
10. **Decrypts and decompresses:** The handheld uses the user encryption key to decrypt and decompress the lookup results so that the user can view them.
11. **Viewed on the handheld:** The user can view or email the lookup matches on the handheld or add them to the handheld address book.

PIM data



Initial synchronization

1. **Receives synchronization service book:** A user activates a new handheld, or upgrades an existing handheld, and receives the synchronization service book.
2. **Handheld requests configuration:** The handheld requests the synchronization configuration from the BlackBerry Synchronization Service. The configuration information includes whether wireless PIM synchronization is enabled on the server, which databases can be synchronized, their synchronization type, and their conflict resolution settings.

i Note: All data sent between the handheld and the BlackBerry Enterprise Server is compressed and encrypted.

3. **Initial synchronization:** The server returns the configuration information, and the databases are synchronized based on the information. A synchronization agent on the handheld tracks which databases can be synchronized wirelessly. After a database is registered for wireless synchronization, it can no longer be synchronized or restored using the Desktop Software. If there is existing data on the handheld and the server, the records are merged, added, or updated during synchronization. If there is data on only the handheld or the server, the data is restored from that location.

i Note: No records are deleted during the initial synchronization process.

4. **Initial synchronization complete:** Initial synchronization is complete when the data on the handheld and the server are synchronized. Future changes on the handheld or the server are synchronized wirelessly through the PIM synchronization process. If the user modifies data in the handheld or

desktop PIM application during initial synchronization, the records are synchronized during the PIM synchronization process after the initial load is complete.



Tip: If the handheld is connected to a computer that has the Handheld Manager installed (either standalone or as part of the optional Desktop Manager) and running, the initial synchronization can take place over the connection to the BlackBerry Router on the BlackBerry Enterprise Server instead of over the wireless network.

PIM synchronization

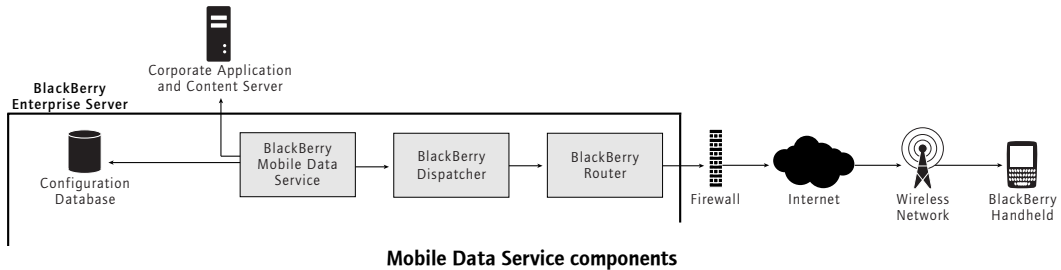
1. **User changes data:** The user saves changes to PIM data or handheld settings (for example, a new autotext entry) in the handheld or desktop PIM application, and the change is added to the changelist on the handheld or the server (depending on where the change was made).
2. **Sends changelist:** The changelist, which includes the target PIM application database and record information, is sent to the Synchronization Service. Changes to PIM data are sent immediately (along with other entries in the changelist for that user). Changes that are not triggered immediately are sent at the batch synchronization interval set on the server; the default is every ten minutes.



Notes: All data sent between the handheld and the BlackBerry Enterprise Server is compressed and encrypted. To prevent change collisions, only a single server or handheld changelist per user can be sent wirelessly at a time.

3. **Database entry:** The Synchronization Service receives the synchronization request and writes a synchronization request entry in the SyncRequest table.
4. **Sends synchronization data:** The Synchronization Service sends the changed records through the BlackBerry Dispatcher to the handheld.
5. **Acknowledgement:** The handheld acknowledges each record that it receives successfully. For each acknowledged record, the Synchronization Service removes the corresponding synchronization request entry from the SyncRequest table and writes an entry in the SyncRecordState table. Each PIM database record has a unique identifier that is mapped to the corresponding record on the handheld. Subsequent changes to a record can be easily associated with the corresponding record on the other side.

Mobile data



BlackBerry Browser content requested on handheld

1. **Content request:** A user requests Internet or intranet content on the handheld.
2. **Sends request:** The request is sent using port 3101 to the BlackBerry Enterprise Server on which the user resides. The BlackBerry Dispatcher sends the request to the Mobile Data Service using port 3201.
3. **Retrieves content:** The Mobile Data Service creates an HTTP session for the user and retrieves the requested content.
4. **Submits content:** The Mobile Data Service converts the content for viewing on the handheld and sends it to port 3201 on the BlackBerry Enterprise Server.
5. **Compresses and encrypts:** The BlackBerry Dispatcher compresses the content, encrypts it with the user's encryption key, and then sends it to the BlackBerry Router for delivery to the handheld.
6. **Sends to the wireless network:** The BlackBerry Router sends the content using port 3101 to the wireless network, which verifies that the PIN belongs to a valid handheld that is registered on the wireless network.
7. **Returns confirmation:** The wireless network locates the BlackBerry handheld and delivers the content. The handheld sends delivery confirmation to the BlackBerry Router. If the Mobile Data Service does not receive confirmation within the flow control timeout limit, it sends a cancellation to the wireless network for the pending content.
8. **Arrives on handheld:** The handheld decrypts and decompresses the content so that the user can view it. The handheld application detects the content and displays it.


Content requested with access control enabled

With access control enabled, the Mobile Data Service requests content from the content server in the following sequence:

1. **Content request:** A user requests Internet content from the content server.
2. **Creates an HTTP session:** If pull access control is enabled for the Mobile Data Service and the request is allowed, the Mobile Data Service creates an HTTP session for the user, and then sends the HTTP request to the content server.
3. **Resends HTTP request:** If pull access control fails for the request, the HTTP request is not sent by the Mobile Data Service to the origin server. The "HTTP 403 error" message displays in the BlackBerry Browser. After the user sends the HTTP authentication login and password, the Mobile Data Service resends the HTTP request with the necessary HTTP authentication information to the content server.

Application content pushed to handheld

1. **Sends request:** A custom push application, which resides on a server behind the corporate firewall, sends an HTTP POST request to the Mobile Data Service central push server to the web server listen port (default 8080). The application specifies the BlackBerry Enterprise Server host name and the Mobile Data Service web server connection listen port.
2. **Configuration database lookup:** The central Mobile Data Service push server checks the configuration database for the following information about the recipients that are defined in the push application:
 - BlackBerry Enterprise Server on which the user account resides
 - the PIN that is associated with the recipient email address
 - whether the recipient account is enabled
 - whether the recipient account was soft-deleted

 **Note:** Recipients who do not appear in the BlackBerry directory, or who have a disabled or soft-deleted BlackBerry account, do not receive push content.
3. **Returns response:** The Mobile Data Service responds to the push application to acknowledge that it is processing the request and closes the connection.
4. **Routes to recipients:** The central Mobile Data Service push server routes the content to the push server connection listen port (default 81) on the Mobile Data Service on the BlackBerry Enterprise Servers on which the recipients reside.
5. **Submits content:** The Mobile Data Service converts the content for viewing on the handheld and sends it using port 3201 to the Messaging Agent.

6. **Sent to the BlackBerry Enterprise Server:** The Messaging Agent sends the message to the BlackBerry Enterprise Server.
7. **Encrypts and compresses:** The BlackBerry Enterprise Server encrypts the content with the user's encryption key, compresses it, and then sends it to the BlackBerry Router for delivery to the handheld.
8. **Sent to the wireless network:** The BlackBerry Router sends the content over port 3101 to the wireless network, which verifies that the PIN belongs to a valid handheld that is registered on the wireless network.
9. **Returns confirmation:** The wireless network locates the BlackBerry handheld and delivers the content. The handheld sends delivery confirmation to the BlackBerry Enterprise Server. If the Mobile Data Service does not receive confirmation within the flow control timeout limit, it sends a cancellation to the wireless network for the pending content.
10. **Detects content:** The handheld application that listens on the port number specified in the push application (for example, the BlackBerry Browser listens for push application connections on port 7874) detects the inbound content, and then displays it when the user invokes it.

Wireless enterprise activation

1. **New BlackBerry:** A user receives or purchases a new BlackBerry and contacts the IT department to activate it.
2. **Administrator creates a password:** The administrator uses the BlackBerry Manager to create a temporary wireless activation password for the user account and communicates that password to the user. The password applies to the user account only and becomes invalid when
 - a handheld is successfully activated on the account using the password
 - five consecutive unsuccessful activation attempts are made on the account
 - the user fails to activate a handheld within the expiry window
3. **User initiates wireless activation:** The user opens the Enterprise Activation application on the handheld and types the appropriate corporate email address and wireless activation password.
4. **Handheld sends activation request:** The handheld sends an activation request email to the corporate email account. The email contains information about the handheld, such as routing information and the handheld activation public keys. See the *BlackBerry Wireless Enterprise Activation Technical Overview* for information on public key encryption.
5. **Server sends activation response:** The BlackBerry Enterprise Server sends the handheld an activation response that contains routing information about the BlackBerry Enterprise Server and the server's public keys.
6. **Establishes and confirms keys:** The BlackBerry Enterprise Server and the handheld establish a master encryption key. Both the BlackBerry Enterprise Server and the handheld confirm their knowledge of the master key to one another. If key confirmation succeeds, the activation proceeds, and further communication is encrypted.
7. **Sends IT policies:** The BlackBerry Enterprise Server sends the user's IT policies that apply to the handheld, and the handheld accepts them. If the handheld cannot accept the IT policies, as a security measure, the activation does not complete.
8. **Sends service books:** The BlackBerry Enterprise Server sends the appropriate service books (for example, messaging service book, wireless calendar service book, browser service book, and other service books) to the handheld. The user can now send messages from and receive messages on the handheld.
9. **Loads data:** If the user is configured for wireless PIM synchronization and wireless backup, and wireless calendar synchronization is enabled, the BlackBerry Enterprise Server sends data to the handheld, including:
 - calendar entries

- address book entries
- tasks
- memos
- email messages
- existing handheld options (if applicable) that were backed up using automatic wireless backup



Tip: If the user is in the office, you can use the Handheld Manager to load the data using a connection to the BlackBerry Router. This option enables you to avoid sending large quantities of data over the wireless network. You can also enforce this option through an IT policy rule.

BlackBerry Router

1. **User connects the handheld:** The user connects the handheld to a desktop computer that is running the Handheld Manager.
2. **Authenticates handheld:** The BlackBerry Router uses a unique authentication protocol to verify that the user is a valid user and is not masquerading as another user. The authentication sequence uses the authentication information that the BlackBerry Enterprise Server and the handheld use to validate each other to determine whether the connection is valid. The BlackBerry Router does not learn the value of the master encryption key that passes between the handheld and the server.
3. **Data bypasses the wireless network:** The BlackBerry Router and the Handheld Manager manage all data flow to and from the handheld over the physical connection behind the firewall.
 - Data from the handheld is sent to the BlackBerry Router using the Handheld Manager.
 - Data to the handheld is sent from the BlackBerry Router to the handheld using the Handheld Manager.

All data sent between the handheld and the BlackBerry Enterprise Server is compressed and encrypted just as it is with wireless data flow. When the user disconnects the handheld or closes the Handheld Manager, the wireless data flow is restored.



Index

A

- access control, Mobile Data Service, 14, 21, 43
- activating, wireless
 - feature description, 12
 - redistribution, 25
 - workflow, 45
- Advanced Encryption Standard, 8, 27, 39
- AES *See* Advanced Encryption Standard
- application data, push, 43
- architecture, BlackBerry Enterprise Server, 31
- assigning roles, using Mobile Data Service, 21
- attachments
 - functional description, 20
 - sending, 37
 - supported formats, 20
 - viewing, 11
- authentication, 21
- auto-signature, 12, 18

B

- backing up, handheld, 12, 19
- BlackBerry Application Loader, upgrading
 - handheld, 12, 26
- BlackBerry Attachment Service, 11, 32, 33, 37
- BlackBerry Configuration Panel, 23
- BlackBerry Controller
 - description, 32
 - monitoring with, 13
- BlackBerry Dispatcher, 32, 35
- BlackBerry Enterprise Server
 - architecture, 31
 - components, 32
 - management tools, 23
 - monitoring with BlackBerry Controller, 13
 - moving users between servers, 13
 - remote components, 33

- troubleshooting documentation, 13
- workflows, 35–46
- BlackBerry Handheld, 13, 24, 26
- BlackBerry Handheld Configuration Tool
 - configuring handheld, 12
 - upgrading handheld, 26
- BlackBerry Handheld Manager
 - pushing data, 11
- BlackBerry Manager, 23, 33
- BlackBerry Messaging Agent, 32
- BlackBerry Policy Service, 32
- BlackBerry Router
 - description, 32, 33
 - workflow, 46
- BlackBerry Synchronization Service, 32, 40
- BlackBerry Wireless Solution
 - benefits, 7–9
 - deployment, 7
 - end-to-end connectivity, 7
 - feature description, 7
 - infrastructure, 8
 - management, 8
 - multiple application support, 7
 - multiple device support, 7
 - multiple network support, 7
 - new features, 11–14
 - pushing information, 8
 - secure data, 8
 - software requirements, 15–17
- browser data, viewing, 42

C

- components, BlackBerry Enterprise Server
 - local installation, 32
 - log files, 23

- remote installation, 33
- confidentiality, 27
- configuration database
 - connected by administration computer, 32
 - description, 32
 - multiple servers sharing, 13
 - remote installation, 33
- configuring
 - BlackBerry Handheld, 12
 - email settings, 12
 - third-party applications, 13
- content protection, 16, 28

D

- data
 - confidentiality, 27
 - integrity, 27
 - protection, 16
 - security, 8, 28
- deployment, streamlining, 7
- Desktop Manager, upgrading handheld, 26

E

- email
 - filters, 12, 18, 35
 - functional description, 18
 - reconciling, 18
 - redirecting, 18
 - saving copy to Sent folder, 18
 - settings, 12
 - wireless settings, 18
 - workflows, 35–37
- encryption key, 13, 16, 26, 35, 39
- end-to-end connectivity, 7

F

- features
 - attachments, 11, 20
 - automatic wireless backup, 12

- BlackBerry Application Loader, 12
- BlackBerry Controller, 13
- BlackBerry Handheld, 13, 24, 26
- BlackBerry Handheld Configuration Tool, 12
- BlackBerry Handheld Manager, 11
- BlackBerry Mobile Data Service, 14, 21
- content protection, 28
- data confidentiality, 27
- data integrity, 27
- email, 18
- failover support, 13
- IT policies, 14, 23, 29
- PIM data, 11, 19
- remote address lookup, 21
- seamless moves between servers, 13
- security, 26
- server management tools, 23
- software requirements, 15–17
- third-party application control, 13, 29
- wireless activation, 12
- wireless email settings, 12
- wireless IT policy and command push, 29
- filters, email, 12, 18, 35

I

- infrastructure, extending, 8
- integrity, 27
- IT policy
 - commands, 24, 29
 - settings, 23
 - user security settings, 30

L

- listen port, 43
- log files, 23
- lookup, remote address
 - feature description, 21
 - workflow, 39

M

managing

- BlackBerry Wireless Solution, 8
- handheld deployment, 24
- handheld requests, 21
- handheld user information, 13
- push requests, 21

Microsoft Exchange Server, 32

Mobile Data Service

- access control, 14, 21, 43
- assigning roles, 21
- authenticating, 21
- converting data for viewing, 22
- description, 32
- managing handheld requests, 21
- managing push requests, 21
- optimizing data for viewing, 22
- proxy URL exclusion list, 14
- supporting proxy servers, 22
- wireless application transport, 14
- XML support, 14

monitoring

- BlackBerry Enterprise Server, 13
- using BlackBerry Controller, 13

multiple

- application support, 7
- device support, 7
- network support, 7
- server support, 13

P

Personal Information Management, see PIM data

phone settings, 23

phone, settings, 15

PIM data

- automatic wireless backup, 19
- BlackBerry Synchronization Service, 32
- categories, 16
- description, 19

synchronizing, 11, 40

processing flow

- access controlled data, 43
- address lookup, 39
- application data, 43
- BlackBerry Router, 46
- browser data, 42
- email to handheld, 35
- email with attachment, 37
- message from handheld, 36
- PIM data, 40
- wireless activation, 45

proxy server, 14, 22

push

- access control, 14
- application data, 43
- functional description, 8
- managing through Mobile Data Service, 21
- through BlackBerry Handheld Manager, 11

R

reconciling email, 18

redirecting email, 18

remote

- address lookup, 21, 39
- components, 33

S

security

- enhancements, 16
- feature description, 26
- handheld, 23
- timeout, 24
- user settings, 30

sending email

- from handheld, 36
- to handheld, 35

service book, 45

software requirements, 15–17

Feature and Technical Overview

synchronizing, PIM data
functional description, 11
workflow, 40

T

third-party applications, controlling, 13, 29
troubleshooting, BlackBerry Enterprise Server, 13

U

upgrading, handheld
using Application Loader, 12, 26
using Configuration Tool, 26
using Desktop Manager, 26

URL routing, 14

V

viewing
attachments, 11, 20
browser data, 42
converting data for, 22
optimizing data for, 22

W

web server, listen port, 43

wireless

activation, 12, 25, 45
application transport, 14
backup, 12, 19
deployment, 24
email settings, 12
IT commands, 24
IT policy settings, 23
redistribution, 25
XML-based data traffic, 14

workflow

looking up address, 39
passing data through the BlackBerry Router,
46
pushing application data to handheld, 43
sending browser data to handheld, 42
sending email from handheld, 36
sending email to handheld, 35
sending email with attachment, 37
synchronizing PIM data, 40
wireless enterprise activation, 45

X

XML support, 14, 22



© 2004 Research In Motion Limited
Published in Canada.