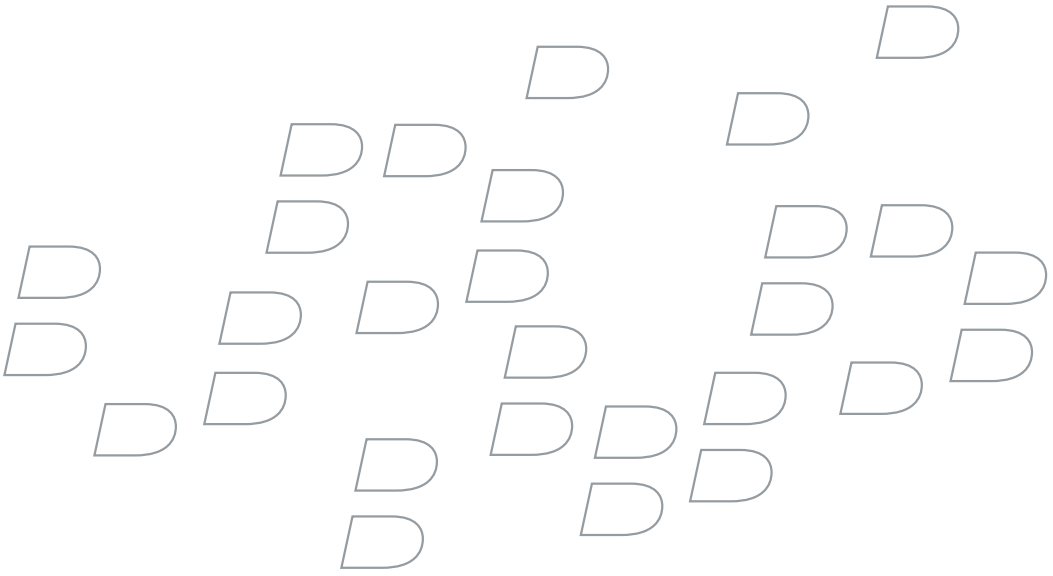


BlackBerry Enterprise Server for Microsoft Exchange

Version 4.1

Feature and Technical Overview

BlackBerry Enterprise Server Version 4.1 for Microsoft Exchange Feature and Technical Overview

Last modified: 20 February 2006

Part number: SWD_X_BES(EN)-150.003

At the time of publication, this documentation is based on BlackBerry Enterprise Server Version 4.1.0 for Microsoft Exchange.

Send us your comments on product documentation: https://www.blackberry.com/DocsFeedback.

©2006 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, "Always On, Always Connected", the "envelope in motion" symbol, BlackBerry, and BlackBerry Enterprise Server are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Adobe and Acrobat are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Corel and WordPerfect are either registered trademarks or trademarks of Corel Corporation and/or its subsidiaries in Canada, the United States and/or other countries. IBM, Lotus, and Sametime are either registered trademarks or trademarks of International Business Machines Corporation in the United States, other countries, or both. Microsoft, Windows, Excel, and PowerPoint are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Novell and GroupWise are either registered trademarks or trademarks of Novell, Inc., in the United States and other countries. SecurID is either a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries. Java is either a registered trademark or trademark of Sun Microsystems, Inc. in the U.S. or other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

The BlackBerry device 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; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents.shtml for a list of RIM [as hereinafter defined] patents.

This document is provided "as is" and Research In Motion Limited and its affiliated companies ("RIM") assume 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 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, hardware or software, products or services and/or third party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, 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 Information or the third party in any way. Installation and use of Third Party Information 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. Any dealings with Third Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses relating to Third Party Information. To the extent that such intellectual property licenses may be

required, RIM expressly recommends that you do not install or use Third Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third Party Information shall be governed by and subject to you agreeing to the terms of the Third Party Information licenses. Any Third Party Information that is provided with RIM's products and services is provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the Third Party Information and RIM assumes no liability whatsoever in relation to the Third Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.

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

1 BlackBerry Enterprise Server architecture 7
Architecture overview 7
Components 8
Remote components 9

2 BlackBerry Enterprise Server features 11
BlackBerry Messaging and Collaboration Services 11
Seamless message handling 11
Integrated instant messaging 12
Synchronized PIM data 13
Supported attachment viewing 14
BlackBerry MDS Services 14
Integrated wireless and enterprise application data 15
Optimized enterprise data for wireless use 15
Safe wireless and enterprise application connections 15
Centralized wireless application distribution 16
Simplified wireless application management 16
BlackBerry Administrative Tools and Services 17
Consolidated administrative interface 17
IT policy 18
BlackBerry device management 19
Wireless implementation of BlackBerry devices 19
Centralized implementation of BlackBerry devices 19
Centralized BlackBerry device maintenance 20
Flexible device software upgrade options 20
Control over wireless applications 20
BlackBerry security management 21
BlackBerry standard encryption 21
Safe and confidential message delivery 22
Protected storage of data and master encryption keys 22
Restricted BlackBerry device access to the BlackBerry Enterprise Server 24
Wireless management of BlackBerry device security 24

3 BlackBerry Enterprise Server workflows 25
Message workflows 25
Send a message to a BlackBerry device 25
Send a message from a BlackBerry device 26
Perform an address lookup 27
Instant messaging workflows 28
Start a Microsoft Windows Messenger instant messaging session on a BlackBerry device 28
Start a Sametime instant messaging session on a BlackBerry device 29
Start a Novell GroupWise Messenger instant messaging session on a BlackBerry device 31
Attachment workflows 32
View an attachment that is embedded in a message 32
View an attachment through a web link 33
PIM data workflows 34
Synchronize PIM data for the first time on the BlackBerry device 35
Synchronize a subsequent PIM data change 35
Mobile data workflows 36
Request BlackBerry Browser content on a BlackBerry device 37
Request content with access control enabled 37
Request content with two-factor authentication enabled 38
Push application content to a BlackBerry device 39
BlackBerry device management workflows 40
Resend an IT policy 40
Activate a BlackBerry device wirelessly 41
Reconcile a BlackBerry device without wireless data flow 42
Send an application to a BlackBerry device wirelessly 42

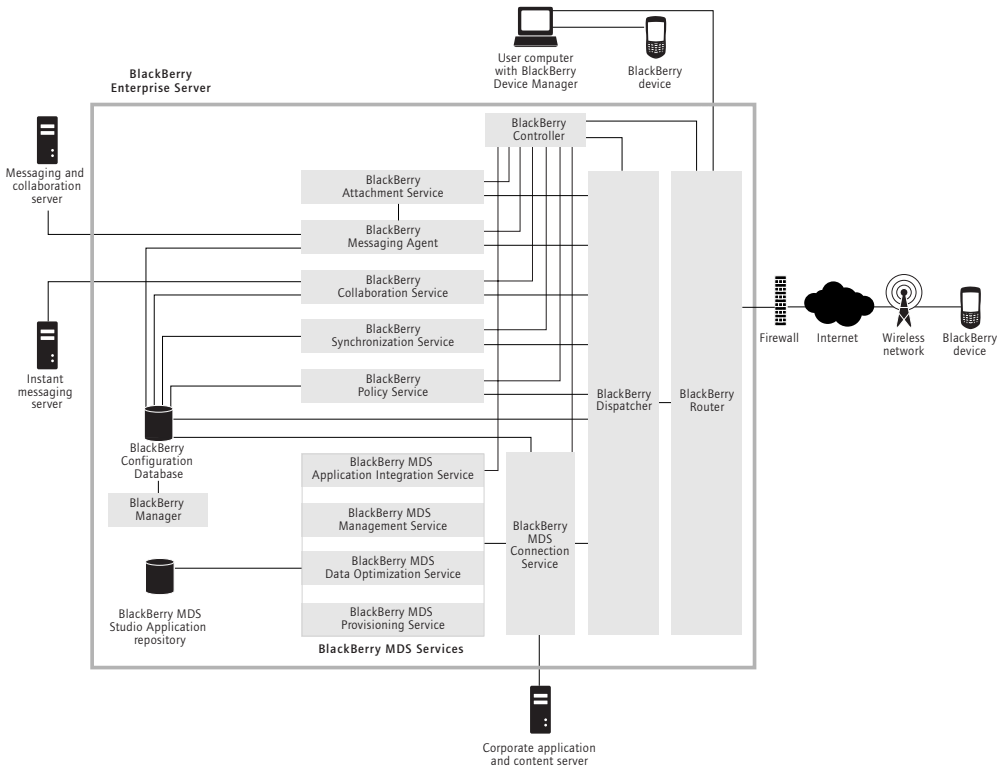
1

BlackBerry Enterprise Server architecture

Architecture overview
Components
Remote components

Architecture overview

The BlackBerry Enterprise Server® consists of services and components. The BlackBerry® services are designed to provide productivity tools—such as email, instant messaging, and personal information management (PIM) functionality—and data from enterprise applications to mobile users. The BlackBerry components are designed to monitor BlackBerry services, to process, route, compress, and encrypt data, and to communicate with the wireless network.



BlackBerry Enterprise Server architecture

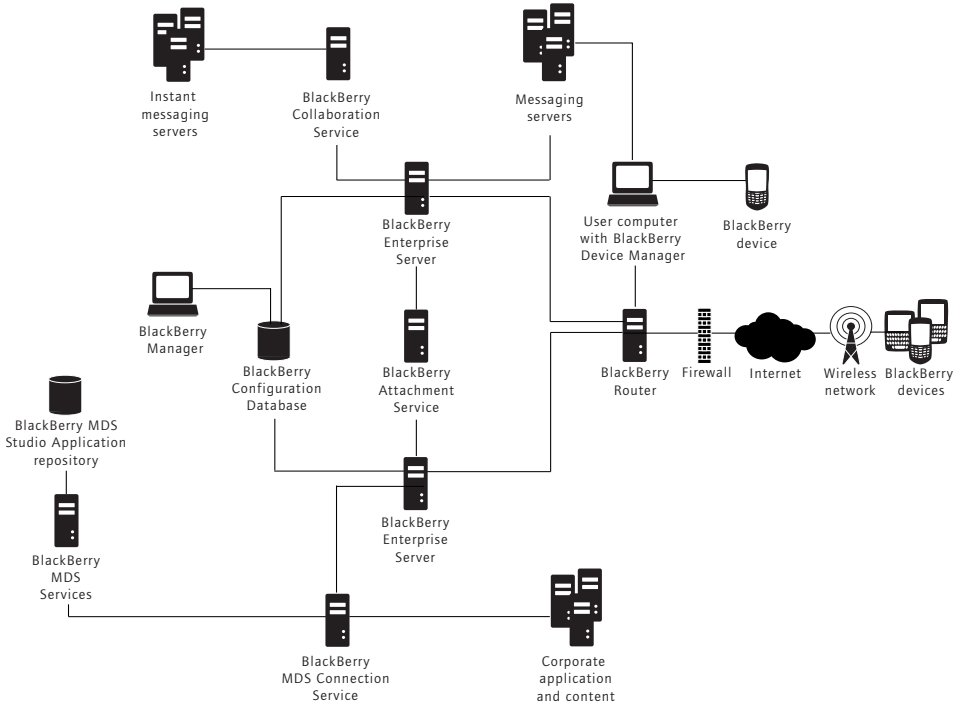
Components

Component	Description
BlackBerry Attachment Service	The attachment service is designed to convert supported attachments into a format that users can view on the BlackBerry device.
BlackBerry Collaboration Service	The collaboration service is designed to provide an encrypted connection between the instant messaging server and the enterprise messenger application on the BlackBerry device.
BlackBerry Configuration Database	The configuration database is a relational database that contains configuration information that is used by the BlackBerry components that do not connect to the messaging server directly. The configuration database includes the following information: • details about the connection from the BlackBerry Enterprise Server to the wireless network • user list • PIN-to-email address mapping for connection service push functionality • read-only copy of each user security key
BlackBerry Controller	The BlackBerry Controller is designed to monitor the BlackBerry components and to restart them if they stop responding.
BlackBerry Dispatcher	The BlackBerry Dispatcher is designed to compress and encrypt all BlackBerry data. It routes the data through the BlackBerry Router to and from the wireless network.
BlackBerry Manager	The BlackBerry Manager is designed to run on the administrator's computer and to connect to the configuration database for remote administration.
BlackBerry Mobile Data System™ (BlackBerry MDS™) Connection Service	The connection service is designed to provide users with access to online content and applications on the corporate intranet or the Internet.
BlackBerry MDS Services	The BlackBerry MDS Services are designed to provide connectivity between BlackBerry MDS Studio™ Applications on BlackBerry devices and enterprise applications.
BlackBerry MDS Studio Application repository	The repository is designed to manage and store BlackBerry MDS Studio Applications.
BlackBerry Messaging Agent	The messaging agent is designed to connect to the messaging and collaboration server to provide message, calendar, address lookup, attachment, and wireless encryption key generation services. The messaging agent also acts as a gateway for the synchronization service to access PIM data on the messaging server. It synchronizes configuration data between the configuration database and user mailboxes.
BlackBerry Policy Service	The policy service is designed to perform administration services wirelessly such as sending IT policies and IT commands, and provisioning service books.
BlackBerry Router	The BlackBerry Router is designed to connect to the wireless network to route data to and from the BlackBerry device. It is also designed to route data within your network to BlackBerry devices that are connected to the user's computer using the BlackBerry Device Manager.
BlackBerry Synchronization Service	The synchronization service is designed to synchronize PIM application data between the BlackBerry device and the messaging server wirelessly.
corporate application and content server	The corporate application and content server is designed to provide push applications and intranet content for the BlackBerry MDS Services.
instant messaging server	The instant messaging server stores instant messaging accounts.
messaging and collaboration server	The messaging server stores messaging accounts.

Component	Description
User computer with device manager	The user computer with the device manager is designed to enable users to connect their BlackBerry devices using a serial or USB connection and use the connection to route all data between the BlackBerry Enterpriser Server and BlackBerry devices. BlackBerry device traffic bypasses the wireless network while the BlackBerry device is connected to the computer. The device manager connects to the BlackBerry Router, which routes data directly to the BlackBerry device through this connection. Users can install the device manager separately or with the BlackBerry Desktop Manager as part of the full BlackBerry Desktop Software installation. The device manager is an optional component, but it is required to support a bypass connection to the BlackBerry Router.

Remote components

You can install all BlackBerry Enterprise Server components on one computer, or you can install particular components on separate computers. Consider any impacts on system resources when deciding where to install a component. You can choose to install only one remote component on each computer in your environment.



Sample BlackBerry Enterprise Server architecture with remote components

Component	Description
BlackBerry Attachment Service	A remote attachment service can support multiple BlackBerry Enterprise Servers. The attachment service can use increased system resources when processing concurrent conversion requests. You can install the attachment service on a remote computer to increase the number of concurrent conversions without impacting message delivery.
BlackBerry Collaboration Service	A remote collaboration service can support one BlackBerry Enterprise Server. The collaboration service uses a persistent socket connection for each instant messaging session. You can install the collaboration service on a remote computer to maximize the number of available sockets. You can install only one type of collaboration service (for example, IBM® Lotus® Sametime®), and users can use only one type of enterprise messenger application on the BlackBerry device.
BlackBerry Manager	A remote BlackBerry Manager enables you to manage multiple BlackBerry Domains from your computer.
BlackBerry MDS Studio Application repository	A remote repository can support one instance of the BlackBerry MDS Services. You must install the repository on the same database server as the configuration database.
BlackBerry MDS Connection Service	A remote connection service can support one BlackBerry Enterprise Server. The connection service can use increased system resources when processing content requests. You can install the connection service on a remote computer to minimize the impact on message delivery.
BlackBerry MDS Services	A remote instance of the BlackBerry MDS Services can support multiple BlackBerry Enterprise Servers and one repository. The BlackBerry MDS Services can use increased system resources when processing content requests. You can install an instance of the BlackBerry MDS Services on a remote computer to minimize the impact on message delivery.
BlackBerry Router	A remote BlackBerry Router can support multiple BlackBerry Enterprise Servers. The BlackBerry Router does not use many system resources, but it is a critical connection point for the BlackBerry Enterprise Solution™. You can install several standby BlackBerry Routers as failover locations in the event that your primary BlackBerry Router is unavailable.
configuration database	A remote configuration database can support multiple BlackBerry Enterprise Servers, creating a BlackBerry Domain.

2

BlackBerry Enterprise Server features

BlackBerry Messaging and Collaboration Services
BlackBerry MDS Services
BlackBerry Administrative Tools and Services
BlackBerry device management
BlackBerry security management

BlackBerry Messaging and Collaboration Services

The BlackBerry Enterprise Solution is designed to provide a wireless extension of the corporate messaging and collaboration environment.

Seamless message handling

The messaging agent is designed to integrate seamlessly with existing corporate email accounts. If users configure identical signatures on their BlackBerry devices and their computers, recipients cannot distinguish between messages that users send from the BlackBerry device and messages that users send from the desktop email program. The messaging agent delivers messages to BlackBerry devices automatically, so users can receive messages on the BlackBerry device with the same speed and reliability as that of the desktop email program.

Wireless message reconciliation

When users move or delete messages from the BlackBerry device or the desktop email program, or mark messages as read or unread, the messaging agent reconciles the changes wirelessly between the BlackBerry device and the desktop email program. Wireless message reconciliation is enabled by default on both the BlackBerry device and the BlackBerry Enterprise Server.

Wireless messaging options

On the BlackBerry device, users can use many of the same features that they can use in their desktop email program.

Feature	Description
message filters	Users can create, edit, and modify filters that define the action to perform if an incoming message matches the filter criteria. For example, users can forward messages from a particular sender to the BlackBerry device with high importance.
message storage	Users can define whether or not to copy messages that they send from the BlackBerry device to the Sent Items folder in the desktop email program.
message redirection	Users can turn off message redirection to the BlackBerry device if, for example, they are outside of a sufficient wireless coverage area.

Feature	Description
message reconciliation	Users can reconcile message removal between their desktop email program and their BlackBerry device. For example, if a user permanently deletes a message, archives a message, or moves a message to a personal folder in their desktop email program, the message no longer appears in the message list on their BlackBerry device.
auto signature	Users can modify the auto signature that appears in messages that they send from the BlackBerry device.
out-of-office notification	Users can create and activate an out-of-office reply message. If users remain out of the office for longer than expected, they can change the settings using their BlackBerry device.
calendar management	Users can create or edit meeting invitations, accept or decline invitations, and customize their calendar view settings.

Remote address lookup

Users can search for contacts in the corporate directory when they compose a message or meeting invitation on their BlackBerry device.

Feature	Description
contact search	Users can search using letters from a contact's first name, last name, or both. The BlackBerry Enterprise Server is designed to search the corporate directory and return up to the 20 closest matches.
address book updates	When users select a match from the lookup results, they can add the match to their BlackBerry device address book.
custom fields	You can map custom fields that users define in their personal address books to corresponding fields that appear in the BlackBerry device address book.
support for hosted BlackBerry Enterprise Server environments	Hosted BlackBerry Enterprise Server environments—where one company sells access to their BlackBerry Enterprise Server to other companies—can limit address lookup results using a custom field in the address book to set the company name. When users search for a contact, they receive the closest matches for other users in their company, and not from other companies on the BlackBerry Enterprise Server.

Integrated instant messaging

The collaboration service is designed to integrate seamlessly with existing third-party desktop instant messaging applications. The collaboration service uses public APIs and protocols defined by IBM, Microsoft®, and Novell®, and a Research In Motion® (RIM®)-proprietary protocol to deliver messages that are designed to be encrypted between the instant messaging server, the BlackBerry Enterprise Server, and the BlackBerry device.

Instant messaging options

On the BlackBerry device, users can set many of the same messaging options that they can set in their desktop instant messaging application.

Feature	Description
session management	You can limit the number of simultaneous instant messaging sessions that the collaboration service supports. You can set a timeout threshold after which the collaboration service ends inactive sessions automatically to permit new sessions to start. You can control whether your Sametime users appear to others as using a mobile instant messaging application, instead of a desktop instant messaging application, when logged in to the enterprise messenger on their BlackBerry device.

Feature	Description
group conversations	Users can start and manage a group conversation on their BlackBerry device.
availability status	Users can set their availability status, for example, away, or busy. Users can also set their availability status to change automatically when they are outside of a sufficient wireless coverage area.
embedded links	Users can click phone numbers in instant messages to make phone calls and click URLs in instant messages to view web pages.
synchronized contact lists	Users can synchronize their contact list wirelessly and request alerts when a contact becomes available.

Synchronized PIM data

The synchronization service is designed to synchronize PIM items such as tasks, memos, and contacts wirelessly so that the entries on the BlackBerry device and in the desktop email program are consistent. If you enable wireless PIM synchronization, PIM items synchronize over the wireless network automatically. With wireless PIM synchronization and wireless message reconciliation, users no longer have to connect the BlackBerry device to the desktop software to synchronize and reconcile messages and PIM data.

PIM settings

You can control PIM synchronization settings to manage the user experience and the use of system resources.

Feature	Description
initial synchronization	When you enable wireless PIM synchronization for users, an initial data synchronization occurs between the BlackBerry device and the BlackBerry Enterprise Server. This initial data synchronization fully synchronizes both the BlackBerry device and the desktop email program in a way that manages resolution of conflicting or duplicate entries to prevent data loss and is optimized for wireless transmission.
synchronization settings	You can configure wireless PIM synchronization settings that apply to all users in the BlackBerry Domain or to individual users. You can define which PIM items the synchronization service synchronizes, the conflict resolution settings, and whether changes made on the BlackBerry device and in the desktop email program synchronize in both directions, or whether only one source creates changes for the other source to receive. You can also control wireless PIM synchronization settings using IT policies.

Automatic wireless backup

Automatic wireless backup is designed to back up user settings and data from the BlackBerry device to the BlackBerry Enterprise Server automatically.

Automatic wireless backup is enabled on the BlackBerry Enterprise Server by default. You can back up the following device settings up using automatic wireless backup:

Application	Settings	
BlackBerry Browser	• bookmarks • channels	• folders • browser options
BlackBerry device options	• AutoText entries • content store • default service selector • BlackBerry device agent • firewall options	• font settings • help options • profiles • Home screen display options • WAP push options

Application	Settings	
Messaging	• attachment viewer options • filters • message list options	• searches • settings
Phone	• recently called list • phone call logs	• phone options
PIM	• address book options • calendar options • categories	• MemoPad options • task list options

Supported attachment viewing

The attachment service enables users to view supported message attachments on their BlackBerry devices in a format that retains most of the layout, appearance, and navigation of the original attachment. The attachment service uses an existing link to the messaging server to access attachments directly on the BlackBerry Enterprise Server.

The attachment service interprets and converts message attachments in binary format, so you do not have to install the applications that are associated with the attachment formats on the BlackBerry Enterprise Server.

The attachment viewer installs automatically with the device software. It supports the following formats:

File format	File extensions
Adobe® Acrobat® versions 1.1, 1.2, 1.3, 1.4	.pdf
Microsoft Excel® versions 97, 2000, 2003, XP	.xls
Microsoft PowerPoint® versions 97, 2000, 2003, XP	.ppt, .pps
Microsoft Word versions 97, 2000, 2003, XP	.doc, .dot
Corel® WordPerfect® versions 6.0, 7.0, 8.0, 9.0 (2000)	.wpd
ASCII text	.txt
HTML	.html, .htm
ZIP archives	.zip
images	.bmp, .jpg, .jpeg, .gif, .png, .tif, .tiff, .wmf

BlackBerry MDS Services

The BlackBerry MDS Services connect mobile users to enterprise applications. Enterprise applications typically use one of three types of interfaces: thin client/portal, thick client/server, or web service. The BlackBerry MDS Services are designed to support comparable BlackBerry applications.

Interface type	BlackBerry application
thin client/portal	BlackBerry MDS Browser Applications that developers create for the BlackBerry Browser.
thick client/server	BlackBerry MDS Java Applications that developers create using the BlackBerry Java Development Environment (JDE).
web service	BlackBerry MDS Studio Applications that developers create using the BlackBerry MDS Studio.

The BlackBerry MDS Services include the following BlackBerry services:

- BlackBerry MDS Application Integration Service
- BlackBerry MDS Data Optimization Service
- BlackBerry MDS Connection Service
- BlackBerry MDS Provisioning Service
- BlackBerry MDS Administrative and Management Service

Integrated wireless and enterprise application data

The application integration service is designed to support standard methods—for example, web services—of integrating wireless and enterprise applications.

Feature	Description
message monitoring	The BlackBerry MDS Studio Applications request content from corporate application and content servers using a series of messages. Content servers return the requested content using the same message format. You can monitor the messages sent between BlackBerry MDS Studio Applications and their content servers. If unusual activity occurs that might indicate a possible issue, you can monitor a single queue between a BlackBerry MDS Studio Application and its content server, or between a BlackBerry device and the BlackBerry MDS Studio Application.
PKI-compliant application certificates	The BlackBerry MDS Studio generates and signs applications with certificates that comply with the Public Key Infrastructure (PKI) X.509 standard. You add these certificates to the application integration service to encrypt connections to enterprise content.

Optimized enterprise data for wireless use

The data optimization service is designed to transform corporate server-side content and data for efficient wireless transmission and use on BlackBerry devices.

Feature	Description
data conversion	The data optimization service transcodes data to a format that the BlackBerry device can interpret and display.
data optimization	The data optimization service optimizes and compresses content for viewing in the BlackBerry Browser. For example, the data optimization service can change the data format or remove extraneous information to reduce network traffic and support a simplified application on the BlackBerry device. The data optimization service compresses XML application data for applications that use the BlackBerry device XML parser/generator.

Safe wireless and enterprise application connections

The connection service is designed to connect wireless applications to the Internet and to enterprise data and applications on the corporate intranet using standard Internet protocols.

Feature	Description
encrypted communications	The connection service encrypts content using the same encryption standard that the BlackBerry Dispatcher uses to encrypt messages and other BlackBerry data.

Feature	Description
protocol connections	You can define connections to content servers on the corporate intranet or the Internet using standard Internet protocols such as HTTP, HTTPS, and TCP/IP.
authentication methods	You can set authentication requirements that match your corporate sign-on scheme using standard methods such as NT Lan Manager (NTLM), Kerberos, and Lightweight Third-Party Authentication (LTPA). You can also define intervals at which the connection service requests users credentials and caches cookies. You can use two-factor authentication to create virtual private network (VPN) connections between wireless applications on the BlackBerry device and your corporate application servers.
integration with corporate proxy servers	You can provide access to internal content through corporate proxy servers using the following items: • proxy exclusion list, which defines internal URLs that the connection service routes directly to external web services instead of going through the corporate proxy server • Proxy Auto-Configuration (PAC) file
content push	The connection service accepts and responds to push requests from server-side push applications, if the application server is behind the corporate firewall. You can determine who receives pushed content—individual users or groups—and limit who can initiate content pushes.

Centralized wireless application distribution

The provisioning service is designed to control which BlackBerry MDS Studio Applications users can download to BlackBerry devices and to support application discovery from a BlackBerry device.

Feature	Description
BlackBerry MDS Studio Application control	Device policies control BlackBerry MDS Studio Applications. You can use device policies to define the user's ability to discover, install, and remove BlackBerry MDS Studio Applications on the BlackBerry device. You can also use device policies to control whether BlackBerry MDS Studio Applications can access other data and applications on the BlackBerry device, and to configure local BlackBerry device storage capacity for BlackBerry MDS Studio Application messages.
performance management	You can limit the inbound queue for BlackBerry MDS Studio Application requests and the outbound queue for BlackBerry MDS Studio Application delivery.

Simplified wireless application management

The administrative and management service is designed to centralize the BlackBerry MDS Studio Application lifecycle management, including centralized installation, upgrade, and removal of BlackBerry MDS Studio Applications.

Feature	Description
installation options	Users can choose which BlackBerry MDS Studio Applications to install or you can force the installation of specific BlackBerry MDS Studio Applications on their BlackBerry devices.
troubleshooting tools	The BlackBerry Manager displays a series of system alerts when unexpected behavior occurs, including possible content server connection failures. You can respond to possible issues by quarantining the BlackBerry MDS Studio Application on either a single user's BlackBerry device or in the BlackBerry MDS Studio Application repository.

BlackBerry Administrative Tools and Services

The BlackBerry Enterprise Server provides a set of tools and services that control, store, and route the data that the BlackBerry Messaging and Collaboration Services and the BlackBerry MDS Services create.

Tool	Description
BlackBerry Configuration Panel	Use the configuration panel to modify the BlackBerry Enterprise Server configuration after you install the BlackBerry Enterprise Server.
BlackBerry Controller	Use the BlackBerry Controller to monitor key BlackBerry services and BlackBerry components and, if necessary, restart them automatically.
wireless IT commands	Use wireless IT commands to respond when a BlackBerry device is misplaced, lost, or stolen.
log files	Use the log files to troubleshoot the BlackBerry Enterprise Server environment.

Consolidated administrative interface

The BlackBerry Manager provides a single interface for BlackBerry Enterprise Server, user, and BlackBerry device administration.

Administrator roles

The BlackBerry Manager uses predefined roles, which correspond to common corporate administrative roles, to limit access to sensitive data.

Feature	Description
data access	Roles are predefined in the configuration database, establishing a granular level of control over administrative tasks.
role management	Only the security administrator, who has the highest level of permission, can manage role membership.
task display	The BlackBerry Manager authenticates administrators and displays the tasks that they have permission to perform and the properties they have permission to edit. If administrators need view-only access to their role (for example, when training new administrators) the security administrator can assign an audit version of the role to them.
role types	Assign administrator roles based on your existing distribution of responsibility. • **Security administrator**: These administrators can perform all tasks. They are the only administrators who can manage role membership and change sensitive security properties, such as licenses and encryption keys. • **Enterprise administrator**: These administrators can perform all tasks that relate to users, services, BlackBerry Enterprise Servers, and global application data. These administrators cannot view role membership, licenses, or encryption keys. • **Device administrator**: These administrators can perform all tasks that relate to users and BlackBerry device management, including supporting new BlackBerry users and implementing BlackBerry devices. • **Senior help desk administrator**: These administrators can perform all user management tasks, including adding, moving, and deleting users, changing IT policy assignments, and issuing IT administration commands. • **Junior help desk administrator**: These administrators can perform user management tasks. These administrators cannot add, move, or delete users or issue certain IT administration commands.

User groups

The BlackBerry Manager is designed to use customized groups to manage multiple users as a single unit. To eliminate repetition of administrative tasks, group users by location, organizational unit, or BlackBerry device type.

Feature	Description
group properties	Create new groups from existing groups.
cross-server groupings	Manage groups that include users with BlackBerry devices that are enabled on different BlackBerry Enterprise Servers. All users in a group must be in the same BlackBerry Domain.
group administration	Group users together to apply common configuration settings or perform administrative tasks that affect all users in the group. For example, you can perform the following actions: • define PIM synchronization field mappings • purge pending messages • turn off message redirection • set access controls • assign an IT policy • resend peer-to-peer encryption keys • assign a software configuration • assign a device policy • install or remove BlackBerry MDS Studio Applications When you add a user to a group, the BlackBerry Manager assigns the properties and settings of the group to a user.

IT policy

Use the policy service to define IT policy settings and deliver them wirelessly to users' BlackBerry devices. An IT policy consists of rules that define BlackBerry device security, PIM synchronization settings, and other behaviors for the group of users that you define.

Feature	Description
wireless delivery	When you define IT policies, all settings are effective immediately because the policy service delivers them wirelessly. To provide wireless delivery of new IT policies and immediate user adoption, IT policy settings write to the user configurations automatically. To make sure that the settings are always current, the BlackBerry Enterprise Server periodically transmits BlackBerry device settings to BlackBerry devices wirelessly.
IT policy coverage	When you install the BlackBerry Enterprise Server and add users to it, the policy service adds the users to the default IT policy automatically. Until the BlackBerry device accepts the IT policy, users are not active on the BlackBerry Enterprise Server. You can assign a different IT policy to users. Users must always be assigned to one IT policy. If you delete all IT policies, the policy service assigns users to the default IT policy automatically.
IT policy assignment	You can assign an IT policy to a group of users or to individual users.

Feature	Description
resend options	If the BlackBerry Enterprise Server cannot immediately deliver an updated IT policy to the BlackBerry device—for example, if the user is outside a sufficient wireless coverage area—you can resend the IT policy manually or configure the interval after which the policy service resends the IT policy automatically. Automatic IT policy resends continue until the BlackBerry Enterprise Server delivers the IT policy successfully.
security enforcement	You can configure IT policies to override user-defined security settings on BlackBerry devices. You can configure IT polices that define security settings for the BlackBerry device and the desktop software. For example, you can specify whether a BlackBerry device password is required, the length of time that a password can exist before it is no longer valid, and the length and composition of a password. You can also specify encryption key details using IT policies.

BlackBerry device management

You can use the BlackBerry Enterprise Server to control how you implement, maintain, and upgrade BlackBerry devices across your organization.

Wireless implementation of BlackBerry devices

Users can activate a BlackBerry device on the BlackBerry Enterprise Server without a physical connection to the network. To initiate the wireless enterprise activation process, users contact an administrator for an activation password. The users open the enterprise activation application on their BlackBerry device and type their corporate email address and the activation password.

During wireless enterprise activation, message prepopulation sends up to 200 of the user's most recent messages, and initial PIM synchronization populates the BlackBerry device with the user's PIM data.

You can use wireless enterprise activation, with message prepopulation and automatic wireless backup, to provide users who are away from the office with a replacement BlackBerry device that contains the same user settings and data as their previous BlackBerry devices.

You can also use wireless enterprise activation to redistribute a BlackBerry device to a new user. You can send the Erase Data and Disable BlackBerry device command to a BlackBerry device that was associated with a different user account, and then implement it wirelessly for a new user.

Centralized implementation of BlackBerry devices

You can use the BlackBerry Manager to implement BlackBerry devices in a BlackBerry Domain from a single location. You can load device software and wireless applications onto BlackBerry devices. When users receive the configured BlackBerry devices, they are fully operational.

Centralized BlackBerry device maintenance

You can use the BlackBerry Manager to manage all BlackBerry devices in a BlackBerry Domain from a single location.

Feature	Description
software repository	Store and load device software and Java™-based applications from a central location. From this location, you can update the version of the software and deliver the software wirelessly to all BlackBerry devices in a BlackBerry Domain.
BlackBerry device configurations	Enforce a consistent BlackBerry device configuration for simplified management. Use the BlackBerry Manager to create standard software configurations and apply them simultaneously to multiple BlackBerry devices. Software configurations create more uniformity among BlackBerry devices. They also decrease your interaction with the BlackBerry Manager when you install software applications on BlackBerry devices. Use software configurations to compare the device software and wireless applications installed on a BlackBerry device with the device software and wireless applications defined in the user's software configuration. The BlackBerry Manager reports this information so that you can identify BlackBerry devices that are not running the most recent or desired version of device software or wireless applications.
BlackBerry device reporting	The BlackBerry Device Agent reports BlackBerry device information to the BlackBerry Manager wirelessly. This enables you to keep a current statistical inventory of the BlackBerry devices that are implemented in your organization.
wireless application delivery	Use software configurations to send Java applications to BlackBerry devices wirelessly.

Flexible device software upgrade options

You can choose the device software upgrade method that best suits your needs.

Feature	Description
local upgrade at administrator's computer	Collect BlackBerry devices that require software upgrades, connect them to an administration computer that is running the BlackBerry Manager, and load the upgrade software onto each BlackBerry device.
remote upgrade requiring user action	If users have the device manager installed on their desktop computer, you can direct them—for example, send a message with the link or post the link on a web site—to the network location from which they can load the software upgrade automatically or interact with the software upgrade process.
remote upgrade requiring no user action	If users have the desktop software, which includes the device manager and the application loader, installed on their desktop computer, you can force upgrades using an IT policy. When users connect their BlackBerry devices to the desktop software, they are informed that they must upgrade their device software. The upgrade process starts automatically.

Control over wireless applications

Feature	Description
control application delivery and removal	Permit users to download wireless applications to BlackBerry devices or prevent them from downloading wireless applications. You can also remove wireless applications from a BlackBerry device wirelessly.

Feature	Description
control the resources that applications can access	Create application control policies or device policies that define which resources (for example, message, phone, and BlackBerry device keystore) wireless applications can access on the BlackBerry device. Create IT policies that define the type of connections that a wireless application on the BlackBerry device can establish (for example, opening network connections inside the firewall).
control the availability of BlackBerry MDS Studio Applications	Create device policies to control whether or not users can search for BlackBerry MDS Studio Applications in the repository.

BlackBerry security management

The BlackBerry Enterprise Server is designed to protect data against attack while BlackBerry devices send and receive messages and access corporate data wirelessly. Only the BlackBerry Enterprise Server and the BlackBerry device have access to the data that they send between them.

The BlackBerry Enterprise Server is designed to prevent anyone except the intended recipient of a message from accessing potentially sensitive company information. The BlackBerry Enterprise Server protects the data by encrypting the data while it is in transit between the BlackBerry Enterprise Server and the BlackBerry device.

The BlackBerry Enterprise Server uses the Triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to encrypt data in transit.

Encryption type	Description
Triple DES	The BlackBerry Enterprise Server uses three iterations of the DES algorithm with two 56-bit keys, in outer cipher block chaining (CBC) mode, for an overall key length of 112 bits. Using two-key Triple DES (EDE), the first key encrypts the data, the second key decrypts it, and then the first key encrypts the data again. With Triple DES encryption, both the message keys and the master encryption keys contain 112 bits (16 bytes) of key data and 16 bits of parity data, which are stored as a 128-bit long binary string. Each parity bit is stored in the least significant bit of each of the 8 bytes of key data.
AES	AES is designed to provide a better combination of security and performance than DES or Triple DES. AES is designed to provide greater security against brute-force attacks by offering a larger key size. The BlackBerry Enterprise Server uses 256-bit keys in CBC mode to encrypt data that is sent between the BlackBerry Enterprise Server and the BlackBerry device. With AES encryption, both message keys and master encryption keys contain 256 bits of key data.

BlackBerry standard encryption

The BlackBerry Enterprise Server uses a symmetric key algorithm to encrypt and decrypt data. The symmetric key algorithm is designed to provide strong security and complete confidentiality of sensitive user information.

Before sending a message, the BlackBerry device compresses the message and then encrypts the message using the master encryption key, which is unique to that BlackBerry device. The BlackBerry device does not use the master encryption key in the compression process.

When the BlackBerry Enterprise Server receives the message from the BlackBerry device, the BlackBerry Dispatcher decrypts the message using the BlackBerry device master encryption key, and then decompresses the message.

Only the BlackBerry Enterprise Server and the BlackBerry device know the value of the master encryption key. The BlackBerry device permits the master encryption key exchange only when it is connected to the user's desktop computer. During wireless enterprise activation of the BlackBerry device, an authenticated link permits the master encryption key exchange.

Safe and confidential message delivery

The BlackBerry Enterprise Server encompasses the following cryptographic concepts:

Concept	BlackBerry Enterprise Server implementation
confidentiality	uses encryption to make sure that only the intended recipient can view the contents of the message
authenticity	uses digital signatures to permit the message recipient to identify and trust the message sender
integrity	uses digital signatures to verify that a third-party did not alter the message data in transit

In addition to providing effective corporate security, the BlackBerry Enterprise Server enables you to

- encrypt data and encryption keys on the BlackBerry device
- encrypt data and encryption keys in the configuration database
- encrypt data traffic in transit between the messaging server and the desktop email program

If the BlackBerry device cannot recognize the message format that the BlackBerry Enterprise Server decryption process produces, the BlackBerry device knows that a third-party altered the message while it was in transit. The BlackBerry device is designed to automatically reject any messages that it receives that do not produce the required message format upon decryption. A message on the BlackBerry device indicates that encryption failure has occurred and that the user must generate a new master encryption key. If the BlackBerry Enterprise Server receives a message that is encrypted with the wrong encryption key, a red X appears beside the failed message in the message list on the BlackBerry device.

BlackBerry standard encryption is designed to encrypt messages that the BlackBerry device sends or that the BlackBerry Enterprise Server forwards to the BlackBerry device. BlackBerry standard encryption encrypts the message

- from the time the user sends an email or PIN message from the BlackBerry device until the BlackBerry Enterprise Server receives the message
- from the time the BlackBerry Enterprise Server receives a message until the user reads the message on the BlackBerry device.

The BlackBerry Enterprise Server does not encrypt messages that it sends from the BlackBerry device to the message recipient unless the user installs additional messaging technology on the BlackBerry device and you enable the BlackBerry device to use that messaging technology. You can turn on the Secure Multipurpose Internet Mail Extensions (S/MIME) Support Package or the PGP Support Package in the BlackBerry Manager.

Protected storage of data and master encryption keys

BlackBerry device content is always protected with the 256-bit AES encryption algorithm. Content protection is designed to

- use 256-bit AES to encrypt stored data and master encryption keys when the BlackBerry device is locked
- use an ECC public key to encrypt data that the BlackBerry device receives when it is locked

During a reset, the BlackBerry device turns off the wireless radio, turns off serial bypass, locks, and stores a plain text copy of the encrypted BlackBerry device master encryption key in RAM. The BlackBerry device never stores the decrypted key in flash memory. Thus, the BlackBerry device master encryption key is not available to encrypt data that the BlackBerry device receives when it is locked. When the user unlocks the BlackBerry device, that action re-establishes the wireless connection and serial bypass resumes. The BlackBerry device then decrypts the master encryption key in RAM and the BlackBerry device resumes encryption of the master encryption keys.

When you (or the user) enable content protection on the BlackBerry device, an unlocked padlock icon appears at the top of the locked BlackBerry device screen.

The BlackBerry device uses content protection to encrypt the following user data items:

BlackBerry device application	User data
messaging	• email addresses • message body • attachments
calendar	• topic • location • organizer • attendees • notes included in the appointment or meeting request
MemoPad	• title • information in the note body
tasks	• topic • information in the task body
contacts	• all information except the title and category
AutoText	• all built-in or user-defined text that automatically replaces text that users type
BlackBerry Browser	• content that is pushed to the BlackBerry device • web sites that are saved on the BlackBerry device • browser cache

When a locked padlock appears at the top of the locked screen, the BlackBerry device is finished encrypting the content.

You can also use content protection to encrypt the master encryption keys stored on the BlackBerry device in flash memory. When you enable content protection of master encryption keys, the same content protection encryption and decryption process that the BlackBerry device uses to encrypt user data on the locked BlackBerry device protects the master encryption keys. If you define the cryptographic strength of the ECC key that encrypts data when the BlackBerry device is locked, the BlackBerry device uses the same key strength when encrypting the master encryption keys.

Restricted BlackBerry device access to the BlackBerry Enterprise Server

Use the enterprise service policy to create whitelists that control which BlackBerry devices can activate, either wirelessly or serially, on a BlackBerry Enterprise Server. The whitelists apply hierarchically; the BlackBerry Enterprise Server can activate a power user's BlackBerry device even if the BlackBerry device PIN does not appear in the PIN whitelist.

Whitelist type	Description
Power users	Authorize users or groups to activate their BlackBerry device on a BlackBerry Enterprise Server, regardless of their BlackBerry device type.
PIN	Authorize PINs or a range of PINs that can activate on a BlackBerry Enterprise Server.
BlackBerry device type	Authorize BlackBerry devices to activate on a BlackBerry Enterprise Server based on the following parameters: • manufacturer • model

Wireless management of BlackBerry device security

You can send IT administration commands to the BlackBerry device wirelessly to manage BlackBerry device security.

Feature	Description
erase application data on a lost or stolen BlackBerry device	If a BlackBerry device is stolen or lost, send the Erase data and disable BlackBerry device command to erase all information and application data on the BlackBerry device and make it unavailable.
lock a misplaced BlackBerry device	If a BlackBerry device is misplaced but likely not stolen or lost, send the Set password and lock the BlackBerry device command to set a password and lock the BlackBerry device. You can also send this command if a user forgets the BlackBerry device password.
label a BlackBerry device with contact information	If a BlackBerry device is stolen or lost, send the Set owner information command to make owner information appear on the screen when the BlackBerry device is locked. The owner information might include contact information that the finder can use to return the BlackBerry device to the owner.

3

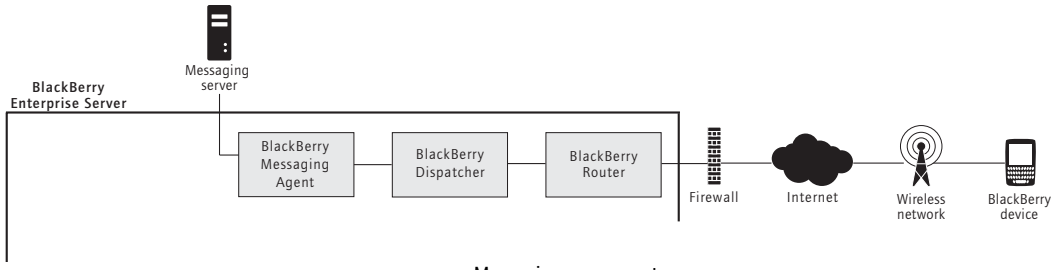
BlackBerry Enterprise Server workflows

Message workflows
Instant messaging workflows
Attachment workflows
PIM data workflows
Mobile data workflows
BlackBerry device management workflows

Message workflows

Workflow	Reference
Send a message to a BlackBerry device	See page 25.
Send a message from a BlackBerry device	See page 26.
Perform an address lookup	See page 27.

Send a message to a BlackBerry device



Messaging components

This workflow applies to new messages, reconciled messages (messages that are moved, deleted, or marked read or unread), and wireless calendar entries.

Step	Action	Description
1	A new message arrives on the messaging server.	A message arrives in the user's Microsoft Exchange mailbox. Microsoft Exchange notifies the messaging agent that a new message has arrived for the user.
2	The messaging agent applies filters.	The messaging agent checks the message fields against global filter rules and filters the messages that meet the filter criteria. If no global filter rules apply, then the messaging agent applies any user-defined filters to messages that meet the filter criteria. When the messaging agent finds a filter rule that applies to a message, it applies the rule and then stops searching filters.

Step	Action	Description
3	The messaging agent sends the first portion of the message to the BlackBerry Dispatcher.	The messaging agent sends the first 2-KB portion of the message to the BlackBerry Dispatcher.
4	The BlackBerry Dispatcher compresses and encrypts the first portion of the message.	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 BlackBerry device. .
5	The BlackBerry Router sends the first portion of the message 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 BlackBerry device that is registered on the wireless network.
6	The BlackBerry device returns delivery confirmation.	The wireless network locates the BlackBerry device and delivers the message. The BlackBerry device sends delivery confirmation to the BlackBerry Dispatcher, which passes it to the messaging agent. If the BlackBerry Enterprise Server does not receive confirmation within 4 hours, it resubmits the message to the wireless network. **Note**: The confirmation is a radio-level confirmation. It confirms that the wireless network delivered the message to the BlackBerry device, but it does not confirm that the user received or read the message.
7	The BlackBerry device processes the message.	The BlackBerry device decrypts and decompresses the message so that the user can view it. The BlackBerry device notifies the user of the arrival of the message.

Send a message from a BlackBerry device

This workflow applies to new messages, reconciled messages (messages that are moved, deleted, or marked read or unread), and wireless calendar entries.

Step	Action	Description
1	The user sends a message.	The user sends a message from the BlackBerry device. The BlackBerry device assigns the message a RefId. If the message is a meeting invitation or calendar item, the BlackBerry device appends the calendar information to the message.
2	The BlackBerry device processes the message.	The BlackBerry device compresses and encrypts the entire message.
3	The BlackBerry device sends the message to the BlackBerry Enterprise Server.	The BlackBerry device sends the message over port 3101 to the wireless network, which sends the message to the BlackBerry Enterprise Server. The BlackBerry Enterprise Server accepts only encrypted messages from the BlackBerry device. If the message is not encrypted, the BlackBerry Enterprise Server rejects it.
4	The BlackBerry Dispatcher decrypts and decompresses the message.	The BlackBerry Dispatcher uses the user encryption key to decrypt and decompress the message. If the BlackBerry Dispatcher cannot decrypt the message using the unique encryption key, the BlackBerry Enterprise Server ignores the message and sends an error to the BlackBerry device.
5	The messaging agent delivers the message to the user's mailbox.	The messaging agent places the message in the user's mailbox.
6	The messaging agent copies the message to the Sent Items folder.	The messaging agent places a copy of the message in the Sent Items view in the desktop email program. This step does not occur if the user has enabled the Don't save a copy to the Sent Items folder option and that setting is permitted on the BlackBerry Enterprise Server.

Step	Action	Description
7	The messaging server routes the message to the recipients.	The messaging server routes the message to the recipients. As a result, messages that users send from their BlackBerry devices are generally the same as messages that they send from their computer; messages originate from the user's corporate email address, and, if necessary, the messaging agent places a copy in the Sent Items folder.

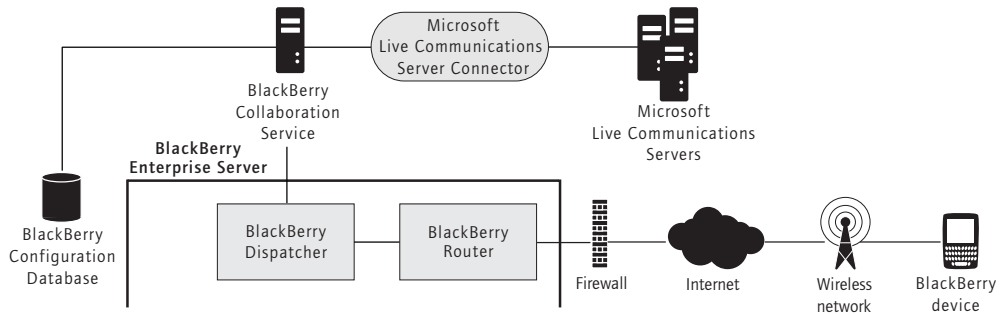
Perform an address lookup

Step	Action	Description
1	The user performs an address lookup on the BlackBerry device.	The user performs an address lookup on the BlackBerry device. The BlackBerry device assigns a RefId to the request.
2	The BlackBerry device processes the request.	The BlackBerry device compresses and encrypts the request using Triple DES or AES.
3	The BlackBerry device sends the request to the BlackBerry Enterprise Server.	The BlackBerry device sends the request over port 3101 to the BlackBerry Enterprise Server.
4	The BlackBerry Dispatcher decrypts and decompresses the request.	The BlackBerry Dispatcher uses the user encryption key to decrypt and decompress the request, and then passes the request to the messaging agent.
5	The messaging agent retrieves matches from the Global Address List.	The messaging agent queries the Global Address List on the Microsoft Exchange server and retrieves the 20 closest matches to the lookup request.
6	The messaging agent sends the results to the BlackBerry Dispatcher.	The messaging agent sends the lookup results to the BlackBerry Dispatcher.
7	The BlackBerry Dispatcher compresses and encrypts the results.	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 BlackBerry device.
8	The BlackBerry Router sends the results 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 BlackBerry device that is registered on the wireless network.
9	The BlackBerry device returns a delivery confirmation.	The wireless network locates the BlackBerry device and delivers the results. The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher, which passes it to the messaging agent. If the BlackBerry Enterprise Server does not receive delivery confirmation within 4 hours, it resubmits the lookup results to the wireless network.
10	The BlackBerry device processes the results.	The BlackBerry device uses the user encryption key to decrypt and decompress the lookup results so that the user can view them.
11	The user views the results.	The user can view the lookup matches on the BlackBerry device or add them to the BlackBerry device address book.

Instant messaging workflows

Workflow	Reference
Start a Microsoft Windows Messenger instant messaging session on a BlackBerry device	See page 28.
Start a Sametime instant messaging session on a BlackBerry device	See page 29.
Start a Novell GroupWise Messenger instant messaging session on a BlackBerry device	See page 30.

Start a Microsoft Windows Messenger instant messaging session on a BlackBerry device

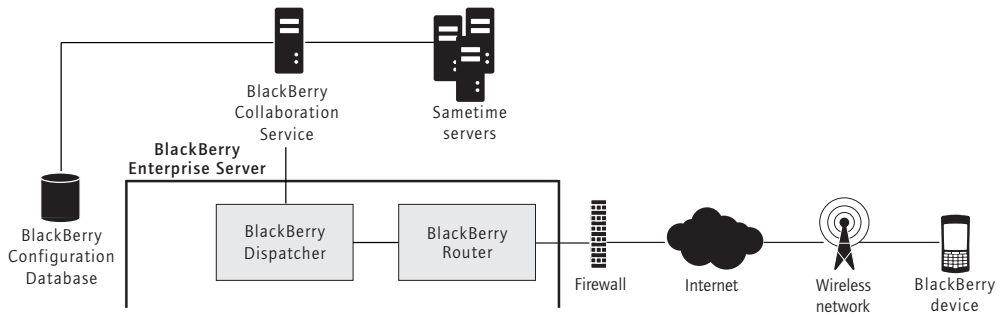


Microsoft Live Communications Server instant messaging components

Step	Action	Description
1	The user logs in to the enterprise messenger on the BlackBerry device.	The BlackBerry device compresses and encrypts the user ID and password and sends them through the BlackBerry Router over port 3101 to the BlackBerry Dispatcher.
2	The BlackBerry Dispatcher sends the request to the collaboration service.	The BlackBerry Dispatcher forwards the request to the collaboration service over port 3200. If the collaboration service is located on a remote computer, the request remains encrypted using a RIM-proprietary protocol.
3	The collaboration service checks for available sessions.	The collaboration service reads the configuration database to check if the maximum number of sessions has been reached and then performs one of the following actions: • logs out idle sessions, if the maximum is reached and a timeout limit is set • sends a "Server Busy (103)" status message to the Blackberry device and rejects the login request, if there are no idle sessions • sends a "Failed (300)" status message to the Blackberry device and rejects the login request, if the maximum number of sessions is not set and the number of sessions equals the total number that the Microsoft Real-time Communications (RTC) API supports
4	The collaboration service checks the user's access.	The collaboration service reads the configuration database to check if the user has permission to use the enterprise messenger application.

Step	Action	Description
5	The collaboration service queues the request for the Microsoft Live Communications Server connector.	The collaboration service places the request in the local queue for the Microsoft Live Communications Server connector. The Microsoft Messaging Queueing (MSMQ) software version 3.0 running on the collaboration service computer sends the request in Extensible Messaging and Presence Protocol (XMPP) format over an encrypted Transport Layer Security (TLS) connection to the Microsoft Live Communications Server connector. By default, the collaboration service starts this connection over port 5061, but you can specify a custom port.
6	The Microsoft Live Communications Server connector creates a connection.	The Microsoft Live Communications Server connector creates an RTC client object for the session, which maintains an open TLS connection between the enterprise messenger application and the Microsoft Live Communications Server for the duration of the session. TLS is the default transport protocol. You can set Transmission Control Protocol (TCP) as the transport protocol, but TCP requires more dedicated connections for each session than TLS, so fewer sessions are supported.
7	The Microsoft Live Communications Server connector returns the acceptance to the collaboration service.	The Microsoft Live Communications Server connector returns the acceptance, with the RTC client object, to the local queue on the collaboration service.
8	The collaboration server returns the acceptance to the BlackBerry device.	The collaboration service returns the acceptance, in encrypted and compressed format through the BlackBerry Dispatcher to the BlackBerry device and creates a cache of the connectivity information to sustain the session for that user.
9	The user's session is active.	The Microsoft Windows® Messenger client on the BlackBerry device starts the session using the RTC connection object. The user can now start a conversation, set availability status, or synchronize the contact list.

Start a Sametime instant messaging session on a BlackBerry device

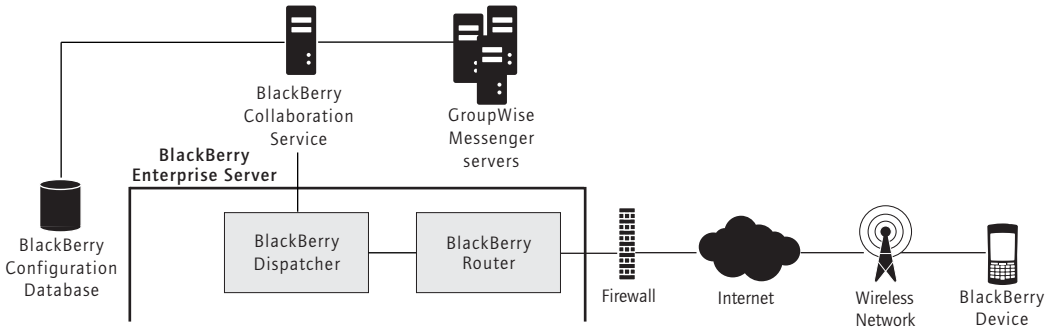


Sametime instant messaging components

Step	Action	Description
1	The user logs in to the enterprise messenger on the BlackBerry device.	The BlackBerry device compresses and encrypts the user ID and password and sends them through the BlackBerry Router over port 3101 to the BlackBerry Dispatcher.

Step	Action	Description
2	The BlackBerry Dispatcher sends the request to the collaboration service.	The BlackBerry Dispatcher forwards the request to the collaboration service over port 3200. If the collaboration service is located on a remote computer, the request remains compressed and encrypted using a RIM-proprietary protocol.
3	The collaboration service checks for available sessions.	The collaboration service reads the configuration database to check if the maximum number of sessions has been reached and then performs one of the following actions: • logs out idle sessions, if the maximum is reached and a timeout limit is set • sends a "Server Busy (103)" status message to the Blackberry device and rejects the login request, if there are no idle sessions • sends a "Failed (300)" status message to the Blackberry device and rejects the login request, if the maximum number of sessions is not set, and the number of sessions equals the total number that the Sametime API supports.
4	The collaboration service checks the user's access.	The collaboration service reads the configuration database to check if the user has permission to use the enterprise messenger application.
5	The collaboration service connects to the Sametime server.	The collaboration service starts an encrypted proxy connection over TCP/IP using the Sametime APIs, reformats the request from the RIM-proprietary protocol format into one that the Sametime API supports, and sends the request. By default, the collaboration service starts this connection over port 1533, but you can specify a custom port.
6	The Sametime server accepts the connection.	The Sametime server accepts the login request from the BlackBerry device. The Sametime server starts a dedicated TCP/IP connection for the session and starts listening for requests from the BlackBerry device for that session.
7	The collaboration server returns the acceptance to the BlackBerry device.	The collaboration service returns the acceptance, in encrypted and compressed format through the BlackBerry Dispatcher to the BlackBerry device and creates a cache of the connectivity information to sustain the session for that user.
8	The user's session is active.	The user can now start a conversation, set availability status, or synchronize the contact list.

Start a Novell GroupWise Messenger instant messaging session on a BlackBerry device



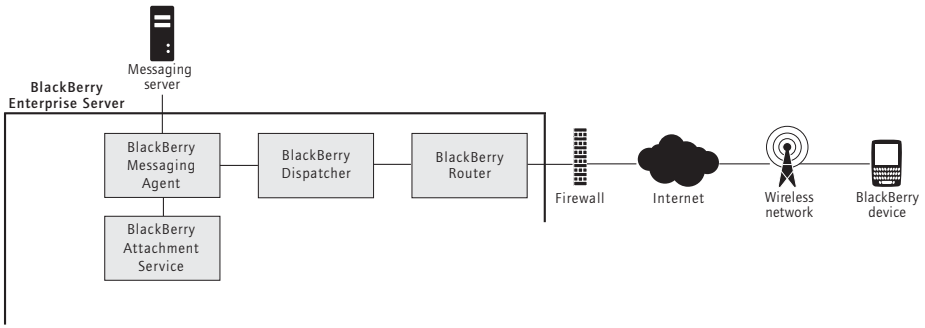
GroupWise Messenger instant messaging components

Step	Action	Description
1	The user logs in to the enterprise messenger on the BlackBerry device.	The BlackBerry device compresses and encrypts the user ID and password and sends them through the BlackBerry Router over port 3101 to the BlackBerry Dispatcher.
2	The BlackBerry Dispatcher sends the request to the collaboration service.	The BlackBerry Dispatcher forwards the request to the collaboration service over port 3200. If the collaboration service is located on a remote computer, the request remains compressed and encrypted using a RIM-proprietary protocol.
3	The collaboration service checks for available sessions.	The collaboration service reads the configuration database to check if the maximum number of sessions has been reached and then performs one of the following actions: • logs out idle sessions, if the maximum is reached and a timeout limit is set • sends a "Server Busy (103)" status message to the Blackberry device and rejects the login request, if there are no idle sessions • sends a "Failed (300)" status message to the Blackberry device and rejects the login request, if the maximum number of sessions is not set, and the number of sessions equals the total number that the GroupWise® protocol supports
4	The collaboration service checks the user's access.	The collaboration service reads the configuration database to check if the user has permission to use the enterprise messenger application.
5	The collaboration service connects to the GroupWise Messenger server.	The collaboration service starts an encrypted proxy connection over Secure Sockets Layer (SSL) using the GroupWise protocol and sends the request. By default, the collaboration service starts this connection over port 8300, but you can specify a custom port.
6	The GroupWise Messenger server accepts the connection.	The GroupWise Messenger server accepts the login request from the BlackBerry device. The GroupWise Messenger server starts a dedicated SSL connection for the session and starts listening for requests from the BlackBerry device for that session.
7	The collaboration service returns the acceptance to the BlackBerry device.	The collaboration service returns the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device and creates a cache of the connectivity information to sustain the session for that user.
8	The user's session is active.	The user can now start a conversation, set availability status, or synchronize the contact list.

Attachment workflows

Workflow	Reference
View an attachment that is embedded in a message	See page 32.
View an attachment through a web link	See page 33.

View an attachment that is embedded in a message

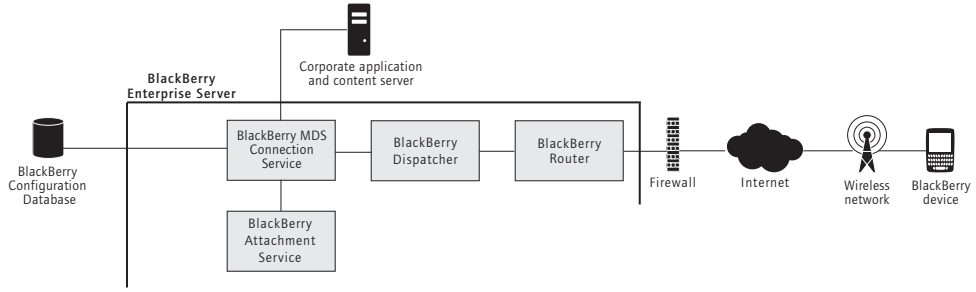


Attachment components

Step	Action	Description
1	The user receives a message with an attachment.	The user receives a message with an attachment on the BlackBerry device.
2	The messaging agent verifies the attachment.	The messaging agent verifies that the attachment is a valid format for conversion. If the format is not valid and the BlackBerry device is a Java-based BlackBerry device, the Open Attachment menu item does not appear on the user's BlackBerry device.
3	The user requests the attachment.	The user clicks the Open Attachment menu item to view the attachment on the BlackBerry device.
4	The attachment viewer sends the conversion request.	The BlackBerry device attachment viewer sends the request to the messaging agent, which invokes the attachment service over port 1900.
5	The attachment service retrieves the attachment.	The attachment service retrieves the attachment in binary format from the user's message store using the messaging agent link to the messaging server.
6	The attachment service distills the attachment.	The attachment service distills the attachment.
7	The attachment service extracts and stores the attachment information.	The attachment service extracts the content, layout and appearance, and navigation information from the attachment. The attachment service organizes, stores, and links the information in an efficient, proprietary Document Object Model (DOM) in a binary Extensible Markup Language (XML) style.
8	The attachment service formats the attachment for the BlackBerry device.	The attachment service formats the attachment for the BlackBerry device 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 BlackBerry device information (for example, screen size, display, or available space).

Step	Action	Description
9	The attachment service sends the converted attachment to the messaging agent.	The attachment service sends the UCS data to the messaging agent using a TCP/IP connection over port 1900.
10	The messaging agent sends the converted attachment to the BlackBerry Dispatcher.	The messaging agent sends the converted attachment to the BlackBerry Dispatcher.
11	The BlackBerry Dispatcher compresses and encrypts the converted attachment.	The BlackBerry Dispatcher compresses the first portion of the attachment, encrypts it with the user encryption key, and then passes the first portion of the attachment to the BlackBerry Router for delivery to the BlackBerry device.
12	The BlackBerry Router sends the converted attachment 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 BlackBerry device that is registered on the wireless network.
13	The BlackBerry device returns delivery confirmation.	The wireless network locates the BlackBerry device and delivers the attachment. The BlackBerry device sends delivery confirmation to the BlackBerry Dispatcher, which passes it to the messaging agent. If the BlackBerry Enterprise Server does not receive confirmation within 4 hours, it resubmits the attachment data to the wireless network.
14	The BlackBerry device decompresses and decrypts the converted attachment.	The BlackBerry device uses the user encryption key to decrypt and decompress the attachment so that the user can view it.
15	The user views the attachment on the BlackBerry device.	The user views the attachment on the BlackBerry device 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 BlackBerry device.

View an attachment through a web link



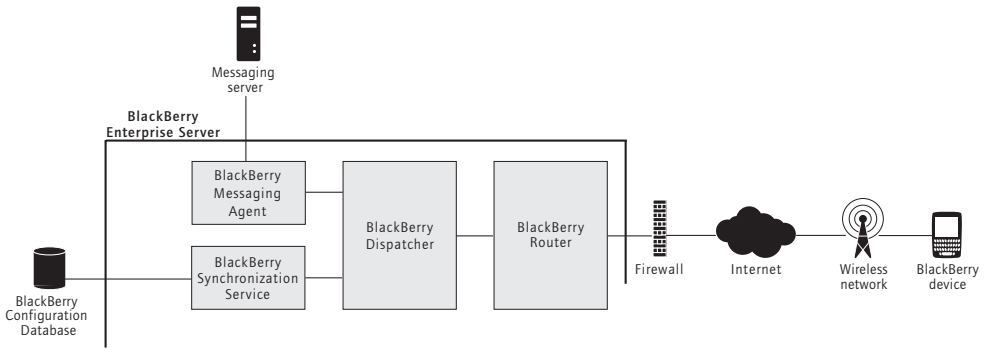
Attachment through a web link components

Step	Action	Description
1	The user requests the attachment.	The user clicks the Get Link menu item to view the document on the BlackBerry device.
2	The BlackBerry device sends the request.	The BlackBerry device sends the request over port 3101 to the BlackBerry Enterprise Server on which the user resides. The BlackBerry Dispatcher sends the request to the connection service over port 3200.
3	The connection service retrieves the attachment.	The connection service creates an HTTP session for the user and sends the request to the web server. The connection service retrieves the requested content.

Step	Action	Description
4	The connection service sends the conversion request.	The connection service sends the downloaded content to the attachment service for conversion.
5	The attachment service extracts and stores the attachment information.	The attachment service extracts the content, layout and appearance, and navigation information from the attachment. The attachment service organizes, stores, and links the information in an efficient, proprietary Document Object Model (DOM) in a binary Extensible Markup Language (XML) style.
6	The attachment service formats the attachment for the BlackBerry device.	The attachment service formats the attachment for the BlackBerry device and converts it to UCS format. The formatting is based on the request for content (for example, page and paragraph information or search words) and the available BlackBerry device information (for example, screen size, display, or available space).
7	The attachment service sends the converted attachment to the connection service.	The attachment service sends the converted attachment to the connection service using HTTP for the browser to display.
8	The connection service sends the converted attachment to the BlackBerry Dispatcher.	The connection service sends the first 250 KB of content to the BlackBerry Dispatcher over port 3200.
9	The BlackBerry Dispatcher compresses and encrypts the converted attachment.	The BlackBerry Dispatcher compresses the content, encrypts it with the user encryption key, and then sends the content to the BlackBerry Router for delivery to the BlackBerry device.
10	The BlackBerry device decompresses and decrypts the converted attachment.	The BlackBerry device uses the user encryption key to decrypt and decompress the attachment so that the user can view it.
11	The user views the attachment is on the BlackBerry device.	The user views the attachment on the BlackBerry device using the attachment viewer browser plug-in. The attachment viewer parses 3-KB at a time.

PIM data workflows

Workflow	Reference
Synchronize PIM data for the first time on the BlackBerry device	See page 35.
Synchronize a subsequent PIM data change	See page 35.



PIM synchronization components

Synchronize PIM data for the first time on the BlackBerry device

Step	Action	Description
1	The user's BlackBerry device receives the synchronization service book.	The user activates a new BlackBerry device or upgrades an existing BlackBerry device and receives the synchronization service book.
2	The BlackBerry device requests synchronization configuration information.	The BlackBerry device requests the synchronization configuration information from the synchronization service. The configuration information indicates if wireless PIM synchronization is enabled on the BlackBerry Enterprise Server and which database can be synchronized. The configuration information also provides database synchronization types and conflict resolution settings. All data that is sent between the BlackBerry device and the BlackBerry Enterprise Server is compressed and encrypted.
3	The synchronization service starts the initial synchronization.	The synchronization service returns the configuration information and synchronizes the databases using that information. A synchronization agent on the BlackBerry device tracks which databases you can synchronize wirelessly. If there is existing data on the BlackBerry device and the BlackBerry Enterprise Server, the synchronization service merges, adds, or updates the records during synchronization process. If there is data on only the BlackBerry device or the BlackBerry Enterprise Server, the synchronization service restores the data from that location. Neither the BlackBerry device nor the BlackBerry Enterprise Server delete records during the initial synchronization process. After the synchronization service registers a database for wireless synchronization, you can no longer synchronize or restore it using the desktop software.
4	The synchronization service completes the initial synchronization	The initial synchronization is complete when the data on the BlackBerry device and the BlackBerry Enterprise Server are synchronized. Future changes on the BlackBerry device or the BlackBerry Enterprise Server are synchronized wirelessly through the PIM synchronization process. If the user modifies data in the BlackBerry device or computer PIM application during the initial synchronization, the synchronization service synchronizes the records during the PIM synchronization process after the initial load is complete. If the user connects the BlackBerry device to a computer that has the device manager installed (either standalone or as part of the optional desktop manager) and running, the initial synchronization can occur over the connection to the BlackBerry Router instead of over the wireless network.

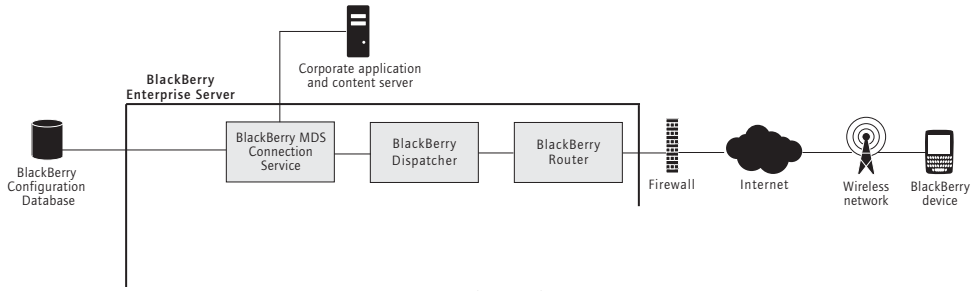
Synchronize a subsequent PIM data change

Step	Action	Description
1	The user saves changes to PIM data.	The user saves changes to PIM data or BlackBerry device settings (for example, a new AutoText entry) in the BlackBerry device or computer PIM application. The BlackBerry device or the BlackBerry Enterprise Server adds the change to the changelist (depending on where the change was made).

Step	Action	Description
2	The synchronization service receives the changelist.	The synchronization service receives the changelist, which includes the target PIM application database and record information. The synchronization service sends changes to PIM data immediately (along with other entries in the changelist for that user). The synchronization service sends other changes at the batch synchronization interval set on the BlackBerry Enterprise Server; the default is every 10 minutes. To prevent change collisions, only a single BlackBerry Enterprise Server or BlackBerry device changelist for each user can be sent wirelessly at one time.
3	The synchronization service writes the request to the configuration database.	The synchronization service receives the synchronization request and writes a synchronization request entry in the SynchRequest table of the configuration database.
4	The synchronization service sends the synchronization data to the BlackBerry Dispatcher.	The synchronization service sends the changed records to the BlackBerry Dispatcher.
5	The BlackBerry Dispatcher compresses and encrypts the synchronization data.	The BlackBerry Dispatcher compresses the content, encrypts it with the user encryption key, and then sends the content to the BlackBerry Router for delivery to the BlackBerry device.
6	The BlackBerry device returns a delivery confirmation.	The BlackBerry device sends a delivery confirmation for each record that it receives. Each time the synchronization service receives a delivery confirmation, it 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 BlackBerry device.

Mobile data workflows

Workflow	Reference
Request BlackBerry Browser content on a BlackBerry device	See page 37.
Request content with access control enabled	See page 37.
Request content with two-factor authentication enabled	See page 38.
Push application content to a BlackBerry device	See page 39.



Connection service components

Request BlackBerry Browser content on a BlackBerry device

Step	Action	Description
1	The user requests content.	The user requests Internet or intranet content on the BlackBerry device.
2	The BlackBerry device sends the request.	The BlackBerry device sends the request over port 3101 to the BlackBerry Enterprise Server on which the user resides. The BlackBerry Dispatcher sends the request to the connection service over port 3200.
3	The connection service retrieves the content.	The connection service creates an HTTP session for the user and retrieves the requested content.
4	The connection service converts the content and sends it to the BlackBerry Dispatcher.	The connection service converts the content for viewing on the BlackBerry device and sends the content to the BlackBerry Dispatcher over port 3200.
5	The BlackBerry Dispatcher compresses and encrypts the content.	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 BlackBerry device.
6	The BlackBerry Router sends the content 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 BlackBerry device that is registered on the wireless network.
7	The BlackBerry device returns a delivery confirmation.	The wireless network locates the BlackBerry device and delivers the content. The BlackBerry device sends a delivery confirmation to the BlackBerry Router. If the connection service does not receive confirmation within the flow control timeout limit, it sends a cancellation to the wireless network for the pending content.
8	The BlackBerry device decompresses and decrypts the content.	The BlackBerry device decrypts and decompresses the content so that the user can view it. The BlackBerry device application detects the content and displays it on the BlackBerry device.

Request content with access control enabled

Step	Action	Description
1	The user requests content.	The user requests content from the content server.
2	The BlackBerry device sends the request.	The BlackBerry device sends the request over port 3101 to the BlackBerry Enterprise Server on which the user resides. The BlackBerry Dispatcher sends the request to the connection service over port 3200.
3	The connection service checks the user's access permissions.	The connection service reads the configuration database to check if pull access control is enabled and if the user has permission to pull content from the specified source. If pull access control is not enabled or of the user does not have permission to pull content, the connection service denies the request and sends a message to the BlackBerry device.
4	The connection service authenticates the user on the content server.	The connection service creates an HTTP session for the user and sends authentication credentials to the content server. When the content server responds to the authentication request, one of the following actions occur: • If the authentication is successful, the connection service sends the HTTP request. • If the authentication is not successful, the connection service does not send the HTTP request. An "HTTP 403 Error" message appears in the BlackBerry Browser and the user is prompted to type correct credentials. The connection service sends another authentication request to the content server with the user credentials and, if successful, sends the HTTP request.

Step	Action	Description
5	The connection service retrieves the content, converts the content, and then sends it to the BlackBerry Dispatcher.	The connection service retrieves the requested content, converts the content for viewing on the BlackBerry device, and then sends it to the BlackBerry Dispatcher over port 3200.
6	The BlackBerry Dispatcher compresses and encrypts the content.	The BlackBerry Dispatcher compresses the content, encrypts it with the user's encryption key, and then sends the content to the BlackBerry Router for delivery to the BlackBerry device.
7	The BlackBerry Router sends the content 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 BlackBerry device that is registered on the wireless network.
8	The BlackBerry device returns a delivery confirmation.	The wireless network locates the BlackBerry device and delivers the content. The BlackBerry device sends a delivery confirmation to the BlackBerry Router. If the connection service does not receive a delivery confirmation within the flow control timeout limit, it sends a cancellation to the wireless network for the pending content.
9	The BlackBerry device decompresses and decrypts the content.	The BlackBerry device decrypts and decompresses the content so that the user can view it. The BlackBerry device application detects the content and displays it on the BlackBerry device.

Request content with two-factor authentication enabled

Step	Action	Description
1	The user requests content.	The user requests Internet content from the content server.
2	The BlackBerry device sends the request.	The BlackBerry device sends the request over port 3101 to the BlackBerry Enterprise Server on which the user resides. The BlackBerry Dispatcher sends the request to the connection service over port 3200.
3	The connection service checks the user's access permissions.	The connection service checks the content request to see if an authenticated session is in progress on the user's BlackBerry device. If a session is not in progress, the connection service redirects the user to a login page.
4	The user types the credentials.	The user types a RSA SecurID® user name and passcode.
5	The connection service creates a safe connection to the content server.	The BlackBerry device caches the credentials for the duration of the session, which is 60 minutes of inactivity or 24 hours of activity, by default.
6	The connection service retrieves the content, converts the content, and then sends it to the BlackBerry Dispatcher.	The connection service retrieves the requested content, converts the content for viewing on the BlackBerry device, and then sends it to the BlackBerry Dispatcher over port 3200.
7	The BlackBerry Dispatcher compresses and encrypts the content.	The BlackBerry Dispatcher compresses the content, encrypts it with the user's encryption key, and then sends the content to the BlackBerry Router for delivery to the BlackBerry device.
8	The BlackBerry Router sends the content 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 BlackBerry device that is registered on the wireless network.
9	The BlackBerry device returns delivery confirmation.	The wireless network locates the BlackBerry device and delivers the content. The BlackBerry device sends delivery confirmation to the BlackBerry Router. If the connection service does not receive confirmation within the flow control timeout limit, it sends a cancellation to the wireless network for the pending content.

Step	Action	Description
10	The BlackBerry device decompresses and decrypts the content.	The BlackBerry device decrypts and decompresses the content so that the user can view it. The BlackBerry device application detects the content and displays it.

Push application content to a BlackBerry device

Step	Action	Description
1	A custom application sends a push request.	A custom push application, which resides on an application server behind the corporate firewall, sends an HTTP POST request to the connection service central push server over the web server listen port (default 8080). The application specifies the BlackBerry Enterprise Server host name and the connection service web server connection listen port.
2	The connection service push server checks recipient information.	The central connection service push server checks the configuration database for the following information about the recipients who are defined in the push application: • BlackBerry Enterprise Server on which the user account resides • PIN that is associated with the user's email address • whether the user's account is pending deletion Users who do not appear in the BlackBerry directory, or whose account is pending deletion, do not receive push content.
3	The connection service responds to the application request.	The connection service responds to the push application to acknowledge that it is processing the request and then closes the connection.
4	The connection service push server sends the push content.	The central connection service push server routes the content to the push server connection listen port (default 8080).
5	The connection service converts the content and sends it to the BlackBerry Dispatcher.	The connection service converts the content for viewing on the BlackBerry device and sends the content to the BlackBerry Dispatcher over port 3200.
6	The BlackBerry Dispatcher compresses and encrypts the content.	The BlackBerry Dispatcher encrypts the content with the user encryption key, compresses it, and then sends the content to the BlackBerry Router for delivery to the BlackBerry device.
7	The BlackBerry Router sends the content 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 BlackBerry device that is registered on the wireless network.
8	The BlackBerry device returns a delivery confirmation.	The wireless network locates the BlackBerry device and delivers the content. The BlackBerry device sends a delivery confirmation to the BlackBerry Enterprise Server. If the connection service does not receive a delivery confirmation within the flow control timeout limit, it sends a cancellation to the wireless network for the pending content.
9	The BlackBerry device decompresses and decrypts the content.	The BlackBerry device application that listens on the port number that the developer specifies in the push application (for example, the BlackBerry Browser listens for push application connections on port 7874) detects the incoming content, and then displays it on the BlackBerry device when the user invokes it.

BlackBerry device management workflows

Workflow	Reference
Resend an IT policy	See page 40.
Activate a BlackBerry device wirelessly	See page 41.
Reconcile a BlackBerry device without wireless data flow	See page 42.
Send an application to a BlackBerry device wirelessly	See page 42.

Resend an IT policy

Step	Action	Description
1	The administrator resends an IT policy.	The administrator clicks a user, and clicks the Resend IT Policy task in the BlackBerry Manager.
2	The policy service checks the user's current IT policy settings.	The policy service reads the user's current IT policy settings from the configuration database to determine which IT policy to send.
3	The policy service prepares the IT policy for delivery	The policy service prepares the IT policy settings for delivery using the general message envelope (GME) protocol. The policy service adds the unique identifier and version of the BlackBerry Enterprise Server to the IT policy packet and adds the unique key that the BlackBerry Domain uses to sign all IT policy packets.
4	The policy service sends the IT policy to the BlackBerry Dispatcher.	The policy services sends the IT policy packet to the BlackBerry Dispatcher.
5	The BlackBerry Dispatcher compresses and encrypts the content.	The BlackBerry Dispatcher encrypts the content with the user encryption key, compresses it, and then sends the content to the BlackBerry Router for delivery to the BlackBerry device.
6	The BlackBerry Router sends the content 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 BlackBerry device that is registered on the wireless network.
7	The BlackBerry device returns a delivery confirmation.	The wireless network locates the BlackBerry device and delivers the content. The BlackBerry device checks the BlackBerry Enterprise Server identifier and the IT policy authentication key on the packet. If the BlackBerry Enterprise Server identifier or the IT policy authentication key do not match those of the current IT policy, the BlackBerry device rejects the packet. If the BlackBerry device accepts the packet, it sends a delivery confirmation to the BlackBerry Enterprise Server. If the policy service does not receive delivery confirmation, it resends the IT policy at the interval specified in the Policy Resend Interval. The policy service continues to resend the IT policy until it receives a delivery confirmation.
8	The BlackBerry device decompresses and decrypts the content.	The BlackBerry device decrypts and decompresses the content. The BlackBerry device stores the IT policy settings.

Activate a BlackBerry device wirelessly

Step	Action	Description
1	The user receives or purchases a new BlackBerry device.	The user receives or purchases a new BlackBerry device and contacts the IT department to activate it.
2	The administrator creates a password.	The administrator uses the BlackBerry Manager to create a temporary wireless enterprise activation password for the user account and communicates that password to the user. The password applies to the user account only. The password is no longer valid if any of the following events occur: • the BlackBerry Enterprise Server successfully activates a BlackBerry device on the account using the password • five consecutive unsuccessful activation attempts are made on the account • user fails to activate a BlackBerry device within the expiry window
3	The user initiates a wireless enterprise activation.	The user opens the enterprise activation application on the BlackBerry device and types the appropriate corporate email address and wireless enterprise activation password.
4	The BlackBerry device sends an activation request.	The BlackBerry device sends an activation request message to the corporate email account. The message contains information about the BlackBerry device, such as routing information and the BlackBerry device activation public keys. See the *BlackBerry Wireless Enterprise Activation Technical White Paper* for more information about public key encryption.
5	The BlackBerry Enterprise Server sends an activation response.	The BlackBerry Enterprise Server sends the BlackBerry device an activation response that contains routing information about the BlackBerry Enterprise Server and the public keys for the BlackBerry Enterprise Server.
6	The BlackBerry Enterprise Server and BlackBerry device establish and confirm encryption keys.	The BlackBerry Enterprise Server and the BlackBerry device establish a master encryption key. The BlackBerry Enterprise Server and the BlackBerry device confirm their knowledge of the master key to one another. If key confirmation succeeds, the activation proceeds and further communication is encrypted.
7	The BlackBerry Enterprise Server sends the IT policy.	The BlackBerry Enterprise Server sends the IT policy. If the BlackBerry device cannot accept the IT policy, as a security measure, the activation does not complete.
8	The BlackBerry Enterprise Server 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 BlackBerry device. The user can now send messages from and receive messages on the BlackBerry device.
9	The BlackBerry Enterprise Server sends 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 BlackBerry device, including the following information: • calendar entries • address book entries • tasks • memos • messages • existing BlackBerry device options (if applicable) that were backed up using automatic wireless backup If the user is at the desktop computer, you can use the device 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.

Reconcile a BlackBerry device without wireless data flow

Step	Action	Description
1	The user connects the BlackBerry device.	The user connects the BlackBerry device to a computer on which the device manager is running.
2	The BlackBerry Router authenticates the BlackBerry device.	The BlackBerry Router uses a unique authentication protocol to verify that the user is a valid user. The authentication sequence uses the authentication information that the BlackBerry Enterprise Server and the BlackBerry device use to validate each other. The BlackBerry Router does not learn the value of the master encryption key that passes between the BlackBerry device and the BlackBerry Enterprise Server.
3	Data bypasses the wireless network.	The BlackBerry Router and the device manager manage all data flow to and from the BlackBerry device over the physical connection behind the firewall. The BlackBerry device sends data to the BlackBerry Router using the device manager. The BlackBerry Router sends data to the BlackBerry device using the device manager. All data that is sent between the BlackBerry device and the BlackBerry Enterprise Server is compressed and encrypted. When the user disconnects the BlackBerry device from the desktop computer or closes the device manager, the wireless data flow is restored.

Send an application to a BlackBerry device wirelessly

Step	Action	Description
1	The administrator installs the application in the shared network drive.	The administrator installs the Java application in a shared network drive on an administration computer.
2	The administrator updates the software configuration.	The administrator adds the application to the user's software configuration and specifies wireless delivery of the application.
3	The policy service sends the software configuration to the BlackBerry Dispatcher.	The policy service sends the software configuration to the BlackBerry Dispatcher.
4	The BlackBerry Dispatcher encrypts and compresses the data.	The BlackBerry Dispatcher encrypts the data with the user encryption key, compresses it, and then sends the data to the BlackBerry Router for delivery to the BlackBerry device.
5	The BlackBerry Router sends the data to the wireless network.	The BlackBerry Router sends the data over port 3101 to the wireless network, which verifies that the PIN belongs to a valid BlackBerry device that is registered on the wireless network.
6	The device agent compares the status of applications in the software configuration to those on the BlackBerry device.	The BlackBerry device accepts the software configuration. The device agent compares the software configuration to the applications currently installed on the BlackBerry device. If the applications do not match those defined in the software configuration (for example, an earlier version is installed on the BlackBerry device), the device agent reports the updates required to the policy service.
7	The policy service sends the applications to the BlackBerry Dispatcher.	The policy service receives the request and sends the applications to the BlackBerry Dispatcher.
8	The BlackBerry Dispatcher encrypts and compresses the data.	The BlackBerry Dispatcher encrypts the data with the user encryption key, compresses it, and then sends the data to the BlackBerry Router for delivery to the BlackBerry device.

Step	Action	Description
9	The BlackBerry Router sends the data to the wireless network.	The BlackBerry Router sends the data over port 3101 to the wireless network, which verifies that the PIN belongs to a valid BlackBerry device that is registered on the wireless network.
10	The BlackBerry device installs the application.	The BlackBerry device decrypts and decompresses the data and installs the application. The application appears on the Home screen as an icon or appears in the list of installed applications on the BlackBerry device.

©2006 Research In Motion Limited

Published in Canada.