

BlackBerry Enterprise Server for Microsoft Exchange

Version: 5.0
Service Pack: 4



Feature and Technical Overview

Contents

1	Document revision history.....	6
2	What's New in BlackBerry Enterprise Server 5.0 SP4.....	7
3	Overview: BlackBerry Enterprise Server.....	9
4	BlackBerry Enterprise Server architecture.....	10
	Architecture: BlackBerry Enterprise Server.....	10
	Architecture: Remote BlackBerry Collaboration Service.....	14
	Architecture: Remote BlackBerry MDS Connection Service.....	16
	Architecture: Remote BlackBerry Router.....	17
	Architecture: Remote BlackBerry Administration Service.....	19
	Architecture: Remote BlackBerry Attachment Service.....	20
	Architecture: BlackBerry Web Desktop Manager.....	22
5	BlackBerry Enterprise Server components and features.....	24
	BlackBerry Administration Service.....	24
	BlackBerry Configuration Panel.....	25
	BlackBerry Mail Store Service.....	25
	Database tables in the BlackBerry Configuration Database that store contact information	26
	Contact information that the BlackBerry Mail Store Service stores in the BlackBerry Configuration Database	26
	How the BlackBerry Mail Store Service accesses contact information that is stored on the messaging server	27
	Configuring the BlackBerry Mail Store Service instance that updates the contact list	27
	BlackBerry messaging and collaboration services	28
	BlackBerry Messaging Agent.....	28
	BlackBerry Collaboration Service.....	31
	BlackBerry Synchronization Service.....	34
	BlackBerry Attachment Service.....	35
	BlackBerry MDS Connection Service.....	36
	BlackBerry Applications.....	38
	BlackBerry Browser Applications.....	38
	BlackBerry Java Applications.....	38
	Managing BlackBerry Java Applications and BlackBerry Device Software.....	39
	BlackBerry device management.....	40
	Controlling third-party applications on BlackBerry devices.....	40
	BlackBerry Policy Service.....	40
	BlackBerry Router.....	41
	BlackBerry Web Desktop Manager	42
	Comparison of BlackBerry Web Desktop Manager and BlackBerry Desktop Software features.....	43

	Managing a distributed environment for BlackBerry Enterprise Server components	47
	Wireless activation	47
6	BlackBerry Enterprise Solution security.....	48
	Security features of the BlackBerry Enterprise Solution.....	49
	Encrypting data that the BlackBerry Enterprise Server and a BlackBerry device send to each other	50
	Algorithms that the BlackBerry Enterprise Solution uses to encrypt data.....	50
	Extending messaging security to a BlackBerry device	51
	Encrypting user data on a locked device.....	51
	Encrypting the device transport key on a locked device.....	52
	Managing device access to the BlackBerry Enterprise Server.....	52
	Using an IT policy to manage BlackBerry Enterprise Solution security.....	53
	Using IT administration commands to protect a lost or stolen device.....	54
7	BlackBerry Enterprise Server high availability.....	56
	BlackBerry Enterprise Server high availability in a small-scale environment.....	56
	How the BlackBerry Enterprise Server calculates health scores	57
	Conditions for failover to a standby BlackBerry Enterprise Server	58
	How a primary BlackBerry Enterprise Server self-demotes	58
	Scenario: What happens after a primary BlackBerry Enterprise Server stops responding.....	59
	Scenario: What happens after the health score of a primary BlackBerry Enterprise Server falls below the failover threshold.....	60
	BlackBerry Configuration Database high availability.....	60
	BlackBerry Configuration Database mirroring	61
	Scenario: What happens after the principal BlackBerry Configuration Database stops responding.....	62
	High availability in a distributed environment.....	63
8	Wi-Fi enabled devices.....	65
	Types of Wi-Fi networks	65
	Wireless access points.....	66
	Connections that BlackBerry devices make to mobile and Wi-Fi networks.....	67
	Connecting Wi-Fi enabled BlackBerry devices to the BlackBerry Enterprise Server over a Wi-Fi connection.....	68
	Direct connections between BlackBerry devices and the BlackBerry Router over an enterprise Wi-Fi network.....	68
	Wi-Fi connection when a VPN connection or direct connection between BlackBerry devices and the BlackBerry Router is not possible.....	69
	Priority for connections that BlackBerry devices make over a Wi-Fi network.....	69
	BlackBerry services that are available over Wi-Fi connections.....	70
	IEEE 802.11 wireless networking standards that Wi-Fi enabled BlackBerry devices support.....	72
	Characteristics of the IEEE 802.11a wireless networking standard that Wi-Fi enabled BlackBerry devices support.....	72
	Characteristics of the IEEE 802.11b wireless networking standard that Wi-Fi enabled BlackBerry devices support.....	73
	Characteristics of the IEEE 802.11g wireless networking standard that Wi-Fi enabled BlackBerry devices support.....	74
	Security features of a Wi-Fi enabled device.....	74
9	BlackBerry Enterprise Server process flows.....	76

	Messaging process flows.....	76
	Process flow: Sending a message to a BlackBerry device.....	76
	Process flow: Sending a message from a BlackBerry device.....	77
	Process flow: Sending a message that contains an attachment from a BlackBerry device.....	78
	Process flow: Searching an organization's address book from a BlackBerry device.....	79
	Instant messaging process flows.....	80
	Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Live Communications Server 2005 (Microsoft Office Communicator).....	80
	Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Communications Server 2007.....	81
	Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010.....	83
	Process flow: Starting an instant messaging session using the BlackBerry Client for IBM Sametime.....	84
	Process flow: Starting an instant messaging session using the BlackBerry Client for Novell GroupWise Messenger.....	85
	Process flow: Sending a file to a contact using the BlackBerry Client for IBM Sametime.....	87
	Message attachment process flows.....	88
	Process flow: Viewing a message attachment.....	88
	Process flow: Viewing an attachment using a link.....	89
	Organizer data process flows.....	91
	Process flow: Synchronizing organizer data for the first time on a BlackBerry device.....	91
	Process flow: Synchronizing subsequent changes to organizer data.....	92
	Process flow: Adding a contact picture on a BlackBerry device.....	93
	Mobile data process flows.....	94
	Process flow: Requesting BlackBerry Browser content on a BlackBerry device.....	94
	Process flow: Requesting BlackBerry Browser content while access control is turned on for the BlackBerry MDS Connection Service.....	96
	Process flow: Requesting BlackBerry Browser content with two-factor authentication turned on.....	97
	Process flow: Pushing application content to a BlackBerry device.....	98
	Process flow: Installing a BlackBerry Java Application on a BlackBerry device over the wireless network.....	99
	BlackBerry device management process flows.....	101
	Process flow: Activating a BlackBerry device over the wireless network.....	101
	Process flow: Resending an IT policy to a BlackBerry device manually.....	102
	Process flow: Authenticating data on a BlackBerry device without connecting to the BlackBerry Infrastructure	102
10	Glossary.....	103
11	Provide feedback.....	107
12	Legal notice	108

Document revision history

1

Date	Description
14 February 2013	Initial version
7 November 2013	Updated for maintenance release 6

What's New in BlackBerry Enterprise Server 5.0 SP4

2

Feature	Description
Upgrade paths	<p>Administrators can upgrade to BlackBerry Enterprise Server 5.0 SP4 from the following software versions:</p> <ul style="list-style-type: none"> • BlackBerry Enterprise Server 5.0 SP2 • BlackBerry Enterprise Server 5.0 SP3 <p>Administrators can upgrade to BlackBerry Enterprise Server 5.0 SP4 for Novell GroupWise from BlackBerry Enterprise Server 5.0 SP1 for Novell GroupWise.</p> <p>There is no direct upgrade path from BlackBerry Enterprise Server 4.x.</p>
Upgraded Java support	BlackBerry Enterprise Server 5.0 SP4 supports JRE v6.31 or higher
BlackBerry Monitoring Service removed	BlackBerry Enterprise Server 5.0 SP4 does not include the BlackBerry Monitoring Service. No version of the BlackBerry Monitoring Service works with BlackBerry Enterprise Server 5.0 SP4.
Character set support	BlackBerry Enterprise Server 5.0 SP4 includes support for sending messages that use Latin characters along with Hebrew or Arabic characters.
Increased message size limit	BlackBerry Enterprise Server 5.0 SP4 increases the maximum size of HTML email messages from 32KB to 300KB.
Increased attachment size limit	BlackBerry Enterprise Server 5.0 SP4 increases the default maximum attachment size from 3MB to 10MB.
Enhancements to email prepopulation	<p>BlackBerry Enterprise Server 5.0 SP4 enhances the email prepopulation process in the following ways:</p> <ul style="list-style-type: none"> • Includes both header and body information in prepopulated messages • Increases the default number of messages to prepopulate to 1000 or 14 days of messages • Performs prepopulation at every activation, not just when a PIN changes (for example if all data and applications are deleted and the smartphone is activated again)

Feature	Description
Increased efficiency of reconciliation process	BlackBerry Enterprise Server 5.0 SP4 includes enhancements that reduce the workload on the computer that hosts the BlackBerry Configuration Database.
Enhancements to security features	BlackBerry Enterprise Server 5.0 SP4 includes security enhancements that are designed to allow verification of data integrity and authenticity for organizations that use multiple layers of encryption.
Full synchronization of sent email messages	BlackBerry Enterprise Server 5.0 SP4 synchronizes the full body of sent messages to the BlackBerry smartphone.
Canceled meeting options	BlackBerry Enterprise Server 5.0 SP4 allows you to leave canceled meetings in the calendar on your BlackBerry smartphone instead of automatically removing them.
Enhancements to access control policies	BlackBerry Enterprise Server 5.0 SP4 allows administrators to assign access control policies to both individuals and groups.
Support for password-protected attachments	The BlackBerry Attachment Service in BlackBerry Enterprise Server 5.0 SP4 supports password-protected attachments.
Changes to sent message timestamps	BlackBerry Enterprise Server 5.0 SP4 uses the time from the BlackBerry smartphone to indicate the time a message was sent instead of using the time on the server. Sent messages now display the correct sent time even if the BlackBerry smartphone is in a time zone that is different from the BlackBerry Enterprise Server.
Support for additional shapes in Microsoft PowerPoint	The BlackBerry Attachment Service for BlackBerry Enterprise Server 5.0 SP4 displays more shapes from Microsoft PowerPoint attachments.
Online help for BlackBerry Enterprise Transporter	The BlackBerry Enterprise Transporter, a tool available in the BlackBerry Enterprise Server Resource Kit 5.0 SP4 includes online help.
BlackBerry Domain Search tool removed	The BlackBerry Enterprise Server Resource Kit 5.0 SP4 does not include the BlackBerry Domain Search tool because BlackBerry Management Studio includes the features the tool offered.
Improvements to certificate administration	Administrators can configure VPN profile certificates for BlackBerry smartphones so that the user does not need to perform this task.

Overview: BlackBerry Enterprise Server

3

The BlackBerry Enterprise Server is designed to be a secure, centralized link between an organization's wireless network, communications software, applications, and BlackBerry smartphones. The BlackBerry Enterprise Server integrates with your organization's existing infrastructure to provide smartphone users with mobile access to your organization's resources.

You can manage the BlackBerry Enterprise Server, smartphones, and user accounts using the BlackBerry Administration Service. You can access the BlackBerry Administration Service web application from any computer that can access the computer that hosts the BlackBerry Administration Service.

You can optionally install BlackBerry Management Studio in your organization's environment to provide a simplified administrative console for your organization's helpdesk administrators and an integrated view of the BlackBerry Enterprise Server and other MDM domains. For more information, visit <http://www.blackberry.com/go/serverdocs> to see the *BlackBerry Management Studio Feature and Technical Overview*.

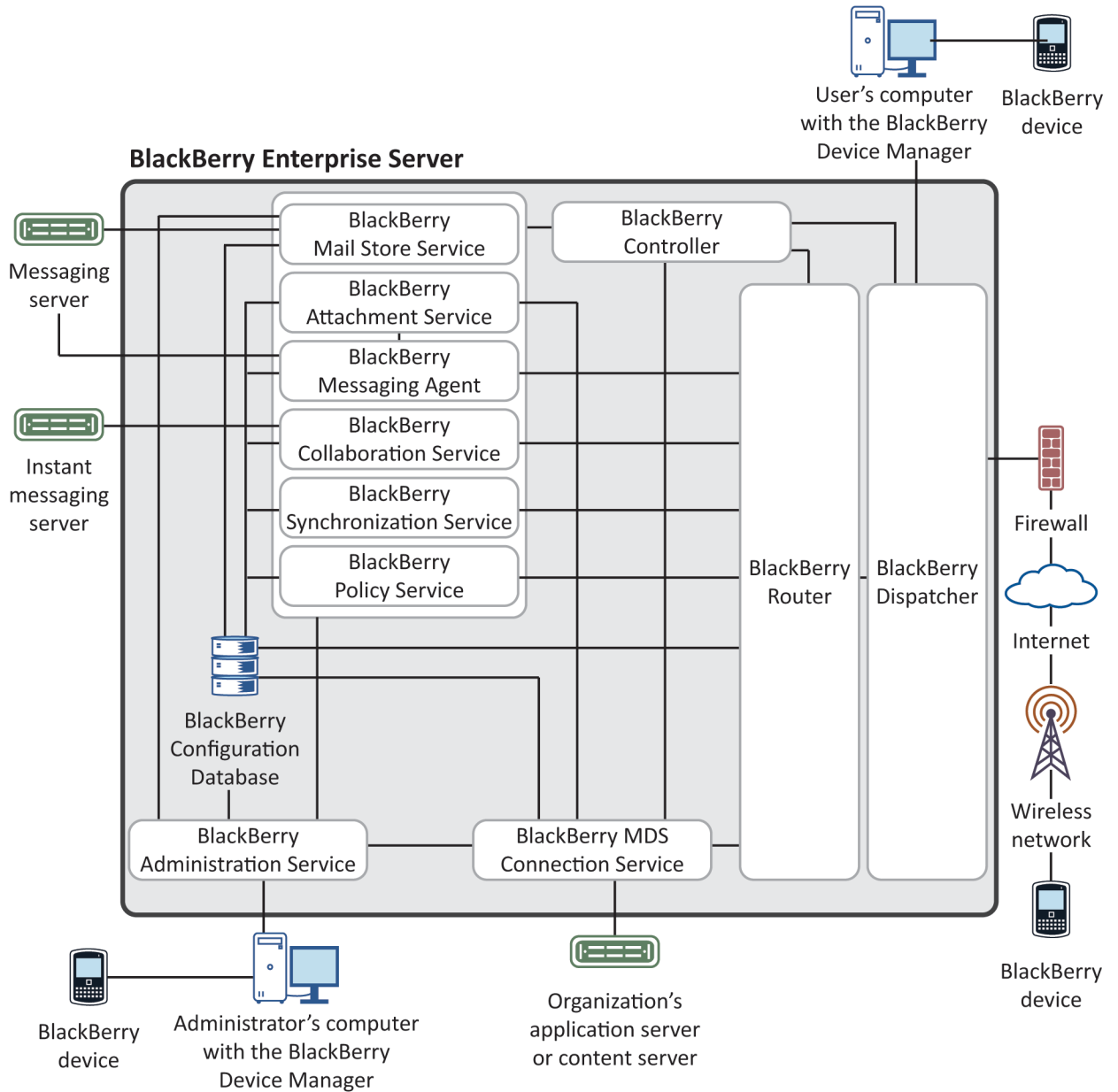
BlackBerry Enterprise Server architecture

4

Architecture: BlackBerry Enterprise Server

The BlackBerry Enterprise Server consists of various components that are designed to perform the following actions:

- Permit BlackBerry device users to access your organization's tools and data from BlackBerry devices and run your organization's applications on devices
- Process, route, compress, and encrypt data
- Communicate with the wireless network



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service connects to the BlackBerry Configuration Database. You can use the BlackBerry Administration Service to manage the BlackBerry Domain, which includes BlackBerry Enterprise Server components, user accounts, and features for BlackBerry device administration.
BlackBerry Mail Store Service	<p>The BlackBerry Mail Store Service connects to the messaging servers in your organization's environment and retrieves the contact information that the BlackBerry Administration Service requires to search for user accounts on the messaging servers.</p> <p>You install a BlackBerry Mail Store Service when you install a BlackBerry Enterprise Server. The BlackBerry Mail Store Service connects to the messaging server using the same connection information that the BlackBerry Enterprise Server uses. The BlackBerry Administration Service is designed to communicate with the BlackBerry Mail Store Service using RPC.</p>
BlackBerry Attachment Service	The BlackBerry Attachment Service converts supported message attachments to a format that users can view on their devices.
BlackBerry Collaboration Service	The BlackBerry Collaboration Service provides a connection between your organization's instant messaging server and the collaboration client on devices.
BlackBerry Configuration Database	<p>The BlackBerry Configuration Database is a relational database that contains configuration information that BlackBerry Enterprise Server components use. For example, the BlackBerry Configuration Database includes the following information:</p> <ul style="list-style-type: none"> • details about the connection from a BlackBerry Enterprise Server to the wireless network • user list • address mappings between PINs and email addresses for BlackBerry MDS Connection Service push features
BlackBerry Controller	The BlackBerry Controller monitors the BlackBerry Enterprise Server components and restarts them if they stop responding.
BlackBerry Dispatcher	The BlackBerry Dispatcher compresses and encrypts all data that devices send and receive. The BlackBerry Dispatcher sends the data through the BlackBerry Router, to and from the wireless network.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service permits users to access web content, the Internet, or your organization's intranet, and also permits applications on devices to connect to your organization's application servers or content servers for application data and updates.
BlackBerry Messaging Agent	The BlackBerry Messaging Agent connects to the IMAP server so that users can activate their devices over the wireless network. The BlackBerry Messaging

Component	Description
	Agent connects to your organization's messaging server to provide messaging services, calendar management, address lookups, attachment viewing, attachment downloading, and encryption key generation. The BlackBerry Messaging Agent also acts as a gateway so that the BlackBerry Synchronization Service can access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and the BlackBerry profiles database. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and the message store databases.
BlackBerry Policy Service	The BlackBerry Policy Service performs administration services over the wireless network. It sends IT policies and IT administration commands and provisions service books. IT policies and IT administration commands specify security, settings for synchronizing data over the wireless network, and other configuration settings on devices. The BlackBerry Policy Service also sends service books to devices to configure settings for features and components on devices.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send data to and from devices. It also sends data over your organization's network to devices that users connected to computers that host the BlackBerry Device Manager.
BlackBerry Synchronization Service	The BlackBerry Synchronization Service synchronizes organizer data between BlackBerry devices and the messaging server over the wireless network.
BlackBerry Web Desktop Manager	The BlackBerry Web Desktop Manager is a web-based application that permits users to manage their devices. For example, users can activate devices, back up and restore data, select messaging options, synchronize data, and install applications. The BlackBerry Web Desktop Manager includes the BlackBerry Device Manager.
organization's application server or content server	Your organization's application server or content server provides push applications and intranet content that the BlackBerry MDS Services use.
instant messaging server	The instant messaging server stores instant messaging accounts.
messaging server	The messaging server stores email accounts.
user's computer that hosts the BlackBerry Device Manager	<p>The user's computer that hosts the BlackBerry Device Manager permits users to connect their devices to their computers using a serial connection or USB connection. The BlackBerry Enterprise Server and devices use the connection to send data between each other.</p> <p>Data traffic from devices bypasses the wireless network when devices are connected to users' computers. The BlackBerry Device Manager connects to the BlackBerry Router, which sends data directly to devices.</p>

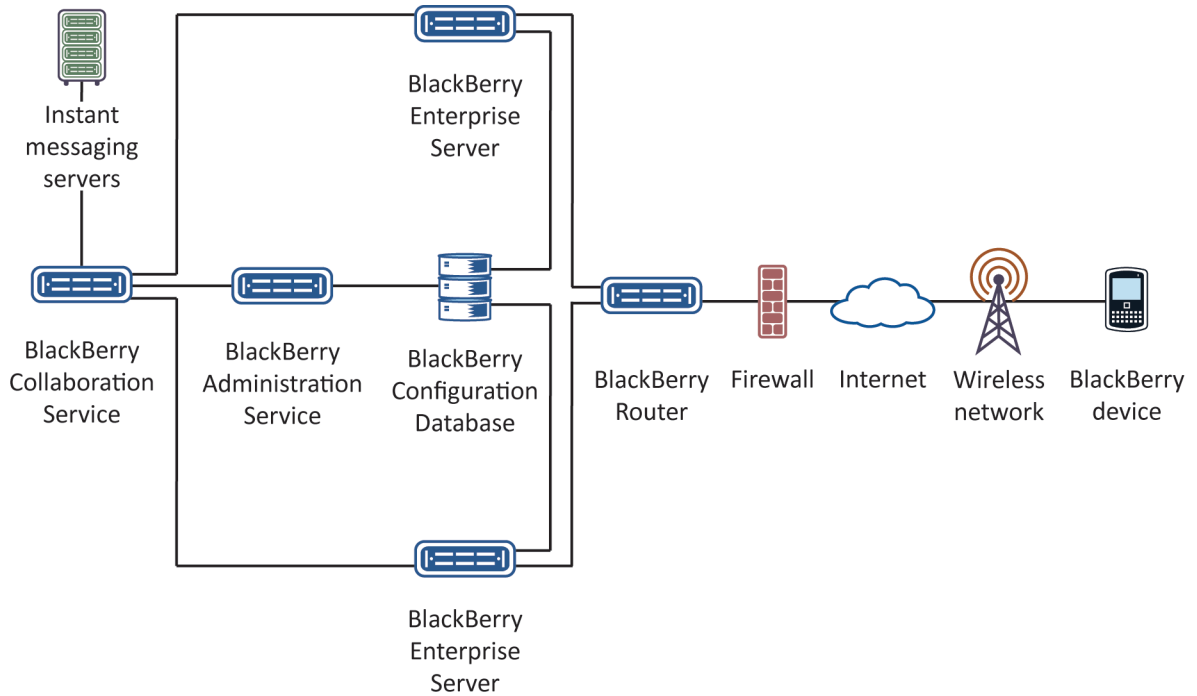
Component	Description
	Users can install the BlackBerry Device Manager when they install the BlackBerry Desktop Software or at another time. The BlackBerry Device Manager is an optional component, but it is required to support a bypass connection to the BlackBerry Router.

Architecture: Remote BlackBerry Collaboration Service

You can install the BlackBerry Collaboration Service on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server. You can install the BlackBerry Collaboration Service on a remote computer to support multiple BlackBerry Enterprise Server instances, configure high availability for the BlackBerry Enterprise Server but exclude the BlackBerry Collaboration Service, or create a BlackBerry Collaboration Service pool that can support multiple BlackBerry Enterprise Server instances. For more information about configuring the BlackBerry Collaboration Service high availability, see the *BlackBerry Enterprise Server Planning Guide*.

The BlackBerry Collaboration Service uses a persistent socket connection for each instant messaging session. You can install the BlackBerry Collaboration Service on a remote computer to maximize the number of available sockets.

You can install only one type of BlackBerry Collaboration Service (for example, IBM Sametime). Users can use only one type of collaboration client on their BlackBerry devices.

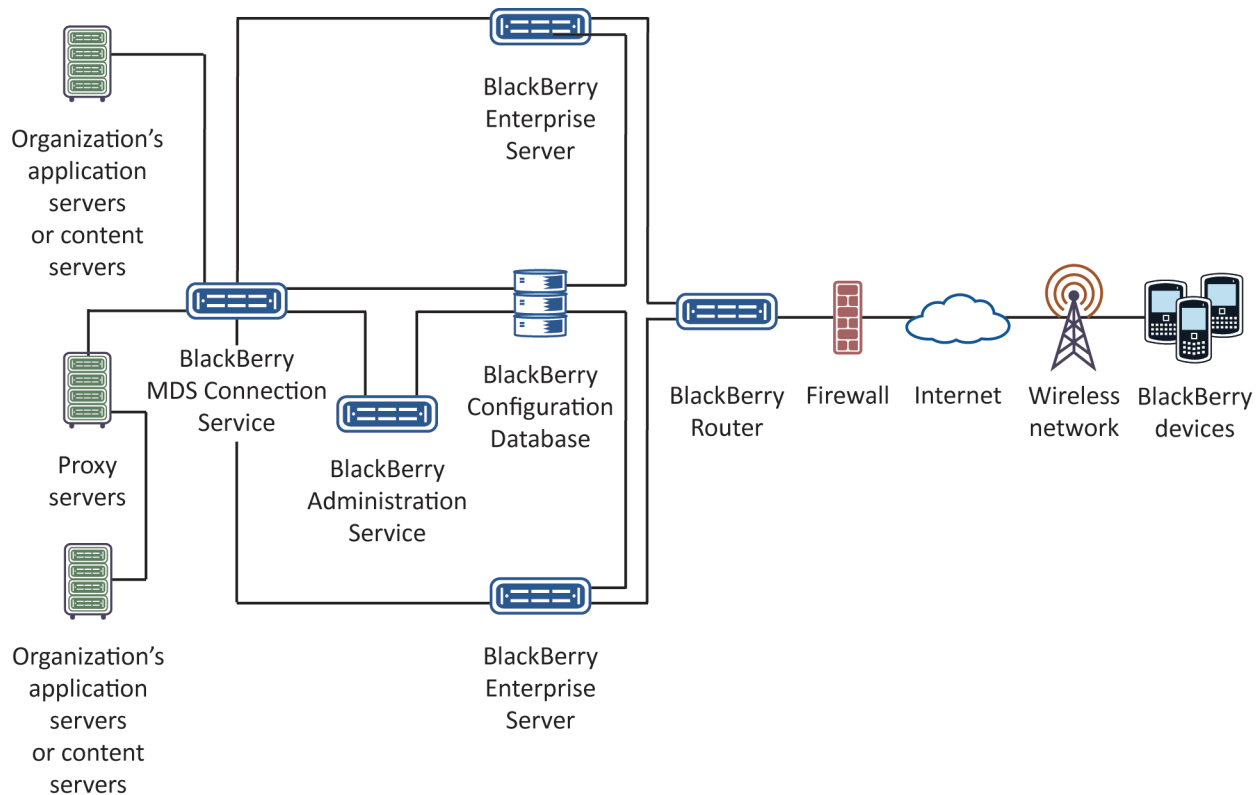


Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Collaboration Service and configure instant messaging features.
BlackBerry Collaboration Service	The BlackBerry Collaboration Service delivers messages between the instant messaging server, BlackBerry Enterprise Server, and BlackBerry devices.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Collaboration Service uses.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses instant messaging data that BlackBerry devices receive, and decompresses and decrypts instant messaging data that BlackBerry devices send.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send instant messaging data to and from BlackBerry devices.

Architecture: Remote BlackBerry MDS Connection Service

You can install the BlackBerry MDS Connection Service on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server. The BlackBerry MDS Connection Service can use increased system resources when it processes requests for content. You can install the BlackBerry MDS Connection Service on a remote computer to minimize the impact on the delivery of messages and data, support multiple BlackBerry Enterprise Server instances, or create a BlackBerry MDS Connection Service pool that can support multiple BlackBerry Enterprise Server instances.

For information about configuring BlackBerry MDS Connection Service high availability, see the *BlackBerry Enterprise Server Planning Guide*.



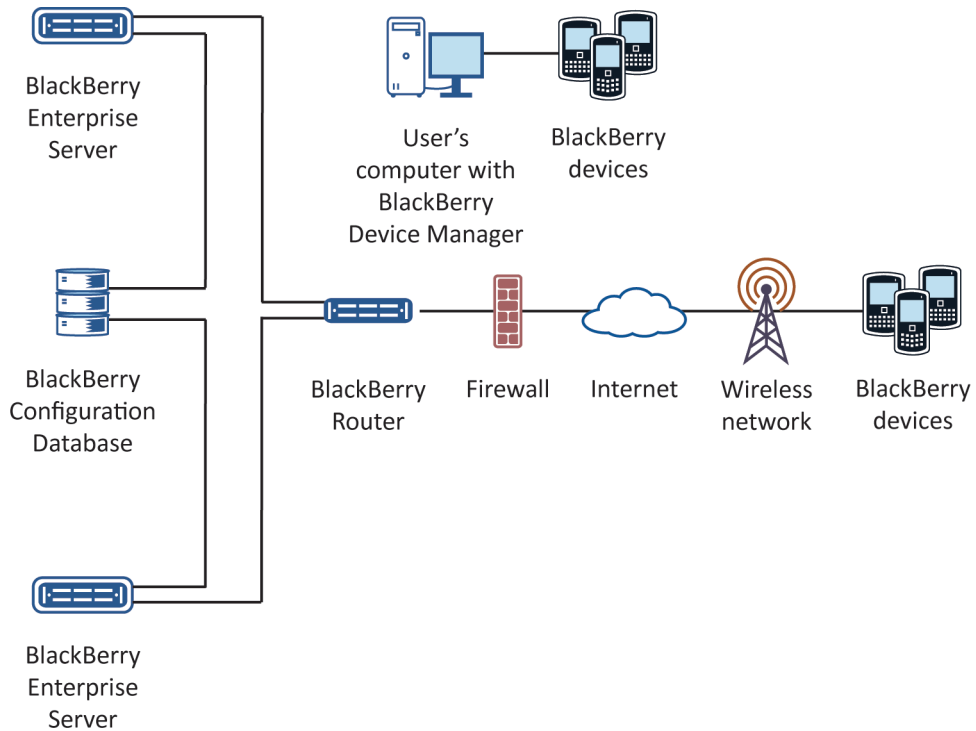
Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry MDS Connection Service, configure the central push server, and configure the browsing and application features.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains the configuration data that the BlackBerry MDS Connection Service uses.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses content data that BlackBerry devices receive, and decompresses and decrypts content data that BlackBerry devices send.
BlackBerry MDS Connection Service	The BlackBerry MDS Connection Service processes requests for web content from the BlackBerry Browser or a BlackBerry Java Application, and it manages the connections between a BlackBerry Application and the application that is located on your organization's application servers, web servers, or databases.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send content to and from BlackBerry devices.
organization's application servers or content servers	Your organization's application servers or content server provide push applications and intranet content for the BlackBerry MDS Services.
proxy servers	Proxy servers authenticate the BlackBerry Browser or a BlackBerry Java Application before they can access push applications or content data.

Architecture: Remote BlackBerry Router

You can install the BlackBerry Router on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server. You can install the BlackBerry Router on a remote computer if you want to support multiple BlackBerry Enterprise Server instances, create a remote BlackBerry Router pool, or if your organization's security policy requires that internal systems cannot make connections directly to the Internet and all systems must connect through another system in the DMZ.

The BlackBerry Router does not use many system resources, but it is a critical connection point for the BlackBerry Enterprise Solution. You can install multiple BlackBerry Router instances for high availability if the primary BlackBerry Router becomes unavailable.

If you install the BlackBerry Router in the DMZ, you can permit users to log in to your organization's LAN remotely and you can deploy BlackBerry devices through a computer that is running the BlackBerry Device Manager.



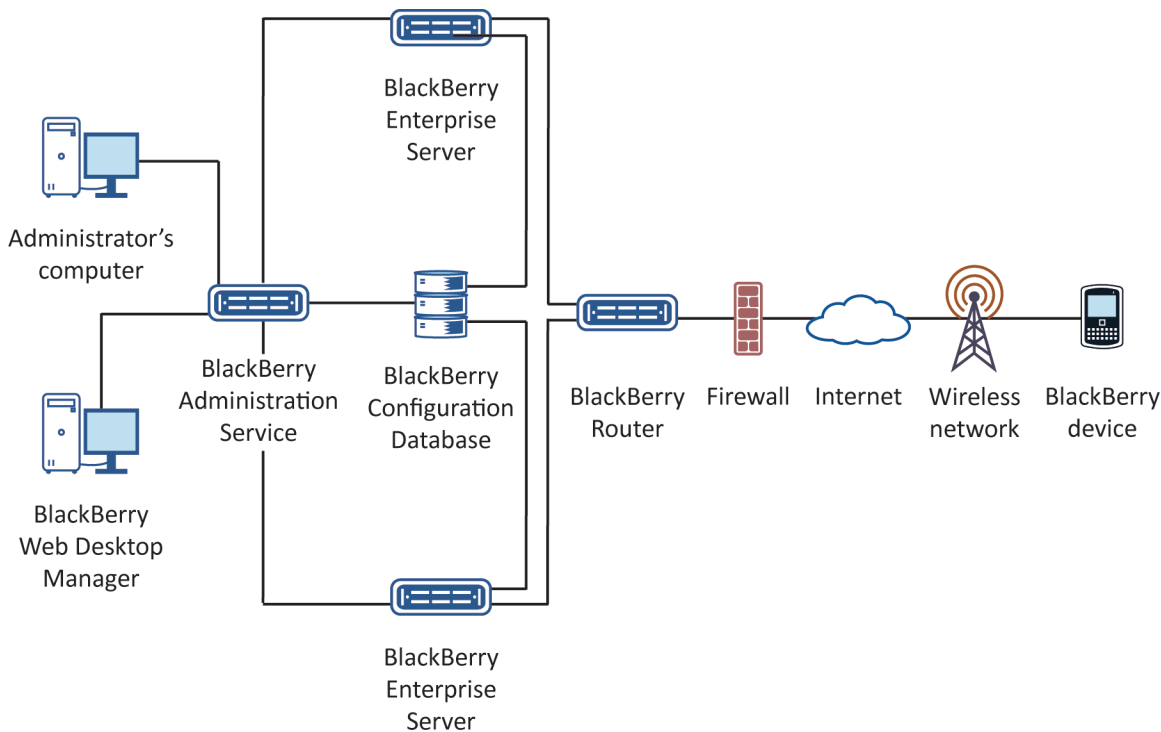
Component	Description
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Administration Service manages.
BlackBerry Device Manager	The BlackBerry Device Manager permits BlackBerry devices to connect to the BlackBerry Router.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses data that BlackBerry devices receive, and decompresses and decrypts data that BlackBerry devices send.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send data to and from BlackBerry devices.

Architecture: Remote BlackBerry Administration Service

You can install the BlackBerry Administration Service on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server. The BlackBerry Administration Service can use increased system resources when it processes requests. You can install the BlackBerry Administration Service remotely to minimize the impact on the delivery of messages and data, or to create a BlackBerry Administration Service pool to support multiple BlackBerry Enterprise Server instances.

For more information about configuring BlackBerry Administration Service high availability, see the *BlackBerry Enterprise Server Planning Guide*.

You can install the BlackBerry Web Desktop Manager with the BlackBerry Administration Service. You can install the BlackBerry Web Desktop Manager separately to make sure that BlackBerry device users cannot access the computer that hosts the BlackBerry Enterprise Server.

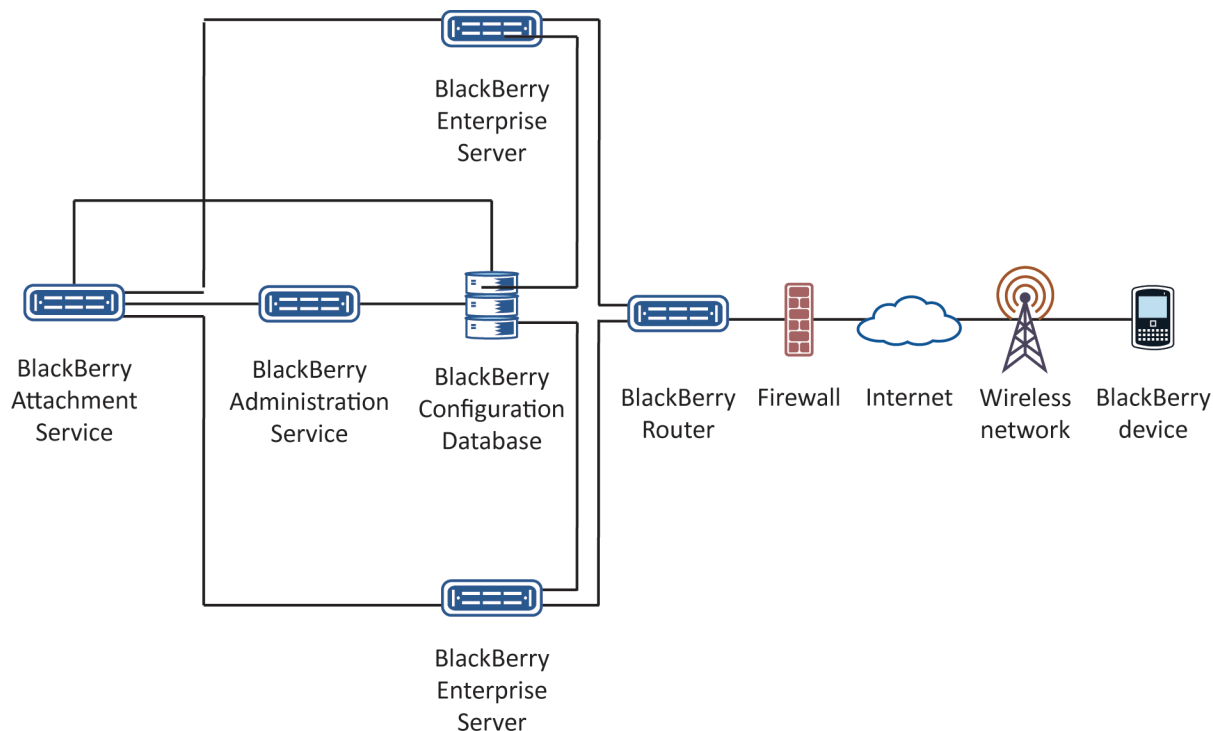


Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Enterprise Server, user accounts, and BlackBerry devices.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains configuration data that the BlackBerry Administration Service manages.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses data that BlackBerry devices receive, and decompresses and decrypts data that BlackBerry devices send.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send data to and from BlackBerry devices.
BlackBerry Web Desktop Manager	The BlackBerry Web Desktop Manager permits users to activate and manage their BlackBerry devices, back up and restore data, configure email settings, update the BlackBerry Device Software, and install new applications.

Architecture: Remote BlackBerry Attachment Service

You can install the BlackBerry Attachment Service on a computer that is separate from the computer that hosts the BlackBerry Enterprise Server. You can install the BlackBerry Attachment Service remotely if you want to increase the number of conversion requests that can occur concurrently without impacting message delivery, support multiple BlackBerry Enterprise Server instances, or create a BlackBerry Attachment Service pool that can support multiple BlackBerry Enterprise Server instances.

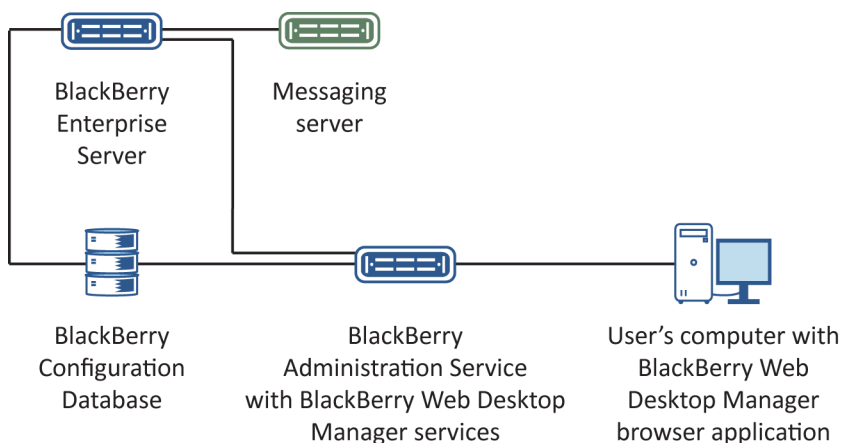
For more information about how to configure the BlackBerry Attachment Service for high availability, see the *BlackBerry Enterprise Server Planning Guide*.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service permits you to manage the BlackBerry Attachment Service instances and set up attachment conversion features.
BlackBerry Attachment Service	The BlackBerry Attachment Service converts the attachment and returns the attachment data to the BlackBerry Attachment Connector.
BlackBerry Configuration Database	The BlackBerry Configuration Database contains the conversion data that the BlackBerry Attachment Service uses when processing attachment data.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server receives requests to convert message attachments from BlackBerry devices and uses the BlackBerry Attachment Connector to send the attachment data to a BlackBerry Attachment Service instance for conversion. After the BlackBerry Attachment Service instance returns the converted attachment to the BlackBerry Attachment Connector, the BlackBerry Enterprise Server sends the attachment data to the user's BlackBerry device for viewing.
BlackBerry Router	The BlackBerry Router connects to the wireless network to send email messages and attachments to and from BlackBerry devices.

Architecture: BlackBerry Web Desktop Manager

The BlackBerry Web Desktop Manager consists of server-side services that are installed with the BlackBerry Administration Service and Microsoft ActiveX controls that are installed on the browser of the BlackBerry device user's computer. HTTPS authentication secures the connection between the server and the browser.



Component	Description
BlackBerry Administration Service	The BlackBerry Administration Service is a web application that is a required component of the BlackBerry Enterprise Server. Administrators use the BlackBerry Administration Service to manage user accounts; assign user groups, administrator roles, software configurations, and IT policies to user accounts; and manage servers and components in a BlackBerry Domain.
BlackBerry Enterprise Server	The BlackBerry Enterprise Server encrypts and compresses data that BlackBerry devices receive, and decompresses and decrypts data that BlackBerry devices send.
BlackBerry Configuration Database	The BlackBerry Configuration Database is a relational database that contains configuration information, such as BlackBerry Enterprise Server connection details and user information.
messaging server	The messaging server stores the email accounts of the BlackBerry device users.

Component	Description
user's computer with BlackBerry Web Desktop Manager browser application	The BlackBerry Web Desktop Manager browser application is the Microsoft ActiveX controls that a user installs in a browser to manage the BlackBerry device.
BlackBerry Administration Service and BlackBerry Web Desktop Manager services	The BlackBerry Administration Service and BlackBerry Web Desktop Manager services provide the server-side services for the BlackBerry Web Desktop Manager browser application.

BlackBerry Enterprise Server components and features

5

BlackBerry Administration Service

The BlackBerry Administration Service is a web application you use to manage user accounts; assign user groups, administrative roles, and software configurations and apply IT policies to user accounts; and manage servers and component instances in a BlackBerry Domain. You can open the BlackBerry Administration Service in a browser on any computer that can access the computer that hosts the BlackBerry Administration Service. You can share administrative duties with multiple administrators who can access the BlackBerry Administration Service simultaneously using unique user names and passwords. When Microsoft ActiveX controls are turned on in your browser, you can connect BlackBerry devices to your computers and manage the BlackBerry devices while you are logged in to the BlackBerry Administration Service.

Feature	Description
high availability of BlackBerry Enterprise Server components	You can install standby instances of BlackBerry Enterprise Server components and configure a manual or automatic failover to a standby instance.
ability to assign users to multiple groups	Groups permit you to share administrative roles, IT policies, and other configuration settings among similar user accounts so that properties can be set once instead of for every user. You can assign a user account to more than one group so that the user inherits the properties of every group that the user belongs to. You can also assign groups to other groups to share the properties of the parent group with all of the user accounts in the child groups.
custom server and component names using friendly names	To help you identify servers and component instances, you can define a friendly name for each BlackBerry Enterprise Server and component instance that displays in the BlackBerry Administration Service. Each regional language that the BlackBerry Administration Service supports can have unique friendly names.
custom administrative roles	Each action that you perform in the BlackBerry Administration Service is associated with a privilege. You can specify the actions that administrators can perform by changing the privilege that you assign to administrative roles.
BlackBerry Administration Service authentication or external authentication	Administrators that log in to the BlackBerry Administration Service must provide their user names and passwords. A user name and a password is a unique combination that is stored securely in the BlackBerry Configuration Database

Feature	Description
options for viewing the BlackBerry Domain	and known only to the BlackBerry Administration Service. Alternatively, you can use external authentication, which permits administrators to log in to the BlackBerry Administration Service using the same information that administrators use to access your organization's messaging server. You can find and manage BlackBerry Enterprise Server component instances using the server view or component view.

BlackBerry Configuration Panel

The BlackBerry Configuration Panel displays data, such as BlackBerry Configuration Database settings, that the BlackBerry Enterprise Server setup application detected during the installation process. You can use the BlackBerry Configuration Panel to change configuration data after you install the BlackBerry Enterprise Server.

BlackBerry Mail Store Service

The BlackBerry Mail Store Service connects to the messaging servers in your organization's environment and retrieves the contact information that the BlackBerry Administration Service requires to search for user accounts on the messaging servers.

The BlackBerry Mail Store Service performs the following actions:

- synchronizes your organization's contact list to the BlackBerry Configuration Database
- updates the contact list in the BlackBerry Configuration Database every 24 hours automatically
- permits the BlackBerry Administration Service to access user account information that is stored in the mailbox or mail file on the messaging servers
- exposes an API that the BlackBerry Administration Service can use to connect to the BlackBerry Mail Store Service
- searches for contact information on behalf of the BlackBerry Administration Service

You install a BlackBerry Mail Store Service when you install a BlackBerry Enterprise Server. The BlackBerry Mail Store Service connects to the messaging server using the same connection information that the BlackBerry Enterprise Server uses. The BlackBerry Administration Service is designed to communicate with the BlackBerry Mail Store Service using RPC.

Database tables in the BlackBerry Configuration Database that store contact information

The BlackBerry Mail Store Service synchronizes contact information to two database tables in the BlackBerry Configuration Database.

Table name	Description
MsDomains	This table contains a list of domains and messaging servers that are located in your organization's environment.
MsAddresses	This table contains a list of the email addresses that are included in your organization's contact list.

Contact information that the BlackBerry Mail Store Service stores in the BlackBerry Configuration Database

The BlackBerry Mail Store Service synchronizes contact information that is stored in the messaging environment to the BlackBerry Configuration Database. To compare the contact information changes that occurred between synchronization processes, the BlackBerry Mail Store Service maintains two copies of the contact information.

The BlackBerry Mail Store Service synchronizes contact information that is stored in the messaging environment to the BlackBerry Configuration Database. The contact information is stored in database properties in the BlackBerry Configuration Database.

Contact information	Database property name	Database property name in BlackBerry Configuration Database version 4.1	Description
address type	Type	—	This property specifies whether this is the address for a user or distribution list.
display name	DisplayName	UserConfig.DisplayName	This property specifies the display name for the user account.
email address	MailboxSMTP	UserConfig.MailboxSMTP Addr	This property specifies the email address for the user account.

Contact information	Database property name	Database property name in BlackBerry Configuration Database version 4.1	Description
mailbox path	MailboxKey	UserConfig.MailboxDN	This property specifies the unique mailbox path.
messaging server path	ServerName	UserConfig.ServerDN	This property specifies the path to the messaging server.

How the BlackBerry Mail Store Service accesses contact information that is stored on the messaging server

In a Microsoft Exchange environment, the BlackBerry Mail Store Service can connect to the messaging server and search for contact information using MAPI or LDAP. By default, the BlackBerry Mail Store Service uses MAPI to search for contact information. If you configure the BlackBerry Enterprise Server to use LDAP to search for contact information, the BlackBerry Mail Store Service can also use LDAP to search for contact information.

For more information about how the BlackBerry Enterprise Server uses LDAP, visit www.blackberry.com/support to read article KB05174.

Configuring the BlackBerry Mail Store Service instance that updates the contact list

The BlackBerry Configuration Database contains your organization's contact list and a list of BlackBerry Enterprise Server instances. By default, the BlackBerry Mail Store Service instance that you installed with the first BlackBerry Enterprise Server instance that appears in the list updates the contact list. If you prevent the BlackBerry Mail Store Service that you installed with the first BlackBerry Enterprise Server instance from updating the contact list, the next available BlackBerry Mail Store Service instance in the list updates the contact list.

By default, if you install multiple BlackBerry Mail Store Service instances, each instance can update the contact list in the BlackBerry Configuration Database. The first BlackBerry Mail Store Service instance that updates the contact list prevents the other instances from also updating the contact list. Each BlackBerry Mail Store Service instance searches for time stamp information in the BlackBerry Configuration Database to determine if another BlackBerry Mail Store Service instance is updating the contact list already before it starts to update the contact list.

You must verify that at least one BlackBerry Mail Store Service instance can update the contact list in the BlackBerry Configuration Database so that the BlackBerry Administration Service can access the latest contact list information when you create and manage user accounts. If you prevent all of the BlackBerry Mail Store Service instances from updating the

contact list, the BlackBerry Configuration Database might not contain the contact information for all user accounts on your organization's messaging server.

If the BlackBerry Configuration Database does not contain contact information for a user account, you cannot create the user account by searching for the contact information in the BlackBerry Administration Service. You can only create the user account if you use the Add from company directory option in the BlackBerry Administration Service. The Add from company directory option permits the BlackBerry Mail Store Service to search the contact information that is stored in the messaging environment so that you can create the user account even if the BlackBerry Configuration Database does not contain the contact information for the user account.

BlackBerry messaging and collaboration services

The BlackBerry messaging and collaboration services provide a wireless extension of your organization's messaging environment. These services include the BlackBerry Messaging Agent, BlackBerry Collaboration Service, BlackBerry Synchronization Service, and BlackBerry Attachment Service.

BlackBerry Messaging Agent

The BlackBerry Messaging Agent connects to your organization's messaging server and provides messaging services, calendar management, address lookups, attachment viewing, attachment downloading, and encryption key generation. The BlackBerry Messaging Agent acts as a gateway for the BlackBerry Synchronization Service to access organizer data on the messaging server. The BlackBerry Messaging Agent synchronizes configuration data between the BlackBerry Configuration Database and user mailboxes.

The BlackBerry Messaging Agent integrates with existing email accounts in your organization. The BlackBerry Messaging Agent redirects messages from users' email applications to their BlackBerry devices automatically. If users configure identical signatures on their BlackBerry devices and in their email accounts, recipients cannot distinguish between messages that users send from BlackBerry devices and messages that they send from email applications.

When users move or delete messages or mark messages as read or unread on their BlackBerry devices or in their email applications, the BlackBerry Messaging Agent reconciles changes over the wireless network between BlackBerry devices and email applications. By default, BlackBerry devices and the BlackBerry Enterprise Server reconcile email messages over the wireless network.

Wireless messaging features

BlackBerry device users can use many of the same messaging features that are available in the email applications on their computers.

Feature	Description
email reconciliation	<p>The BlackBerry Enterprise Server reconciles the status of messages between users' BlackBerry devices and their email applications. If users delete, archive, or move messages to personal folders in their email applications, the messages are deleted from the message list on the users' BlackBerry devices. If users mark messages as read or unread in their email applications, the messages appear with the same status on their BlackBerry devices.</p> <p>You can turn off wireless email reconciliation.</p>
email message filters	<p>You or users can create and change email message filters. Email message filters determine the actions that the BlackBerry Enterprise Server takes if incoming messages match specific criteria: forward, forward with priority, or do not forward to BlackBerry devices. For example, users can create email message filters to forward messages from specific senders to their BlackBerry devices with high priority.</p>
message forwarding	<p>Users can turn off message forwarding to their BlackBerry devices (for example, if users are outside of a wireless coverage area). You can also turn off message forwarding to users' BlackBerry devices.</p>
signature	<p>Users can add a signature to all messages that they send from their BlackBerry devices. You can add a signature and disclaimers to all messages that the members of a user group send or a specific user sends.</p>
out-of-office reply	<p>Users can set and change their out-of-office replies using their BlackBerry devices.</p>
contact lookup	<p>Users can search for a contact's first name, last name, or both in their organization's directory. The BlackBerry Enterprise Server returns results for a maximum of 20 of the closest matches.</p>
contact list updates	<p>When users select contacts from the contact lookup results, they can add the contacts to the contact lists on their BlackBerry devices.</p>
custom fields in the contact list	<p>If your organization maintains custom fields in users' personal contact lists, you can map these fields to corresponding fields that appear in the contact list on BlackBerry devices. Users can use these custom fields to search for contacts on their BlackBerry devices.</p>
attachments	<p>Users can send messages that contain attachments from their BlackBerry devices. The BlackBerry Attachment Service does not convert these messages; the BlackBerry Messaging Agent processes them only. Attachments must meet the following requirements:</p> <ul style="list-style-type: none"> • If a user sends one attachment in a message, the file size of the attachment cannot exceed 3 MB. • If a user sends multiple attachments in a message, the total file size of the attachments cannot exceed 5 MB.

Feature	Description
	<ul style="list-style-type: none"> If an attachment exceeds 64 KB, the BlackBerry device sends the attachment in multiple data packets. <p>Users can send messages with attachments only from supported BlackBerry devices that are running BlackBerry Device Software version 4.2 or later. If you want to manage the system resources that the BlackBerry Messaging Agent uses to upload and send attachments, you can limit the file size of attachments or prevent users from attaching files to messages. For example, if too many users are sending large attachments, such as pictures or videos, you might want to limit the file size of supported attachments or turn off support for message attachments.</p>
downloading attachments	<p>Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can download attachments and store them on their BlackBerry devices. Users can open and make changes to the downloaded attachments using an appropriate third-party application on their BlackBerry devices. Users can open supported attachment file formats using the media application on their BlackBerry devices.</p> <p>To manage network resources in your organization's environment, you can change the maximum file size of attachments that users can download to their BlackBerry devices.</p>
save sent messages	<p>Users can configure their BlackBerry devices to save copies of messages that they send from their BlackBerry devices in the sent items folder in their email applications.</p>
personal distribution lists	<p>Users with BlackBerry Device Software version 5.0 or later can view personal distribution lists in their contact lists. Users can send messages to the personal distribution lists and delete personal distribution lists from their BlackBerry devices.</p>
public folders	<p>Users with BlackBerry Device Software version 5.0 or later can view and use contacts in public folders from their BlackBerry devices, and copy the contacts to their contact lists. Users can only view the public folders that they have the appropriate permissions for.</p> <p>Users can specify which public folders they want to synchronize to their BlackBerry devices using the BlackBerry Desktop Manager or BlackBerry Web Desktop Manager. You can limit the number of public folders that users can synchronize to their BlackBerry devices.</p>
personal folders	<p>Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can add, delete, move, and rename personal folders from their BlackBerry devices.</p>
follow up flag	<p>Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can flag messages from their BlackBerry devices and set reminder times.</p>

Feature	Description
personal contact subfolders	<p>Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can view personal contact subfolders on their BlackBerry devices and change contact information.</p> <p>Users can specify which contact subfolders that they want to synchronize to their BlackBerry devices using BlackBerry Desktop Manager or BlackBerry Web Desktop Manager. You can limit the number of contact subfolders that a user can synchronize to their BlackBerry devices.</p>
forwarding calendar entries	Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can forward meeting invitations and calendar entries from their BlackBerry devices.
availability of meeting participants	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can view the availability of meeting invitees on their BlackBerry devices. You can turn off this feature using the BlackBerry Administration Service.
remote search for email messages	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can search for email messages that are located on the messaging server from their BlackBerry devices. You can turn off this feature using the BlackBerry Administration Service.
rich content email messages	Users with BlackBerry devices that are running BlackBerry Device Software version 4.5 or later can view HTML and rich content email messages. You can turn off this feature using the BlackBerry Administration Service.

Access to documents on a network from BlackBerry devices

Users with BlackBerry devices that are running BlackBerry Device Software version 5.0 or later can use a file browser on their BlackBerry devices to access documents that are located in a shared location such as a network drive. Users can view document information such as the file name, file type, file size, author, and date the file was last changed. Users must have access to the shared location using their network credentials, or you must configure the BlackBerry Enterprise Server to access the documents for the users.

Users can send the documents as attachments in messages or instant messages, view supported document types using the attachment viewer, download copies of the documents, or open and make changes to the documents using an appropriate third-party application on their BlackBerry devices. They can also add attachments from messages or documents that they access using the BlackBerry Browser to the network drive.

BlackBerry Collaboration Service

The BlackBerry Collaboration Service provides a connection between your organization's instant messaging server and the collaboration client on BlackBerry devices. The BlackBerry Collaboration Service integrates with existing instant messaging applications. The BlackBerry Enterprise Server supports the following collaboration clients:

- BlackBerry Client for use with Microsoft Office Live Communications Server 2005

- BlackBerry Client for use with Microsoft Office Communications Server 2007
- BlackBerry Client for use with Microsoft Office Communications Server 2007 R2
- BlackBerry Client for use with Microsoft Lync Server 2010
- BlackBerry Client for IBM Sametime
- BlackBerry Client for Novell GroupWise Messenger

The BlackBerry Collaboration Service sends instant messages between your organization's instant messaging server, BlackBerry Enterprise Server, and devices using public APIs, a Research In Motion proprietary protocol, and protocols that IBM, Microsoft, and Novell specify.

Instant messaging features

Using the collaboration clients on their BlackBerry devices, users can use many of the same features that are available in the instant messaging applications on their computers.

Feature	Description
session management	<p>You can specify the number of simultaneous instant messaging sessions that the BlackBerry Collaboration Service supports. You can also specify a timeout threshold, after which the BlackBerry Collaboration Service ends inactive sessions automatically and permits new sessions to start.</p> <p>You can control whether users of specific versions of the BlackBerry Client for IBM Sametime or the BlackBerry Client for Novell GroupWise Messenger can see an icon on their BlackBerry devices when contacts in their contact lists are using the same collaboration clients. By default, the icon appears.</p>
conversations with multiple contacts	Users can start and manage conversations with multiple instant messaging contacts on their BlackBerry devices.
availability status	Users can change their availability status when they are logged in to their collaboration clients. For example, users can set their availability status to away or busy.
presence updates	Using the latest versions of the collaboration clients, users can set their availability status to display as away if they do not use their BlackBerry devices for a specified period of time.
access levels	Using the latest version of the BlackBerry Client for use with Microsoft Office Communications Server 2007, users can set the access level of contacts in their contact lists. Each access level consists of rules that define how contacts can interact with a user through the instant messaging application. For example, users can assign the Personal access level to their contacts.
contact pictures	Using the latest versions of the collaboration clients, users can add pictures to the contacts in their contact lists. The pictures that users add using the collaboration clients on their BlackBerry devices are not synchronized with the instant messaging applications on users' computers.

Feature	Description
synchronized contact lists	The instant messaging contact lists on users' BlackBerry devices are synchronized with the contact lists in their organization's instant messaging application.
contact alerts	Users can request alerts when specific contacts become available.
file transfer	Using the latest version of the BlackBerry Client for IBM Sametime, users can send files to contacts in their contact lists. Recipients can open supported file formats on their BlackBerry devices.
link instant messaging contacts to the contact list on BlackBerry devices	Using the latest versions of the collaboration clients, users can link instant messaging contacts to existing contact list entries on their BlackBerry devices. They can also create new contact list entries for instant messaging contacts and populate them with information from their organization's messaging server.
send email messages from contact list	Using the latest versions of the collaboration clients, users can send email messages to contacts directly from their contact lists.
call contacts	Using the latest versions of the collaboration clients, users can call instant messaging contacts directly from their contact lists. After a user starts an instant messaging conversation with a contact, the user can make a call to that contact from the conversation window. Phone numbers for contacts are retrieved from the messaging server or from the contact list on the BlackBerry device if the user is linked to an existing contact list entry.
email conversation history	Using the latest versions of the collaboration clients, users who participate in an instant messaging conversation can send the history of the conversation as an email message to other participants of the conversation and to additional contacts from their contact lists on their BlackBerry devices.
embedded links	Users can click phone numbers in instant messages to make calls. They can also click links in instant messages to view web pages.
public groups	Using the latest version of the BlackBerry Client for IBM Sametime, users can add public groups to their instant messaging contact lists.
location information	Using the latest version of the BlackBerry Client for IBM Sametime or the BlackBerry Client for use with Microsoft Office Communications Server 2007, users can set their current location to display in their contact information. For example, users can set their current location to "In the office". This feature is not available if your organization's environment uses IBM Sametime version 6.5.1.
announcements	Using the latest version of the BlackBerry Client for IBM Sametime or BlackBerry Client for Novell GroupWise Messenger, users can send announcements to groups or multiple contacts in their contact lists.
send messages to contacts who are not included in a contact list	Using the latest version of the BlackBerry Client for IBM Sametime, BlackBerry Client for use with Microsoft Office Live Communications Server 2005, or

Feature	Description
	BlackBerry Client for use with Microsoft Office Communications Server 2007, users can send instant messages to contacts that are not included in their contact lists.
dormant mode	The collaboration clients enter dormant mode after five minutes of inactivity. In dormant mode, the applications do not receive presence updates for contacts. Dormant mode is designed to reduce wireless network traffic in an organization's messaging environment. The collaboration clients turn off dormant mode when users open or use the applications, or receive conference requests, alerts, or messages from contacts.

BlackBerry Synchronization Service

The BlackBerry Synchronization Service synchronizes organizer data such as tasks, memos, and contacts over the wireless network so that the entries on BlackBerry devices are consistent with the entries in the email applications. With wireless data synchronization and wireless email reconciliation, users are not required to connect their BlackBerry devices to the BlackBerry Desktop Software to synchronize organizer data and reconcile email messages.

The BlackBerry Synchronization Service backs up user settings and data over the wireless network from BlackBerry devices to the BlackBerry Configuration Database. You can restore the user settings and data to BlackBerry devices when the BlackBerry devices are activated over the wireless network. By default, the BlackBerry Enterprise Server automatically backs up the user settings and data over the wireless network.

Synchronization features

You can change the settings for synchronization features so that users can manage the user experience and system resources in your organization's environment.

Feature	Description
initial synchronization	<p>When the BlackBerry Enterprise Server sends service books to BlackBerry devices to turn on wireless data synchronization, an initial data synchronization process starts. The process synchronizes the data for calendar items and messages between users' BlackBerry devices and the email applications on their computers. It also resolves conflicting or duplicate entries to prevent data loss.</p> <p>By default, the calendar on the BlackBerry device synchronizes up to 31 days in the past from the activation date, and up to 28 years into the future from the activation date.</p>
synchronization settings	You can configure settings for wireless data synchronization that apply to specific users, user groups, or all users on all BlackBerry Enterprise Server instances. You can define which organizer data items the BlackBerry Synchronization Service synchronizes, how data conflicts are resolved, and whether changes are synchronized in both directions or in one direction only

Feature	Description
	between BlackBerry devices and email applications. You can use IT policies to configure the settings for wireless data synchronization.
support for different types of user access	The BlackBerry Enterprise Server requires access to the organizer application databases for all users. You can define the location of the database replicas in each user's profile, create roaming user profiles, or use web access templates in your organization's messaging environment.
synchronization of contact pictures	<p>The BlackBerry Synchronization Service synchronizes contact pictures between users' BlackBerry devices and the email applications on their computers. If users use their BlackBerry devices to add, change, or delete contact pictures, the contact lists in their email applications reflect the changes.</p> <p>The BlackBerry Synchronization Service cannot synchronize contact pictures that exceed 32 KB.</p>

BlackBerry Attachment Service

The BlackBerry Attachment Service converts supported message attachments into a format that users can view on their BlackBerry devices. The BlackBerry Attachment Service processes attachments and converts them into a binary format that retains most of the layout, appearance, and navigation of the original attachments. You do not have to install the applications that are associated with the attachment formats on BlackBerry devices. The attachment viewer installs automatically with the BlackBerry Device Software.

The BlackBerry Attachment Service receives attachments that are embedded in messages from the messaging server, through the BlackBerry Messaging Agent. The BlackBerry Attachment Service also receives attachments that are accessed through links in the BlackBerry Browser.

The BlackBerry Attachment Service enables users to play supported audio attachments on supported BlackBerry devices that are running BlackBerry Device Software version 4.2 or later. The BlackBerry Attachment Service can convert .wav files into an audio format that a BlackBerry device series supports (for example, .mp3 files on BlackBerry 8700 Series devices).

If the BlackBerry Attachment Service is hosted on a computer that uses Windows Server 2008, the BlackBerry Attachment Service does not support .mp3 audio files on BlackBerry devices, and the BlackBerry Attachment Service does not support any audio file formats on BlackBerry 7100 Series devices that support CDMA networks. You must host the BlackBerry Attachment Service on a computer that uses Windows Server 2003 if you want the BlackBerry Attachment Service to support .mp3 audio files on BlackBerry devices and all audio formats on BlackBerry 7100 Series devices that support CDMA networks.

Attachment file formats that the BlackBerry Attachment Service supports

Format	Extension
Adobe Acrobat	.pdf
ASCII text	.txt

Format	Extension
audio	.amr, .mp3, .wav, .wma
Corel WordPerfect 7-10	.wpd
HTML	.htm, .html
images	.bmp, .gif, .jpeg, .jpg, .png, .ppm, .tif, .tiff, .wmf
Microsoft Excel 97-2003, 2007, 2013*, and XP	.xls, .xlsx
Microsoft PowerPoint 97-2003, 2007, 2013*, and XP	.pps, .ppsx, .ppt, .pptx
Microsoft Word 97-2003, 2007, 2013*, and XP	.doc, .dot, .dotx, .docx
OpenOffice Format version 1.1	.odp, .ods, .odt, .ott
RTF	.rtf
ZIP archives	.zip

* Some new features in Microsoft Office 2013 attachment files may not be viewable with BlackBerry devices. BlackBerry will provide limited support for Microsoft Office 2013 attachment files.

BlackBerry MDS Connection Service

The BlackBerry MDS Connection Service connects wireless applications on BlackBerry devices to the applications on an organization's application servers or web servers. After a wireless application is installed on BlackBerry devices, the application can receive data from push applications that are located on application servers or web servers. The application can also receive data by sending pull requests from BlackBerry devices to applications that are located on application servers or web servers. The BlackBerry MDS Connection Service processes push and pull requests and delivers data and updates to BlackBerry Applications.

The BlackBerry MDS Connection Service also receives and responds to web requests from the BlackBerry Browser and other BlackBerry Applications, so that users can view Internet and intranet content on their BlackBerry devices. The BlackBerry MDS Connection Service sends login requests and requests for instant messaging sessions from BlackBerry devices to the BlackBerry Collaboration Service. If you stop the BlackBerry MDS Connection Service, you also stop the BlackBerry Collaboration Service.

Feature	Description
protocol connections	You can define connections to the web servers on your organization's intranet or the Internet using standard Internet protocols such as HTTP, HTTPS, and TCP/IP.
encrypted communications	The BlackBerry MDS Connection Service encrypts content using the same standard BlackBerry encryption that the BlackBerry Dispatcher uses to encrypt messages and other data.
data conversion	The BlackBerry MDS Connection Service converts data from application servers and web servers to a format that BlackBerry Applications can interpret and display.
data optimization	The BlackBerry MDS Connection Service processes content that users can view in the BlackBerry Browser. For example, the BlackBerry MDS Connection Service can change the data format or remove extraneous data to reduce network traffic.
authentication methods	<p>You can configure authentication requirements that match your organization's sign-on scheme using standard methods such as NTLM, Kerberos, and LTPA. You can also define a period of time after which the BlackBerry MDS Connection Service requests user information and caches cookies.</p> <p>You can use two-factor authentication to create VPN connections between wireless applications on BlackBerry devices and your organization's application servers and web servers.</p>
integration with proxy servers	<p>You can provide access to specific content through your organization's proxy servers using the following items:</p> <ul style="list-style-type: none"> • proxy exclusion list, which defines the organization-specific URLs that the BlackBerry MDS Connection Service uses to connect directly to external web services instead of routing the connections through your organization's proxy server • proxy auto-configuration (.pac) file
access control	You can configure push initiators and push rules that define which server-side push applications can send application data and updates to BlackBerry devices, and which users can receive push requests. You can configure pull rules to specify which web servers users can access using the BlackBerry Browser and other applications on BlackBerry devices.
media content management	You can control which media files users can receive and access using the BlackBerry Browser and BlackBerry Applications. You can prevent users from receiving specific media types (for example, video files) or specific subtypes of media (for example, .mp3 files). You can also configure size limits for media files that users can receive on their BlackBerry devices.

BlackBerry Applications

BlackBerry devices support BlackBerry Applications and BlackBerry Browser Applications. Application developers in your organization can create BlackBerry Applications using BlackBerry development tools or third-party development tools. You can install and manage BlackBerry Java Applications on BlackBerry devices using the BlackBerry Administration Service.

For more information about the options for developing BlackBerry Applications, visit www.blackberry.com/developers.

BlackBerry Browser Applications

BlackBerry Browser Applications are simplified, web-based applications that you can use to push web content to the BlackBerry Browser on BlackBerry devices. Developers can create BlackBerry Browser Applications using BlackBerry templates or standard web development tools.

The BlackBerry Enterprise Server supports the following types of BlackBerry Browser Applications.

Type	Description
browser channel push applications	An icon displays on the Home screens of users' BlackBerry devices to indicate whether users viewed the latest version of the web content that the Browser Push Engine has pushed to their BlackBerry devices.
browser cache push applications	The Browser Push Engine pushes web content to the cache of the BlackBerry Browser on users' BlackBerry devices. To view the web content, users browse to the appropriate web address using the BlackBerry Browser.
browser message push applications	A message appears in the message list on users' BlackBerry devices to provide a link to new or updated web content.

For more information about developing BlackBerry Browser Applications and sending BlackBerry Browser Applications to BlackBerry devices, visit www.blackberry.com/developers.

BlackBerry Java Applications

BlackBerry Applications can range from simple applications, such as a game on BlackBerry devices, to complex applications with advanced UIs and various options for data management, storage, and network communication. BlackBerry Java Applications can use a client-only architecture (the applications do not send data to or receive data from a content server) or they can use a client/server application model (the applications send data to and receive data from a content server). For example, a developer can create a BlackBerry Java Application so that users can send data to and receive data from a central sales database.

Developers can create BlackBerry Java Applications using BlackBerry developer tools or other Java authoring tools. BlackBerry devices run BlackBerry Java Applications using BlackBerry APIs and Java ME, which are standard on BlackBerry devices.

For more information about developing and customizing BlackBerry Applications, visit www.blackberry.com/developers.

Managing BlackBerry Java Applications and BlackBerry Device Software

You can use the BlackBerry Administration Service to install and manage the BlackBerry Device Software and BlackBerry Java Applications on BlackBerry devices.

To send BlackBerry Java Applications to devices, you must first add the applications to the application repository. You can use the application repository to store and manage all versions of the BlackBerry Java Applications that you want to install on, update on, or remove from devices.

In the BlackBerry Administration Service, you create software configurations to specify the versions of the BlackBerry Device Software and BlackBerry Java Applications that you want to install on, update on, or remove from devices. You also use software configurations to specify which applications are required, optional, or not permitted. When you create a software configuration, you must also specify whether users can install applications that are not listed in the software configuration.

When you add a BlackBerry Java Application to a software configuration, you must assign an application control policy to the application to specify what resources the application can access. You can use default application control policies or you can create and use custom application control policies. If you permit users to install unlisted applications, you must create an application control policy for unlisted applications that specifies what resources the applications can access.

When you assign a software configuration to a group or individual user accounts, the BlackBerry Administration Service creates a deployment job to install the BlackBerry Device Software and BlackBerry Java Applications on devices and to apply application control policies to the devices. A deployment job consists of a number of tasks. Each task manages the delivery of a specific object (for example, a BlackBerry Java Application or an application control policy) by communicating with the appropriate BlackBerry Enterprise Server components.

If you assign more than one software configuration to a user account, all of the settings in the multiple software configurations are applied to the user's device. The BlackBerry Enterprise Server resolves conflicting settings using predefined reconciliation rules and prioritized rankings that you can specify using the BlackBerry Administration Service. After you install the BlackBerry Device Software and BlackBerry Java Applications on devices, you can view details about how the BlackBerry Administration Service resolved software configuration conflicts.

For more information about installing and managing the BlackBerry Device Software on devices, visit www.blackberry.com/go/serverdocs to see the *BlackBerry Device Software Update Guide*.

BlackBerry device management

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

Controlling third-party applications on BlackBerry devices

Feature	Description
control the installation and removal of third-party applications	You can use the BlackBerry Administration Service to install applications on BlackBerry devices over the wireless network, or you can permit users to download and install third-party applications on their BlackBerry devices. You can remove applications from BlackBerry devices over the wireless network, and you can also prevent users from downloading applications.
control the resources that third-party applications can access	<p>You can use standard application control policies or create custom application control policies to specify the resources that third-party applications can access on BlackBerry devices (for example, message, phone, and key store).</p> <p>You can create IT policies that specify the types of connections that third-party applications on BlackBerry devices can establish (for example, opening network connections inside the firewall).</p>

BlackBerry Policy Service

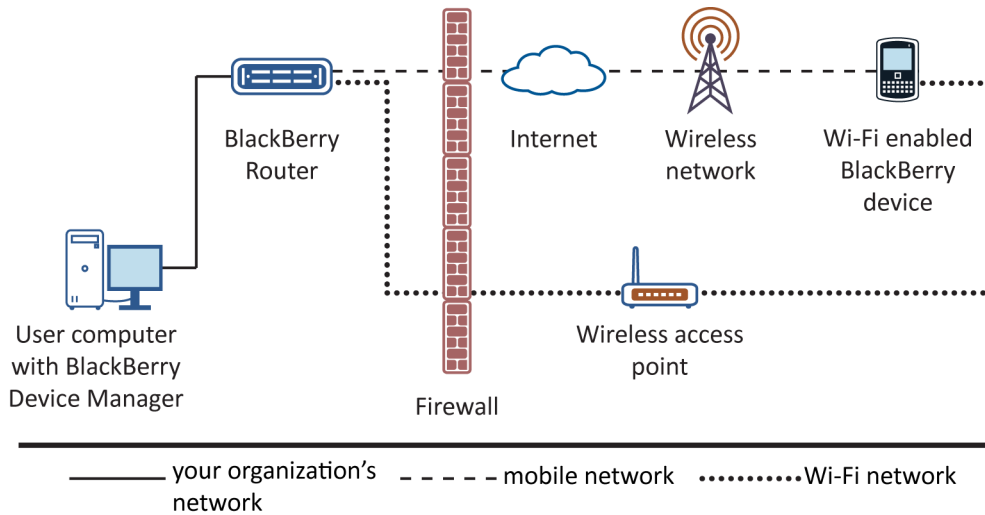
The BlackBerry Policy Service sends IT policies and IT administration commands to BlackBerry devices and provisions service books over the wireless network. When you activate a BlackBerry device, change an IT policy, or request that a BlackBerry Enterprise Server resend service books, the BlackBerry Enterprise Server uses the BlackBerry Policy Service to send the updates to the BlackBerry device.

An IT policy consists of rules that define BlackBerry device security, settings for synchronizing data over the wireless network, and other behaviors for the individual groups or user accounts that you define. You can configure IT policies using the BlackBerry Administration Service.

Feature	Description
wireless delivery	<p>When you configure an IT policy, all rules take effect when the BlackBerry Policy Service delivers the IT policy to a BlackBerry device over the wireless network. The BlackBerry device stores new IT policy rule values in the user configurations on the BlackBerry device automatically.</p> <p>To keep the IT policy rules current, a BlackBerry Enterprise Server sends the IT policy to the BlackBerry device over the wireless network periodically.</p>
IT policy coverage	<p>When you add a user account to a BlackBerry Enterprise Server, the BlackBerry Policy Service applies the Default IT policy to the user account automatically. The user account is not active on the BlackBerry Enterprise Server until a BlackBerry device accepts the IT policy.</p> <p>You can apply a different IT policy to a user account. If you delete an IT policy that you applied to a user account, the BlackBerry Policy Service applies the user account to the Default IT policy automatically.</p>
IT policy assignment	You can apply an IT policy to a group or an individual user account.
resend options	<p>If a BlackBerry Enterprise Server cannot send an updated IT policy to a BlackBerry device immediately (for example, if a user is outside of a wireless coverage area), you can resend the IT policy manually or configure when the BlackBerry Policy Service resends the IT policy. The BlackBerry Enterprise Server continues to resend the IT policy until it delivers the IT policy.</p>
security enforcement	<p>You can configure IT policies that define security settings for BlackBerry devices, the BlackBerry Desktop Software and the BlackBerry Web Desktop Manager, and that override security settings that users define on their BlackBerry devices. For example, you can configure whether a password is required for a BlackBerry device, the length of time that the password can exist before it becomes invalid, and the length and composition of the password. You can also use IT policies to specify encryption key details.</p>

BlackBerry Router

The BlackBerry Router connects to the wireless network and sends data to and receives data from the BlackBerry Infrastructure on behalf of the BlackBerry Enterprise Server. The BlackBerry Router also sends data to and receives data from BlackBerry devices that are connected to the BlackBerry Device Manager or a Wi-Fi network. The BlackBerry Device Manager is included with the BlackBerry Device Software, BlackBerry Web Desktop Manager, and BlackBerry Administration Service.



When the BlackBerry Enterprise Server detects a BlackBerry Router, it identifies the IP address of the computer that hosts the BlackBerry Router and writes the IP address to the BlackBerry Configuration Database. When BlackBerry device users activate devices that are running BlackBerry Device Software 4.0 or later, the BlackBerry Router sends the IP address to the devices in a service book.

If you change the IP address of the computer that hosts the BlackBerry Router, devices detect the change automatically. Users do not need to reconnect devices to the BlackBerry Device Manager to receive the new IP address and a new service book. However, a delay occurs before devices detect the change. During the delay, devices cannot connect to the BlackBerry Device Manager or a Wi-Fi network.

The BlackBerry Router supports the use of multiple network cards on users' computers, which is also known as multihoming.

BlackBerry Web Desktop Manager

The BlackBerry Web Desktop Manager is a web application that provides many of the same features that the BlackBerry Desktop Manager does. Users can connect their BlackBerry devices to their computers using a USB connection or Bluetooth connection, and log in to BlackBerry Web Desktop Manager to activate and manage their BlackBerry devices, back up and restore data, define email settings, and update the BlackBerry Device Software.

Feature	Description
access	Users can access device management and configuration capabilities from any computer that can access the intranet.
application management	Users can use the BlackBerry Web Desktop Manager to install, manage, and remove the applications that are installed on their BlackBerry devices.

Feature	Description
BlackBerry Device Software management	Users can use the BlackBerry Web Desktop Manager to update the BlackBerry Device Software on their BlackBerry devices.
control user's access to features	You can specify the BlackBerry Web Desktop Manager features that users can access using IT policies and settings in the BlackBerry Administration Service.
customizable interface	You can customize the appearance of the UI to match your organization's requirements. You can customize the font colors, logo, and the help.
device activation	Users can use the BlackBerry Web Desktop Manager to set activation passwords and activate their BlackBerry devices.
switch devices	Users can use the BlackBerry Web Desktop Manager to switch BlackBerry devices, and migrate from third-party devices that have BlackBerry Application Suite installed, to BlackBerry devices.
folder redirection	Users can use the BlackBerry Web Desktop Manager to select the folders that the BlackBerry Enterprise Server redirects messages from.
language support	The BlackBerry Web Desktop Manager is available in English, French, German, Italian, Spanish, and Japanese. Users can select a language before they log in to the BlackBerry Web Desktop Manager.
simplified administration	The web UI does not require you to deploy, support, and maintain client-side software such as the BlackBerry Desktop Manager.
service statistics	The BlackBerry Web Desktop Manager provides users with statistics about the message status (forwarded, sent, pending, expired, filtered), last contact time, and information about the last message sent or received.
synchronization of contact folders	Users can use the BlackBerry Web Desktop Manager to select the public or private contact folders that they want to synchronize to their BlackBerry devices over the wireless network.

Comparison of BlackBerry Web Desktop Manager and BlackBerry Desktop Software features

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Software
ability to view the BlackBerry Desktop Software that is installed on the users' computers	supported	supported
application loader tool	supported with the following conditions:	supported with the following conditions:

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Software
	<ul style="list-style-type: none"> option to choose not to save the backup file BlackBerry services are not maintained if the users disconnect their BlackBerry devices before completing the process 	<ul style="list-style-type: none"> no option to choose whether to save the backup file BlackBerry services are maintained if the users disconnect their BlackBerry devices before clicking the Close button in the Load was successful dialog box
BlackBerry Desktop Redirector	not included	included
BlackBerry Device Software updates	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> you install the software on a shared network drive BlackBerry Web Desktop Manager forces users to update the BlackBerry Device Software when a software configuration is assigned to the user accounts 	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> users install the software on their computers and run the application loader tool BlackBerry Desktop Manager notifies the users when a newer version of BlackBerry Device Software is available on their computers
certificate synchronization	not supported	supported
changing the email profile options	not supported	supported
connections to BlackBerry devices	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> users can connect to multiple BlackBerry devices at the same time BlackBerry Web Desktop Manager does not prompt users if they want to switch from using a Bluetooth connection to using a USB connection 	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> users can connect to only one BlackBerry device at a time BlackBerry Desktop Software prompts users if they want to switch from using a Bluetooth connection to using a USB connection
device activation	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> occurs automatically for new users if users without active BlackBerry devices connect BlackBerry 	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> occurs automatically each time users plug in a BlackBerry device

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Software
	<p>devices that belong to other users, the BlackBerry Web Desktop Manager prompts the users who connected the BlackBerry devices if they want to switch to the BlackBerry devices</p>	<ul style="list-style-type: none"> • if users without active BlackBerry devices connect BlackBerry devices that belong to other users, the BlackBerry Desktop Software notifies the users who connected the BlackBerry devices that an activation process is underway by asking the users whether an encryption key should be created
switching devices	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> • users can switch from third-party devices that are running BlackBerry Application Suite to BlackBerry devices • users can switch between BlackBerry devices • BlackBerry services are not maintained if users disconnect their BlackBerry devices before completing the process 	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> • users can switch from third-party devices to BlackBerry devices • BlackBerry services are maintained if users disconnect their BlackBerry devices before clicking the Close button in the Switch was successful dialog box
email message settings	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> • users can import data from the address book when creating or changing a filter • users cannot turn off message redirection while their BlackBerry devices are connected • users cannot generate encryption keys • users cannot override email addresses 	<p>supported with the following conditions:</p> <ul style="list-style-type: none"> • users can import data for filtering • users can turn off message redirection while their BlackBerry device are connected • users can generate encryption keys • users can override email addresses
media management	not supported	supported
modem support for devices	not supported	supported

Supported feature	BlackBerry Web Desktop Manager	BlackBerry Desktop Software
prompt for BlackBerry device password	BlackBerry devices can connect without a prompt for the device password	required before BlackBerry devices can connect to the users' computers
statistics for user accounts	supported with the following conditions: <ul style="list-style-type: none"> • all supported messaging environments • users cannot clear the redirection queue • users cannot clear the redirection statistics 	supported with the following conditions: <ul style="list-style-type: none"> • Microsoft Exchange environments only • users can clear the redirection queue • users can clear the redirection statistics
supported BlackBerry Device Software versions	BlackBerry Device Software version 4.0 and later	all
supported IT policies	<ul style="list-style-type: none"> • Auto Backup Enabled • Auto Backup Exclude Messages • Auto Backup Exclude Sync • Auto Backup Frequency • Auto Backup Include All • Desktop Allow Device Switch • Desktop Password Cache Timeout • Do Not Save Sent Messages • Force Load Message 	<ul style="list-style-type: none"> • Auto Backup Enabled • Auto Backup Exclude Messages • Auto Backup Exclude Sync • Auto Backup Frequency • Auto Backup Include All • Desktop Allow Device Switch • Desktop Password Cache Timeout • Disable Media Manager • Do Not Save Sent Messages • Force Load Count • Forward Message In Cradle • Message Prompt • Show AppLoader • Show Web Link
synchronization over a serial connection	users cannot synchronize the following data over a serial connection: <ul style="list-style-type: none"> • organizer data • email messages • third-party application data • date and time 	users can synchronize the following data over a serial connection: <ul style="list-style-type: none"> • organizer data • email messages • third-party application data • date and time

Managing a distributed environment for BlackBerry Enterprise Server components

You can install the BlackBerry Enterprise Server components on multiple computers so that you can manage the size of your organization's BlackBerry Domain. For example, you can install the BlackBerry Attachment Service and BlackBerry MDS Connection Service on separate computers to provide the computer that hosts the BlackBerry Enterprise Server with additional resources that the BlackBerry Enterprise Server can use to process email messages.

Wireless activation

The wireless activation process activates BlackBerry devices that are associated with a BlackBerry Enterprise Server over the wireless network. Neither you nor the BlackBerry device users are required to connect the BlackBerry devices to a computer in your organization's network to complete the activation process.

You can use wireless activation to activate a large number of BlackBerry devices over the wireless network. When BlackBerry device users want to activate new or replacement BlackBerry devices that are associated with the BlackBerry Enterprise Server over the wireless network, they must notify you or access the provisioning server console. You or the BlackBerry device user can create activation passwords.

The BlackBerry Enterprise Solution can begin the wireless activation process automatically or when BlackBerry device users open the activation application on their BlackBerry devices and type their activation passwords and email addresses. When the activation process completes, the BlackBerry device users are activated and can send email messages from and receive email messages on their BlackBerry devices.

If users purchase BlackBerry devices, you must make sure that the BlackBerry devices can be associated with the BlackBerry Enterprise Server and not the BlackBerry Internet Service. You must create user accounts and activate BlackBerry devices so that you can associate the BlackBerry devices with a BlackBerry Enterprise Server.

BlackBerry Enterprise Solution security

6

The BlackBerry Enterprise Solution consists of various products and components that are designed to extend your organization's communication methods to BlackBerry devices. The BlackBerry Enterprise Solution is designed to help protect data that is in transit at all points between a device and the BlackBerry Enterprise Server. To help protect data that is in transit over the wireless network, the BlackBerry Enterprise Server and device use symmetric key cryptography to encrypt the data sent between them. The BlackBerry Enterprise Solution is designed to prevent third parties, including wireless service providers, from accessing your organization's potentially sensitive information in a decrypted format.

The BlackBerry Enterprise Solution uses confidentiality, integrity, and authenticity, which are principles for information security, to help protect your organization from data loss or alteration.

Principles	Description
confidentiality	The BlackBerry Enterprise Solution uses symmetric key cryptography to help make sure that only intended recipients can view the contents of email messages.
integrity	<p>The BlackBerry Enterprise Solution uses symmetric key cryptography to help protect every email message that the device sends and to help prevent third parties from decrypting or altering the message data.</p> <p>Only the BlackBerry Enterprise Server and the device know the value of the keys that they use to encrypt messages and recognize the format of a decrypted and decompressed message. The BlackBerry Enterprise Server or the device rejects a message automatically if it is not encrypted with keys that they recognize as valid.</p>
authenticity	Before the BlackBerry Enterprise Server sends data to the device, the device authenticates with the BlackBerry Enterprise Server to prove that the device knows the device transport key that is used to encrypt data.

Security features of the BlackBerry Enterprise Solution

Feature	Description
data protection	The BlackBerry Enterprise Solution is designed to protect data that is in transit between the BlackBerry Enterprise Server and a BlackBerry device and data that is in transit between your organization's messaging server and the email application on a user's computer. The BlackBerry Enterprise Solution encrypts data that is stored on the device and in the BlackBerry Configuration Database. To help protect data that is stored on the device, you can require a user to authenticate to the device using a password, a smart card, or both.
encryption key protection	The device is designed to protect the encryption keys that are stored on the device. The device encrypts the encryption keys when the device is locked.
control of device connections	<p>The BlackBerry Enterprise Solution is designed to control the following connections:</p> <ul style="list-style-type: none"> • connections using Bluetooth technology to and from the device • connections from a Wi-Fi enabled device to enterprise Wi-Fi networks <p>The BlackBerry Enterprise Solution is designed to control which devices can connect to the BlackBerry Enterprise Server.</p>
control of the behavior of the device and BlackBerry Desktop Software	<p>To control the behavior of the device and BlackBerry Desktop Software, you can send IT administration commands, IT policies, and application control policies to the device. You can use IT administration commands, IT policies, and application control policies to perform the following actions:</p> <ul style="list-style-type: none"> • You can send IT administration commands to lock the device, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values. • You can send an IT policy to a device to change security settings. You can use the IT policy to enforce the device password and BlackBerry Smart Card Reader password. • You can send an application control policy to a device to control whether third-party applications are available and can connect to the device and whether third-party applications or add-on applications developed by Research In Motion can access work data.

Encrypting data that the BlackBerry Enterprise Server and a BlackBerry device send to each other

To encrypt data that is in transit between the BlackBerry Enterprise Server and a BlackBerry device in your organization, the BlackBerry Enterprise Solution uses BlackBerry transport layer encryption. BlackBerry transport layer encryption is designed to encrypt data from the time that a BlackBerry device user sends a message from the BlackBerry device to when the BlackBerry Enterprise Server receives the message, and from the time that the BlackBerry Enterprise Server sends a message to when the BlackBerry device receives the message.

Before the BlackBerry device sends a message, it compresses and encrypts the message using the device transport key. When the BlackBerry Enterprise Server receives a message from the BlackBerry device, the BlackBerry Dispatcher decrypts the message using the device transport key, and then decompresses the message.

Algorithms that the BlackBerry Enterprise Solution uses to encrypt data

The BlackBerry Enterprise Solution uses AES or Triple DES as the symmetric key cryptographic algorithm for encrypting data. By default, the BlackBerry Enterprise Server uses the strongest algorithm that both the BlackBerry Enterprise Server and the BlackBerry device support for BlackBerry transport layer encryption.

If you configure the BlackBerry Enterprise Server to support AES and Triple DES, by default, the BlackBerry Enterprise Solution generates device transport keys using AES encryption. If a BlackBerry device uses BlackBerry Device Software version 3.7 or earlier or BlackBerry Desktop Software version 3.7 or earlier, the BlackBerry Enterprise Solution generates the device transport keys of the BlackBerry device using Triple DES.

How the BlackBerry Enterprise Solution uses AES to encrypt data

By default, when a BlackBerry device supports AES, the BlackBerry Enterprise Solution uses AES for BlackBerry transport layer encryption. The BlackBerry Enterprise Solution uses AES in CBC mode to generate the message keys and device transport keys. The keys consist of 256 bits of data.

BlackBerry Enterprise Server version 4.0 or later, BlackBerry Device Software version 4.0 or later, and BlackBerry Desktop Software version 4.0 or later support AES.

For more information about how the BlackBerry Enterprise Server uses AES for BlackBerry transport layer encryption to communicate with BlackBerry devices, visit www.blackberry.com/support to read article KB05429.

How the BlackBerry Enterprise Solution uses Triple DES to encrypt data

The BlackBerry Enterprise Solution uses a two-key Triple DES encryption algorithm to generate message keys and device transport keys. In the three iterations of the DES algorithm, the first 56-bit key in outer CBC mode encrypts the data, the second 56-bit key decrypts the data, and the first key encrypts the data again.

The BlackBerry Enterprise Solution stores the message keys and device transport keys as 128-bit binary strings with each parity bit in the least significant bit of each of the 8 bytes of key data. The message keys and device transport keys have overall key lengths of 112 bits and include 16 bits of parity data.

All versions of the BlackBerry Enterprise Server, BlackBerry Device Software, and BlackBerry Desktop Software support Triple DES.

For more information about Triple DES, see *Federal Information Processing Standard - FIPS PUB 81 [3]*.

Extending messaging security to a BlackBerry device

If your organization's messaging environment supports secure messaging technology such as PGP encryption or S/MIME encryption, you can configure the BlackBerry Enterprise Solution to encrypt a message using PGP encryption or S/MIME encryption so that the message remains encrypted when the BlackBerry Enterprise Server forwards the message to the email applications of recipients. To extend messaging security, the sender and recipient must install highly secure messaging technology on the computers that host the email applications and on their BlackBerry devices, and you must configure the BlackBerry devices to use the highly secure messaging technology.

Encrypting user data on a locked device

If you or a BlackBerry device user turns on content protection, you or the user can configure a locked device to encrypt stored user data and data that the locked device receives. When you or a user turns on content protection, a locked device is designed to use AES-256 encryption to encrypt stored data and an ECC public key to encrypt data that the locked device receives.

For example, the locked device uses content protection to encrypt the following items:

- subject, location, meeting organizer, attendees, and any notes in all appointments or meeting requests
- all contact information in the contact list except for the contact title and category
- subject, email addresses of intended recipients, message body, and attachments in all email messages
- title and information that is included in the body of a note for all memos (also known as posted messages)
- subject and all information that is included in the body of tasks (also known as posted all day appointments)

- if you use software tokens, contents of the .sdtid file seed that is stored in flash memory
- all data that is associated with third-party applications that a user installs on the device
- in the BlackBerry Browser, content that web sites or third-party applications push to the device, any web sites that the user saves on the device, and the browser cache
- all text that replaces the text automatically that the user types on the device

You can change the Content Protection of Contact List IT policy rule to Required to prevent the user from turning off content protection for the contact list on the device. If you change the Content Protection of Contact List IT policy rule to Required, the device does not permit call display and does not share contacts over a Bluetooth connection when the device is locked.

Encrypting the device transport key on a locked device

If you turn on content protection for device transport keys, a BlackBerry device uses the principal encryption key to encrypt the device transport keys that are stored in flash memory. The device encrypts the principal encryption key using the content protection key. When a locked device receives data that is encrypted using the device transport key, it uses the decrypted principal encryption key to decrypt the device transport key in flash memory and then uses the decrypted device transport key to decrypt data.

When you, a user, or a password timeout locks the device, the wireless transceiver remains on and the device does not delete the memory that is associated with the principal encryption key or device transport key. The device is designed to prevent the decrypted principal encryption key and the decrypted device transport key from appearing in flash memory.

You can turn on content protection for device transport keys on the device when you configure the Force Content Protection of Master Keys IT policy rule. When you turn on content protection of device transport keys, the device uses the ECC key strength that you specified in the Content Protection Strength IT policy rule to encrypt the device transport keys.

Managing device access to the BlackBerry Enterprise Server

You can use the Enterprise Service Policy to control which BlackBerry devices can connect to a BlackBerry Enterprise Server. By default, after you turn on the Enterprise Service Policy, the BlackBerry Enterprise Server permits connections from any device that you previously associated with the BlackBerry Enterprise Server. The BlackBerry Enterprise Server also prevents connections from any device that you associate with the BlackBerry Enterprise Server after you turn on the Enterprise Service Policy.

You can configure an allowed list to determine which devices can access a BlackBerry Enterprise Server. A device that meets the criteria that you specify in the allowed list can associate with the BlackBerry Enterprise Server when the device activates over the wireless network.

You can define the following types of criteria:

- specific device PINs
- range of device PINs
- specific manufacturers
- specific device models

The BlackBerry Administration Service includes lists of permitted manufacturers and models of devices that you associated with the BlackBerry Enterprise Server previously.

You can permit a user to override the Enterprise Service Policy so that a device can connect to the BlackBerry Enterprise Server even if you configure the allowed list with criteria that exclude that device.

For more information, see the *BlackBerry Enterprise Server Administration Guide*.

Using an IT policy to manage BlackBerry Enterprise Solution security

You can use an IT policy to control and manage BlackBerry devices, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager in your organization's environment. An IT policy consists of multiple IT policy rules that manage the security and behavior of the BlackBerry Enterprise Solution. For example, you can use IT policy rules to manage the following security features and behaviors of the device:

- encryption (for example, encryption of user data and messages that the BlackBerry Enterprise Server forwards to message recipients) and encryption strength
- use of a password or pass phrase
- connections that use Bluetooth wireless technology
- protection of user data and device transport keys on the device
- control of device resources, such as the camera or GPS, that are available to third-party applications

The BlackBerry Enterprise Server includes preconfigured IT policies that you can use to manage the security of the BlackBerry Enterprise Solution. The Default IT policy includes IT policy rules that are configured to indicate the default behavior of the device or BlackBerry Desktop Software.

After a device user activates a device, the BlackBerry Enterprise Server automatically sends to the device the IT policy that you assigned to the user account or group. By default, if you do not assign an IT policy to the user account or group, the BlackBerry Enterprise Server sends the Default IT policy. If you delete an IT policy that you assigned to the user account or group, the BlackBerry Enterprise Server automatically re-assigns the Default IT policy to the user account and resends the Default IT policy to the device.

For more information, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Using IT administration commands to protect a lost or stolen device

The BlackBerry Enterprise Server includes IT administration commands that you can send over the wireless network to protect sensitive data on a BlackBerry device. You can use the commands to lock the device, permanently delete work data, permanently delete user information and application data, and return the device settings to the default values.

IT administration command	Description
Specify new device password and lock device	<p>This command creates a new password and locks a device over the wireless network. You can communicate the new password to the user verbally when the BlackBerry device user locates the device. When the user unlocks the device, the device prompts the user to accept or reject the new password.</p> <p>You can use this command if the device is lost. If you or a user turned on content protection and a device is running BlackBerry Device Software 4.3.0 or later, you can use this command. If you or a user turned on two-factor content protection, you cannot use this command.</p>
Delete only the organization data and remove device	<p>This command permanently deletes all work data that the device stores and removes the device from the BlackBerry Enterprise Server. All personal data remains on the device.</p> <p>You can send this command to a personal device when a user no longer works at your organization and you want to delete work data from the device.</p> <p>You can also specify whether you want to delete or disable a user account from the BlackBerry Enterprise Server after the device deletes all work data.</p>
Delete all device data and remove device	<p>This command permanently deletes all user information and application data that the device stores. You can configure the following options when you use this command:</p> <ul style="list-style-type: none"> • specify a delay, in hours, that must occur before the device starts to delete all the user information and application data • require the device to return to its factory default settings when it receives this command • specify whether to permit the user to stop permanently deleting data from the device and making the device unavailable during the delay period <p>You can send this command to a device that you want to distribute to another user in your organization, or to a device that is lost and that the user might not recover.</p>

IT administration command	Description
	You can also specify whether you want to delete or disable a user account from the BlackBerry Enterprise Server after the device deletes all user information and application data.

BlackBerry Enterprise Server high availability

7

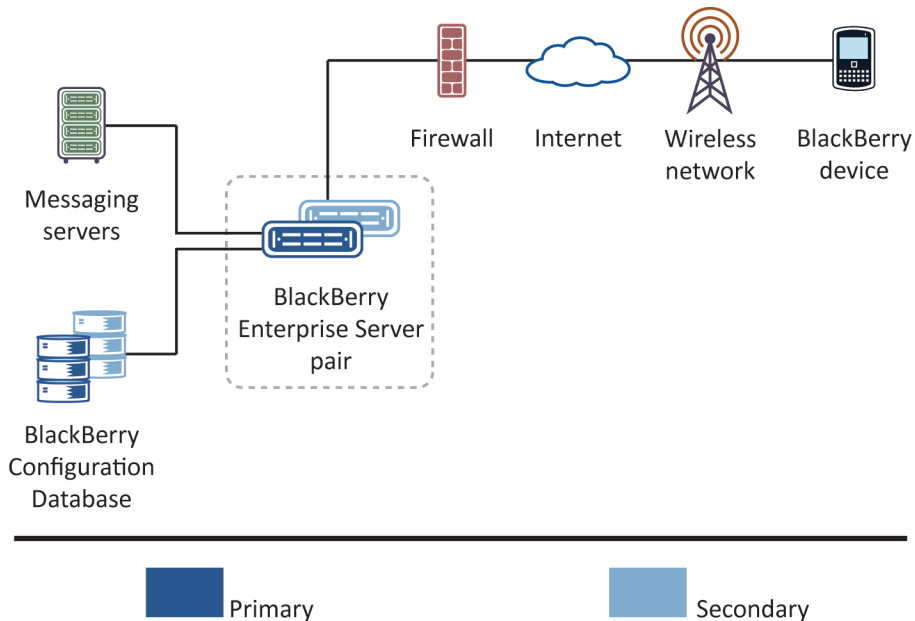
High availability permits you to provide minimum downtime for BlackBerry services if BlackBerry Enterprise Server components stop responding or if they require maintenance. BlackBerry Enterprise Server high availability consists of a minimum of two BlackBerry Enterprise Server instances and the BlackBerry Configuration Database which is replicated across two database servers. High availability is designed so that no single point of failure exists in the BlackBerry Enterprise Solution that could break the messaging data flow and application data flow to and from BlackBerry devices.

When you configure the BlackBerry Enterprise Server for high availability, you install a primary BlackBerry Enterprise Server and a standby BlackBerry Enterprise Server on different computers within the same network segment. These BlackBerry Enterprise Server instances create a BlackBerry Enterprise Server pair. Both BlackBerry Enterprise Server instances use the same SRP credentials and BlackBerry Configuration Database. You can configure an automatic failover process or a manual failover process.

The standby BlackBerry Enterprise Server connects to the primary BlackBerry Enterprise Server and checks periodically that the primary BlackBerry Enterprise Server is healthy. The health of a BlackBerry Enterprise Server is determined by thresholds that you can configure. If the health of the primary BlackBerry Enterprise Server falls below the failover threshold or if the primary BlackBerry Enterprise Server stops responding, the standby BlackBerry Enterprise Server tries to promote itself. If the messaging server and the BlackBerry Configuration Database remain available during the failover process, the message delays that device users might experience are similar to the delays that users experience when you start a BlackBerry Enterprise Server instance.

BlackBerry Enterprise Server high availability in a small-scale environment

The following diagram shows how you can configure a BlackBerry Enterprise Server for high availability in a small-scale environment. Each primary BlackBerry Enterprise Server instance requires its own standby BlackBerry Enterprise Server instance. You install the primary BlackBerry Enterprise Server and standby BlackBerry Enterprise Server on different computers. You can install all BlackBerry Enterprise Server components on both computers to minimize the number of computers that the BlackBerry Enterprise Server environment requires.



Both BlackBerry Enterprise Server instances in the BlackBerry Enterprise Server pair include, by default, the BlackBerry Attachment Service, BlackBerry Dispatcher, BlackBerry MDS Connection Service, BlackBerry Messaging Agent, BlackBerry Policy Service, BlackBerry Router, and BlackBerry Synchronization Service. By default, if you choose to install the BlackBerry Collaboration Service with both instances, the BlackBerry Collaboration Service is included in the BlackBerry Enterprise Server pair.

To administer the BlackBerry Enterprise Server pair, you can install the BlackBerry Administration Service with both BlackBerry Enterprise Server instances and configure high availability for the BlackBerry Administration Service separately.

In a large-scale environment, you can add any number of BlackBerry Enterprise Server pairs that use the same BlackBerry Configuration Database.

How the BlackBerry Enterprise Server calculates health scores

Certain BlackBerry Enterprise Server components calculate a health score that indicates how well the component can provide specific services. The components send their health scores to the BlackBerry Dispatcher, which combines the health scores of the components to calculate the overall health score of the BlackBerry Enterprise Server. The BlackBerry Dispatcher writes the information to the BlackBerry Configuration Database, and it provides the information to a BlackBerry Enterprise Server that requests it.

The BlackBerry Enterprise Server components calculate their health scores by examining their operating health, the stability of their connections to other components, and the health scores of the other components.

The health score of the BlackBerry Enterprise Server consists of various health parameters. Each health parameter indicates whether a particular service or feature is available. If you turn on the automatic failover feature for the BlackBerry Enterprise Server, you can configure health parameters so that the BlackBerry Enterprise Server fails over automatically when critical services or features are no longer available.

Conditions for failover to a standby BlackBerry Enterprise Server

Failover between the primary and standby BlackBerry Enterprise Server instances occurs when the standby BlackBerry Enterprise Server determines that its health score is above the promotion threshold and one or more of the following events occurred:

- The standby BlackBerry Enterprise Server receives a health score from the primary BlackBerry Enterprise Server that is below the failover threshold.
- The standby BlackBerry Enterprise Server reads, in the BlackBerry Configuration Database, a health score for the primary BlackBerry Enterprise Server that is below the failover threshold.
- The standby BlackBerry Enterprise Server does not receive a response when it checks the BlackBerry Dispatcher for the health score of the primary BlackBerry Enterprise Server.
- The standby BlackBerry Enterprise Server pings the BlackBerry Dispatcher on the network but cannot determine whether the primary BlackBerry Enterprise Server is running.

How a primary BlackBerry Enterprise Server self-demotes

After the primary BlackBerry Enterprise Server receives a request from a standby BlackBerry Enterprise Server to self-demote, the primary BlackBerry Enterprise Server performs the following actions:

- closes its SRP connection to the BlackBerry Infrastructure
- stops the flow of all messages
- stops the Novell GroupWise SOAP connector if your organization's environment includes the BlackBerry Enterprise Server for Novell GroupWise
- demotes its connections to the messaging server and BlackBerry Configuration Database to standby connections

- informs the standby BlackBerry Enterprise Server that it self-demoted

Scenario: What happens after a primary BlackBerry Enterprise Server stops responding

If a primary BlackBerry Enterprise Server stops responding, the standby BlackBerry Enterprise Server performs one of two actions depending on whether its health score is above or below the promotion threshold.

The standby BlackBerry Enterprise Server can perform the following actions if the messaging server, BlackBerry Infrastructure, and BlackBerry Configuration Database are available.

Action that the standby BlackBerry Enterprise Server performs when its health score is above the promotion threshold

1. The standby BlackBerry Enterprise Server determines that the primary BlackBerry Enterprise Server stopped responding.
2. The standby BlackBerry Enterprise Server checks its own health score and determines that the health score is above the promotion threshold.
3. The standby BlackBerry Enterprise Server opens active connections to the BlackBerry Configuration Database and messaging server.
4. If your organization's environment includes the BlackBerry Enterprise Server for Novell GroupWise, the standby BlackBerry Enterprise Server starts the GroupWise SOAP connector.
5. The standby BlackBerry Enterprise Server tries to open an SRP connection to the BlackBerry Infrastructure.
6. When the connection to the BlackBerry Infrastructure is stable, the standby BlackBerry Enterprise Server writes its identity as the primary BlackBerry Enterprise Server to the BlackBerry Configuration Database.

Action that the standby BlackBerry Enterprise Server performs when its health score is below the promotion threshold

1. The standby BlackBerry Enterprise Server determines that the primary BlackBerry Enterprise Server stopped responding.
2. The standby BlackBerry Enterprise Server checks its own health score and determines that the health score is below the promotion threshold.

The standby BlackBerry Enterprise Server cannot become the primary instance. You must resolve any issues before the standby BlackBerry Enterprise Server can recover.

Scenario: What happens after the health score of a primary BlackBerry Enterprise Server falls below the failover threshold

The following scenario can occur if the messaging server, BlackBerry Infrastructure, and BlackBerry Configuration Database are available.

1. The standby BlackBerry Enterprise Server determines that the health score of the primary BlackBerry Enterprise Server fell below the failover threshold.
2. The standby BlackBerry Enterprise Server checks its own health score and determines that its health score is above the promotion threshold and higher than the health score of the primary BlackBerry Enterprise Server.
3. The standby BlackBerry Enterprise Server sends a demotion request to the primary BlackBerry Enterprise Server.
4. The primary BlackBerry Enterprise Server self-demotes.
5. If your organization's environment includes the BlackBerry Enterprise Server for Novell GroupWise, the primary BlackBerry Enterprise Server stops the Novell GroupWise SOAP connector.
6. The standby BlackBerry Enterprise Server opens active connections to the BlackBerry Configuration Database and messaging server.
7. If your organization's environment includes the BlackBerry Enterprise Server for Novell GroupWise, the standby BlackBerry Enterprise Server starts the GroupWise SOAP connector.
8. The standby BlackBerry Enterprise Server tries to open an SRP connection to the BlackBerry Infrastructure.
9. The standby BlackBerry Enterprise Server writes its identity as the primary BlackBerry Enterprise Server to the BlackBerry Configuration Database.

BlackBerry Configuration Database high availability

The type of BlackBerry Configuration Database high availability that you can configure depends on the type of database server that is in your organization's environment.

If your organization's environment includes Microsoft SQL Server 2005 SP2 or later, you can configure database mirroring. Database mirroring requires a principal database, a mirror database, and a witness. Although the BlackBerry Enterprise Server can contact the mirror database, it opens active connections to the principal database only. If the principal

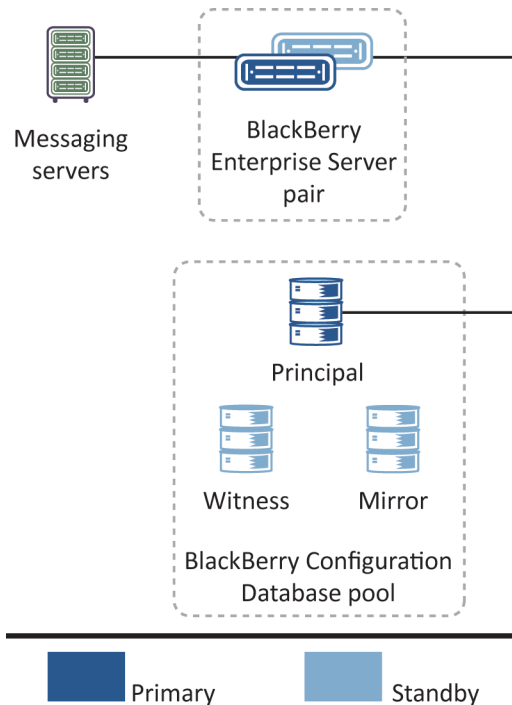
database stops responding, the BlackBerry Enterprise Server opens an active connection to the mirror database automatically. Database mirroring provides fault tolerance for the BlackBerry Enterprise Solution.

If your organization's environment includes a version of Microsoft SQL Server that is earlier than version 2005 SP2, you can configure transactional replication of the BlackBerry Configuration Database and create a replicated BlackBerry Configuration Database. If the BlackBerry Configuration Database stops responding, you must fail over the BlackBerry Enterprise Server to the replicated BlackBerry Configuration Database manually.

For more information about database mirroring, visit www.microsoft.com.

BlackBerry Configuration Database mirroring

The following diagram shows how you can configure the BlackBerry Configuration Database with principal and mirror instances and a witness for high availability. The BlackBerry Enterprise Server connects to the principal BlackBerry Configuration Database directly, and can fail over to the mirror BlackBerry Configuration Database if the principal BlackBerry Configuration Database stops responding.



The primary BlackBerry Enterprise Server connects to the principal BlackBerry Configuration Database and accesses data from it. The name of the mirror BlackBerry Configuration Database is stored in the Windows registry of the computers that hosts the primary and standby BlackBerry Enterprise Server instances. The BlackBerry Enterprise Server instances do not connect to the mirror BlackBerry Configuration Database until after the principal BlackBerry Configuration Database stops responding.

The primary BlackBerry Enterprise Server connects to the messaging server and processes the messaging data that it sends to and receives from BlackBerry devices.

The standby BlackBerry Enterprise Server opens standby connections to the principal BlackBerry Configuration Database and the messaging server.

Scenario: What happens after the principal BlackBerry Configuration Database stops responding

If a principal BlackBerry Configuration Database stops responding, the response of the primary BlackBerry Enterprise Server depends on whether it can connect to the mirror BlackBerry Configuration Database.

The following responses assume that the messaging server and BlackBerry Infrastructure are available.

Response of a primary BlackBerry Enterprise Server that can connect to the mirror BlackBerry Configuration Database

1. The primary BlackBerry Enterprise Server loses its connection to the principal BlackBerry Configuration Database.
2. The primary BlackBerry Enterprise Server connects to the mirror BlackBerry Configuration Database.
3. The primary BlackBerry Enterprise Server remains the primary instance.

Response of a primary BlackBerry Enterprise Server that cannot connect to the mirror BlackBerry Configuration Database

1. The primary BlackBerry Enterprise Server loses its connection to the principal BlackBerry Configuration Database.
2. The primary BlackBerry Enterprise Server tries to connect to the mirror BlackBerry Configuration Database, but is unsuccessful.
3. The primary BlackBerry Enterprise Server lowers its health score and continues to provide limited services.

One of the following events occurs:

- If the standby BlackBerry Enterprise Server can open a connection to the principal or mirror BlackBerry Configuration Database, it demotes the primary BlackBerry Enterprise Server and promotes itself to become the primary instance.
- If the standby BlackBerry Enterprise Server cannot open a connection to the principal or mirror BlackBerry Configuration Database, it cannot promote itself. You must resolve any issues before the BlackBerry Enterprise Server pair can recover.

High availability in a distributed environment

If you install multiple BlackBerry Enterprise Server components on different computers to create a distributed environment, you can configure the components for high availability. High availability for a distributed component requires that you install two or more instances of the component in your organization's environment. When an instance stops responding, the other instances can take over.

When you install multiple BlackBerry Enterprise Server components in a distributed environment, each BlackBerry Enterprise Server component implements high availability differently.

Component	High availability type	Description
BlackBerry Administration Service	load balancing using DNS round robin, or a hardware load balancer	When you install two or more BlackBerry Administration Service instances, you can create a BlackBerry Administration Service pool. You can access the BlackBerry Administration Service instances using a single web address. The load is distributed across the instances. If a BlackBerry Administration Service instance stops responding, the pool routes requests to the available instances.
BlackBerry Attachment Service	load-balancing with primary and secondary groups	When you install two or more BlackBerry Attachment Service instances, you can create a BlackBerry Attachment Service pool for each BlackBerry Enterprise Server instance. You can configure a pool with a primary group of instances and, optionally, a secondary group of instances. The BlackBerry Enterprise Server sends all requests to the primary group. If the primary group cannot convert a specific file format, the BlackBerry Enterprise Server forwards conversion requests for the specific file format to the secondary group.
BlackBerry Collaboration Service	failover with an active connection to one instance and standby connections to other instances	When you install two or more BlackBerry Collaboration Service instances, you can create a BlackBerry Collaboration Service pool for each BlackBerry Enterprise Server instance. Each BlackBerry Enterprise Server assigns one of the connections to the BlackBerry Collaboration Service instances as the active connection, and the other connections as standby connections. If the BlackBerry Collaboration Service that the active connection is assigned to stops responding, the BlackBerry Enterprise Server

Component	High availability type	Description
BlackBerry Configuration Database	database mirroring	assigns the active connection to another BlackBerry Collaboration Service instance. If you install the BlackBerry Configuration Database on Microsoft SQL Server 2005 SP2 or later, you can configure database mirroring. If the principal BlackBerry Configuration Database stops responding, the BlackBerry Enterprise Server fails over to the mirror BlackBerry Configuration Database.
BlackBerry MDS Connection Service	failover with an active connection to one instance and standby connections to other instances	When you install two or more BlackBerry MDS Connection Service instances, you can create a BlackBerry MDS Connection Service pool for each BlackBerry Enterprise Server instance. Each BlackBerry Enterprise Server assigns one of the connections to the BlackBerry MDS Connection Service instances as the active connection, and the other connections as standby connections. If the BlackBerry MDS Connection Service that the active connection is assigned to stops responding, the BlackBerry Enterprise Server assigns the active connection to another BlackBerry MDS Connection Service instance.
BlackBerry Router	failover	When you install two or more BlackBerry Router instances, you can create a BlackBerry Router pool for each BlackBerry Enterprise Server or BlackBerry Enterprise Server pair. If a BlackBerry Router stops responding, the BlackBerry Enterprise Server selects another instance using information that is stored in the BlackBerry Configuration Database.

Wi-Fi enabled devices

8

Wi-Fi enabled BlackBerry devices permit users with qualifying data plans to access BlackBerry services over a mobile network, Wi-Fi network, or both networks simultaneously.

When users can access a mobile network and Wi-Fi network simultaneously, users can perform multiple tasks over both networks. For example, a user with a BlackBerry 8820 smartphone can send messages over a Wi-Fi network and can make a call over the mobile network at the same time.

If users' mobile network providers make UMA technology (GAN technology) available, and users have subscribed to the UMA feature, Wi-Fi enabled devices can access the mobile network providers' voice services and data services over a mobile network or a Wi-Fi network.

Wi-Fi enabled devices can open a Wi-Fi connection from an enterprise Wi-Fi network or, with a VPN session, from a home Wi-Fi network or Wi-Fi hotspot to connect directly to the BlackBerry Router.

Wi-Fi enabled devices are designed to open a connection to the BlackBerry Internet Service to access the BlackBerry MDS Connection Service, BlackBerry Messenger, and other devices for PIN messaging. You can verify with your organization's wireless service provider whether your organization's service plan provides access to these services over a Wi-Fi network.

Types of Wi-Fi networks

Wi-Fi enabled BlackBerry devices can access BlackBerry services using enterprise Wi-Fi networks, home Wi-Fi networks, or hotspots.

Type	Description
Enterprise Wi-Fi networks	<p>An enterprise Wi-Fi network has multiple wireless access points to provide ubiquitous coverage, hotspot coverage, or ubiquitous and hotspot coverage. You can use a Wi-Fi enabled BlackBerry device in any coverage area.</p> <p>You can configure an enterprise Wi-Fi network to require layer 2 authentication. An organization might consider an enterprise Wi-Fi network to be untrusted and require that all Wi-Fi connections to the organization's network occur through a VPN concentrator. You must configure Wi-Fi enabled BlackBerry devices to support the authentication type that your organization uses.</p> <p>An enterprise Wi-Fi network permits optimized access to the BlackBerry Enterprise Server over a direct IP connection to the BlackBerry Router.</p>
Home Wi-Fi networks	<p>A home Wi-Fi network uses a single access point to provide Internet access through a broadband gateway. The broadband gateway can implement NAT and</p>

Type	Description
	<p>permit VPN connections through the firewall. You can configure a home Wi-Fi network with layer 2 security and password authentication. You must configure BlackBerry devices to support the authentication that the home Wi-Fi network requires.</p> <p>A home Wi-Fi network permits users to access all BlackBerry services from Wi-Fi enabled BlackBerry devices using the BlackBerry Infrastructure.</p>
Hotspots	<p>A hotspot offered by an ISP, a mobile network provider, or a property owner can provide a Wi-Fi connection in public and semipublic areas. The network can be an open network without layer 2 security and use a captive portal for authentication. The captive portal blocks all network traffic except traffic that uses HTTP and it redirects HTTP requests to a login page.</p> <p>After a user logs in to the hotspot, the captive portal permits the user to access wireless network services.</p> <p>Hotspots can use a firewall and they can permit VPN connections. A hotspot permits users to access all BlackBerry services from their Wi-Fi enabled BlackBerry devices using the BlackBerry Infrastructure.</p>

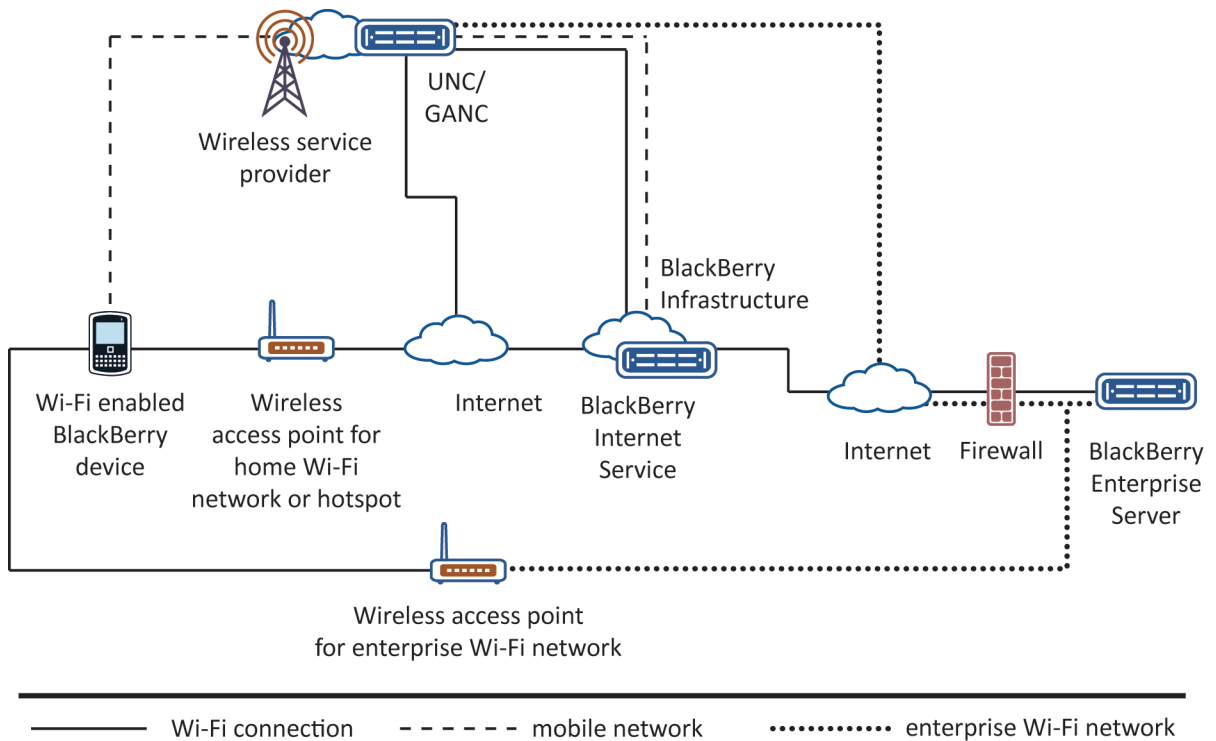
Wireless access points

Wi-Fi enabled BlackBerry devices use wireless access points to connect to the Wi-Fi network. An access point must conform to the IEEE 802.11a, IEEE 802.11b, or IEEE 802.11g wireless networking standard.

Type	Description
thin access point	<p>A thin access point (or controller-based access point) is part of an enterprise Wi-Fi network that you can manage from a central location. This type of access point requires an external controller to manage network traffic. You can administer one or more thin access points through the controller.</p> <p>Thin access points with an external controller can provide a more seamless roaming experience for users with Wi-Fi enabled BlackBerry devices during data and voice sessions.</p>
thick access point	<p>A thick access point (or intelligent or autonomous access point), has the intelligence to operate as a standalone component without a controller.</p>

Connections that BlackBerry devices make to mobile and Wi-Fi networks

Wi-Fi enabled BlackBerry devices connect to different components in the mobile and Wi-Fi networks so that they can communicate with the BlackBerry Enterprise Server and provide BlackBerry services for users.



Component	Description
BlackBerry Enterprise Server	The BlackBerry Enterprise Server provides productivity tools and data from an organization's applications to BlackBerry devices over the wireless network, and processes, routes, compresses, and encrypts data.
BlackBerry Infrastructure	The BlackBerry Infrastructure is designed to communicate with the BlackBerry Enterprise Server using a RIM proprietary protocol SRP.

Component	Description
BlackBerry Internet Service	The BlackBerry Internet Service is an email and Internet service for BlackBerry devices that is designed to provide subscribers with automatic delivery of email messages, mobile access to email message attachments, and convenient access to Internet content.
UNC/GANC	The UNC/GANC is the gateway for Wi-Fi or mobile communications. The UNC/GANC exists in your organization's gateway only if the wireless service provider supports UMA.
wireless access point for a home Wi-Fi network or hotspot	An access point for a home Wi-Fi network or hotspot permits the BlackBerry device to connect to a home Wi-Fi network or hotspot.
wireless access point for an enterprise Wi-Fi network	An access point for an enterprise Wi-Fi network permits a BlackBerry device to connect to an enterprise Wi-Fi network using strong authentication and link layer security.
wireless service provider	A wireless service provider is a telephone company that provides services for BlackBerry devices.
Wi-Fi enabled BlackBerry device	A Wi-Fi enabled BlackBerry device permits a user to access voice and data services across multiple radio technologies.

Connecting Wi-Fi enabled BlackBerry devices to the BlackBerry Enterprise Server over a Wi-Fi connection

Direct connections between BlackBerry devices and the BlackBerry Router over an enterprise Wi-Fi network

Wi-Fi enabled BlackBerry devices can open a direct connection to the BlackBerry Router over an enterprise Wi-Fi network after you configured a Wi-Fi profile for the user accounts. You can use direct connections to the BlackBerry Router when Wi-Fi enabled BlackBerry devices are located in your organization's existing Wi-Fi environment. When BlackBerry devices connect to the BlackBerry Router, they can bypass SRP connectivity and authentication to connect to the BlackBerry Enterprise Server directly.

After BlackBerry devices connect to the Wi-Fi network using a Wi-Fi profile, the BlackBerry devices try to make a direct IP connection to the BlackBerry Router. With some network architectures, a VPN session might be required to complete the direct connection to the BlackBerry Router.

Wi-Fi enabled BlackBerry devices include a built-in VPN client that you can configure and assign to any Wi-Fi profile on the BlackBerry devices. If a direct connection to the BlackBerry Router is possible (with or without a VPN session), the BlackBerry Enterprise Server starts sending data.

Wi-Fi connection when a VPN connection or direct connection between BlackBerry devices and the BlackBerry Router is not possible

If Wi-Fi enabled BlackBerry devices cannot connect directly to the BlackBerry Router (with or without a VPN connection) over a Wi-Fi network that can access the Internet (for example, a home Wi-Fi network or hotspot), the Wi-Fi enabled BlackBerry devices open SSL connections over the Internet to the BlackBerry Infrastructure. After the Wi-Fi enabled BlackBerry devices connect to the BlackBerry Infrastructure, the users' provisioned data services start to send data to the Wi-Fi enabled BlackBerry devices.

Priority for connections that BlackBerry devices make over a Wi-Fi network

Wi-Fi enabled BlackBerry devices connect over a Wi-Fi network to the BlackBerry Router or BlackBerry Infrastructure using the best possible connection or combination of available connections in the following order:

- connection to the BlackBerry Enterprise Server or BlackBerry MDS Connection Service over a serial, USB, or Bluetooth connection that uses the BlackBerry Device Manager
- connection to the BlackBerry Router from a Wi-Fi network, with or without a VPN connection
- SSL connection through the Internet to the BlackBerry Infrastructure over a Wi-Fi network
- connection to the BlackBerry Infrastructure provided by a wireless service provider that uses the GSM network, EDGE network, or UMA

The order of connections assumes that all routes to the BlackBerry Router and Internet are available when the Wi-Fi enabled BlackBerry devices connect to the Wi-Fi network.

BlackBerry services that are available over Wi-Fi connections

For more information about supported services and features, contact your organization's wireless service provider. Not all BlackBerry data plans support Wi-Fi access to BlackBerry data services.

When you configure a Wi-Fi network to open a connection (with or without a VPN connection) to the BlackBerry Router, you can keep all data transfers entirely within the enterprise Wi-Fi network and reduce the routing required.

BlackBerry services	Service provider with GSM/EDGE network or UMA network	Wi-Fi network and service provider with GSM/EDGE network	Wi-Fi network and no service provider with GSM/EDGE network or UMA, and no UMA available	Enterprise Wi-Fi network and service provider with GSM/EDGE network, and no UMA, and no UMA available	Enterprise Wi-Fi network and no service provider with GSM/EDGE network, and no UMA available
services from the BlackBerry Enterprise Server (for example, messaging, organizer data synchronization)	X	X	X	X	X
services from the BlackBerry Internet Service (for example, messaging, browsing)	X	X	X	X	X
services from the BlackBerry MDS Connection Service (for example, application push, application access, browsing)	X	X	X	X	X

BlackBerry services	Service provider with GSM/EDGE network or UMA network	Wi-Fi network and service provider with GSM/EDGE network	Wi-Fi network and no service provider with GSM/EDGE network or UMA, and no UMA available	Enterprise Wi-Fi network and service provider with GSM/EDGE network, and no UMA, and no UMA available	Enterprise Wi-Fi network and no service provider with GSM/EDGE network, and no UMA available
BlackBerry Messenger	X	X	X	X	X
PIN messaging	X	X	X	X	X
instant messaging using a collaboration client (for example, Microsoft Office Live Communications Server)	X	X	X	X	X
instant messaging using a third-party instant messaging application (for example, Windows Messenger)	X	X	X	X	X
BlackBerry Maps	X	X	X	X	X
service provider messaging (for example, SMS)	X	X		X	
content downloading provided by a wireless service provider (for example, ring tones)	X	X		X	
web browsing provided by a	X	X		X	

BlackBerry services	Service provider with GSM/EDGE network or UMA network	Wi-Fi network and service provider with GSM/EDGE network	Wi-Fi network and no service provider with GSM/EDGE network or UMA, and no UMA available	Enterprise Wi-Fi network and service provider with GSM/EDGE network, and no UMA, and no UMA available	Enterprise Wi-Fi network and no service provider with GSM/EDGE network, and no UMA available
wireless service provider (for example, WAP)					
voice plan provided by a wireless service provider	X	X		X	

IEEE 802.11 wireless networking standards that Wi-Fi enabled BlackBerry devices support

Wi-Fi enabled BlackBerry devices support the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g wireless networking standards.

Characteristics of the IEEE 802.11a wireless networking standard that Wi-Fi enabled BlackBerry devices support

Characteristic	Description
fallback speeds	48, 36, 24, 18, 12, 9, and 6 Mbps
frequency	5 GHz
maximum speed	54 Mbps

Characteristic	Description
nonoverlapping channels	up to 19
sources of interference	<ul style="list-style-type: none"> • Bluetooth wireless technology • some satellite systems • 5 GHz cordless phones
throughput speed	23 Mbps

Characteristics of the IEEE 802.11b wireless networking standard that Wi-Fi enabled BlackBerry devices support

Characteristic	Description
fallback speeds	5.5, 2, and 1 Mbps
frequency	2.4 GHz
maximum speed	11 Mbps
nonoverlapping channels	3
sources of interference	<ul style="list-style-type: none"> • Bluetooth wireless technology • microwave ovens • 2.4 GHz cordless phones
throughput speed	4.5 Mbps

Characteristics of the IEEE 802.11g wireless networking standard that Wi-Fi enabled BlackBerry devices support

Characteristic	Description
fallback speeds	48, 36, 24, 18, 12, 9, and 6 Mbps
frequency	2.4 GHz
maximum speed	54 Mbps
nonoverlapping channels	3
sources of interference	<ul style="list-style-type: none"> • Bluetooth wireless technology • microwave ovens • 2.4 GHz cordless phones
throughput speed	19 Mbps

Security features of a Wi-Fi enabled device

Feature	Description
Activation of BlackBerry devices over an enterprise Wi-Fi network	Activation of devices over an enterprise Wi-Fi network is designed to simplify the actions of activating or updating devices.
Authenticated connection with BlackBerry Router	<p>An authenticated connection with a BlackBerry Router permits devices to open a direct connection to the BlackBerry Enterprise Server after they authenticate with the BlackBerry Router.</p> <p>Devices connected to an enterprise Wi-Fi network do not use an SRP connection to send data to the BlackBerry Enterprise Server.</p>
BlackBerry transport layer encryption	BlackBerry transport layer encryption is designed to encrypt messages that the device and the BlackBerry Enterprise Server send between each other after they open an authenticated connection.

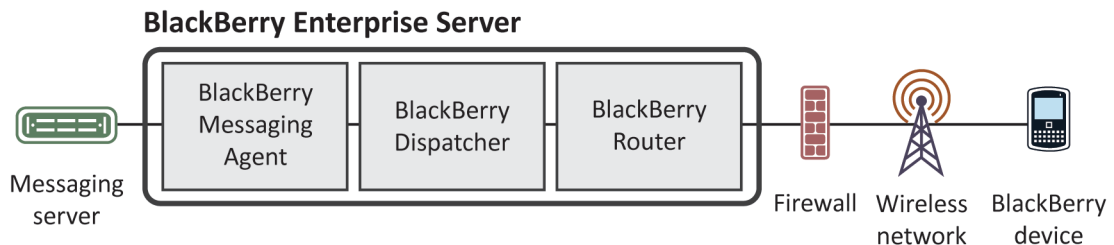
Feature	Description
Direct access to the BlackBerry Infrastructure over a Wi-Fi connection	<p>Direct access to the BlackBerry Infrastructure over a Wi-Fi connection permits Wi-Fi enabled devices to access BlackBerry services over the Internet, even if UMA is not available.</p> <p>You can verify with your organization's wireless service provider that your organization's service plan supports access to BlackBerry services over a Wi-Fi connection.</p>
Encrypted communication over the Wi-Fi network	Devices support multiple security methods that are designed to encrypt communication over the enterprise Wi-Fi network between the device and wireless access points or a network firewall on the enterprise Wi-Fi network.
Expanded groups of Wi-Fi and VPN configuration settings	Expanded groups of Wi-Fi and VPN configuration settings permit you to control Wi-Fi connections from devices.
Limited connections	Wi-Fi enabled devices are designed to reject incoming connections, to support limited connections in infrastructure mode only, and to prevent ad-hoc mode (also known as peer-to-peer) connections.
Multiple Wi-Fi and VPN profiles	Multiple Wi-Fi and VPN profiles are designed to address user requirements in a variety of different environments.
Proxy server	Devices supports the use of a transparent proxy server that you can configure between the enterprise Wi-Fi network and the device.
Software token provisioning	<p>Software token provisioning is designed to permit you to provision and manage the seed for software token authentication on devices. You can use software token authentication for VPN connections.</p> <p>The BlackBerry Enterprise Server is designed to work with the RSA Authentication Manager to provide software token support for use with layer 2 and layer 3 authentication on supported devices.</p>
User-specific configuration settings and IT policy rules	User-specific configuration settings and IT policy rules are designed to simplify the configuration of user-specific Wi-Fi and VPN information (such as user IDs and passwords).
Wireless backup of Wi-Fi and VPN profiles	Backup of Wi-Fi and VPN profiles on devices over a Wi-Fi connection permits users to restore the profiles, if necessary.

BlackBerry Enterprise Server process flows

9

Messaging process flows

Process flow: Sending a message to a BlackBerry device



1. A message arrives in a user's mailbox. Microsoft Exchange notifies the BlackBerry Messaging Agent.
2. The BlackBerry Messaging Agent applies global filter rules to the messages in the user's mailbox and filters the messages that match the filter criteria.
If global filter rules do not apply, the BlackBerry Messaging Agent applies filter rules that the user specified to the messages in the user's mailbox.
3. The BlackBerry Messaging Agent sends the first 2 KB of the message (plain text, or in an HTML message, the equivalent to 2 KB of plain text) to the BlackBerry Dispatcher.
4. The BlackBerry Dispatcher compresses the first 2 KB of the message, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted data to the BlackBerry Router.
5. The BlackBerry Router sends the encrypted data to the wireless network over port 3101, or over port 4101 if the BlackBerry device is a Wi-Fi enabled BlackBerry device that is connected to the enterprise Wi-Fi network.
6. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network, and sends the message data to the BlackBerry device.

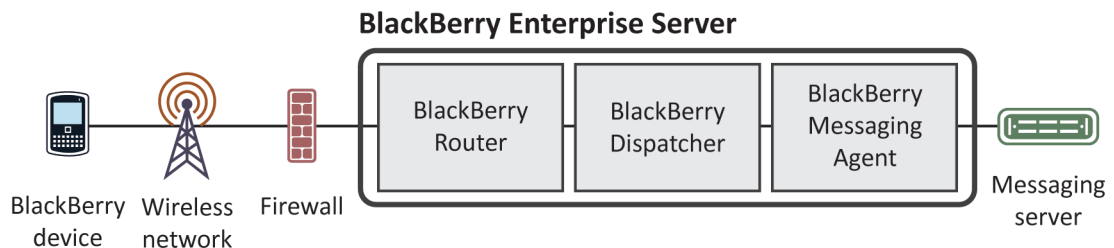
- The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher. The BlackBerry Dispatcher sends the delivery confirmation to the BlackBerry Messaging Agent.

If the BlackBerry Messaging Agent does not receive a delivery confirmation within four hours, it sends the message to the wireless network again.

The delivery confirmation verifies that the wireless network delivered the message to the BlackBerry device, but it does not verify that the user received or opened the message.

- The BlackBerry device decrypts and decompresses the message so that the user can view it, and notifies the user that the message arrived.

Process flow: Sending a message from a BlackBerry device



This process flow applies to new messages, reconciled messages (messages that a user moved, deleted, or marked as read or unread), and wireless calendar entries.

- A user sends a message from a BlackBerry device.

The BlackBerry device assigns a RefId to the message. If the message is a meeting invitation or calendar entry, the BlackBerry device appends the calendar information to the message. The BlackBerry device compresses and encrypts the message, and sends the message to the wireless network over port 3101, or over port 4101 if the BlackBerry device is a Wi-Fi enabled BlackBerry device that is connected to the enterprise Wi-Fi network.

- The wireless network sends the message to the BlackBerry Enterprise Server.

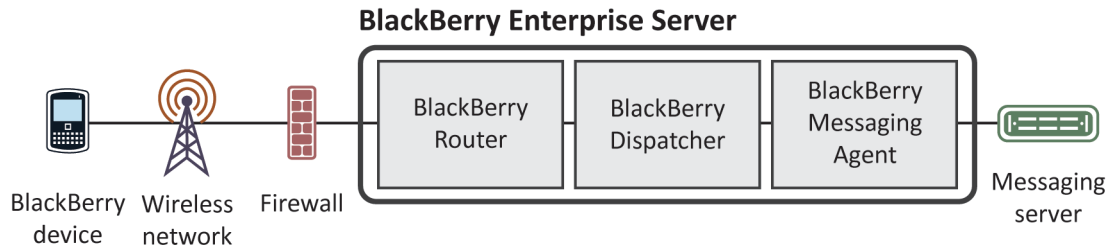
The BlackBerry Enterprise Server accepts only encrypted messages from the BlackBerry device.

- The BlackBerry Dispatcher uses the device transport key of the BlackBerry device to decrypt and decompress the message.

If the BlackBerry Dispatcher cannot decrypt the message using the device transport key, the BlackBerry Enterprise Server ignores the message and sends an error message to the BlackBerry device.

- The BlackBerry Messaging Agent sends the message to the user's email application.
- The BlackBerry Messaging Agent sends a copy of the message to the Sent Items view in the user's email application.
- The messaging server delivers the message to the recipients.

Process flow: Sending a message that contains an attachment from a BlackBerry device



1. A user attaches a file to a message on a BlackBerry device and sends the message.
 - If the BlackBerry device is not running BlackBerry Device Software version 4.2 or later, and if the BlackBerry device does not have a CMIME service book that indicates that the BlackBerry Enterprise Server supports attachment uploads, the Add Attachment menu item does not appear on the BlackBerry device.
 - If the user tries to attach a file that exceeds the maximum file size that you specified, a notification appears and the user cannot attach the file.
2. The BlackBerry device compresses and encrypts the message, and sends the message to the wireless network over port 3101.
The BlackBerry device formats the header of the message to indicate that a large attachment is part of the message. The BlackBerry device does not send the attachment content.
3. The wireless network sends the message to the BlackBerry Enterprise Server.
4. The BlackBerry Dispatcher decrypts and decompresses the message using the device transport key of the BlackBerry device.
If the BlackBerry Dispatcher cannot decrypt the message using the device transport key, the BlackBerry Enterprise Server ignores the message and sends an error message to the BlackBerry device.
5. The BlackBerry Messaging Agent stores the message properties in the user's mailbox.
The BlackBerry Messaging Agent sends a request for the attachment content through the BlackBerry Dispatcher to the BlackBerry device.
6. The BlackBerry device sends the attachment content through the BlackBerry Dispatcher to the BlackBerry Messaging Agent.
If the file size of the attachment content exceeds a single data packet, the BlackBerry device divides the content into multiple data packets and sends the data packets to the BlackBerry Messaging Agent.

- The BlackBerry Messaging Agent verifies the validity of the attachment content, and stores the content in memory as the content arrives.

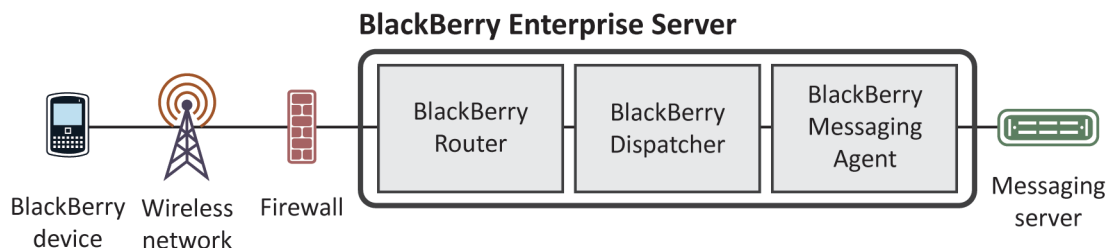
During the delivery of the attachment content, if the BlackBerry Messaging Agent does not receive content from the BlackBerry device for 15 minutes, the BlackBerry Messaging Agent cancels the message, deletes the partial attachment content from temporary storage, and sends an error message to the BlackBerry device.

After all of the attachment content arrives, the BlackBerry Messaging Agent checks for other attachments that might be part of the same message.

- If other attachments exist, the BlackBerry Messaging Agent requests the attachment content.
- If no additional attachments exist, the BlackBerry Messaging Agent finishes processing the message and sends the message to the user's email application.

The messaging server delivers the message to the intended recipients.

Process flow: Searching an organization's address book from a BlackBerry device



- A user searches for a contact on a BlackBerry device.
- The BlackBerry device assigns a RefId to the search request, compresses and encrypts the request, and sends the request to the BlackBerry Enterprise Server over port 3101.
- The BlackBerry Dispatcher decrypts and decompresses the request using the device transport key of the BlackBerry device, and sends the request to the BlackBerry Messaging Agent.
- The BlackBerry Messaging Agent searches the GAL on the Microsoft Exchange server and retrieves the 20 closest matches for the contact lookup request.

The BlackBerry Messaging Agent sends the contact lookup results to the BlackBerry Dispatcher.

- The BlackBerry Dispatcher encrypts the results using the device transport key of the BlackBerry device, compresses the encrypted data, and sends it to the BlackBerry Router for delivery to the BlackBerry device.
- The BlackBerry Router sends the encrypted data to the wireless network over port 3101.
- The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network, and sends the encrypted data to the BlackBerry device.

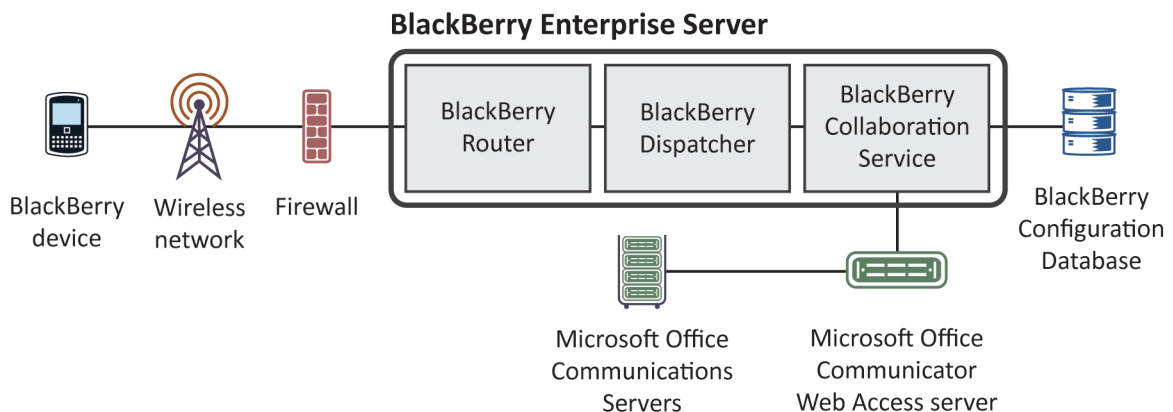
- The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher, which sends it to the BlackBerry Messaging Agent.

If the BlackBerry Enterprise Server does not receive a delivery confirmation within four hours, it resubmits the contact lookup results to the wireless network.

- The BlackBerry device decrypts and decompresses the contact lookup results with the device transport key so that the user can view them on the BlackBerry device or add them to the contact list on the BlackBerry device.

Instant messaging process flows

Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Live Communications Server 2005 (Microsoft Office Communicator)



- A user logs in to a collaboration client on a BlackBerry device.
- The device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
- The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion proprietary protocol.

4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
 - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
 - If no idle sessions exist, the BlackBerry Collaboration Service sends a Server Busy status message to the 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 HTTP persistent connection supports, the BlackBerry Collaboration Service sends a Failed status message to the device and rejects the login request.

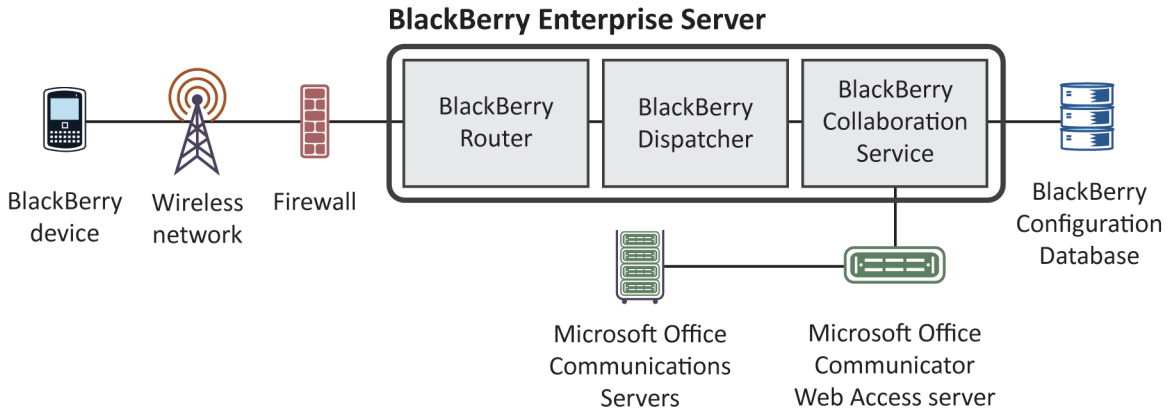
The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and tries to authenticate the user using Integrated Windows Authentication. If the authentication is not successful, the BlackBerry Collaboration Service tries a forms-based login process instead. The BlackBerry Collaboration Service sends a login request in JSON, a lightweight data-interchange format, to the Microsoft Office Communicator Web Access server.

The BlackBerry Collaboration Service opens the connection using HTTPS over port 443. You can also configure the connection to use HTTP, the transport protocol that the AJAX service uses, or a custom port number.

5. The Microsoft Office Communicator Web Access server formats the request using a Microsoft API and sends the request to the Microsoft Office Live Communications Server over an MTLS connection.
6. The Microsoft Office Live Communications Server accepts the request, processes the login information, and sends the acceptance to the Microsoft Office Communicator Web Access server.
7. The Microsoft Office Communicator Web Access server sends the acceptance to the BlackBerry Collaboration Service.
8. The BlackBerry Collaboration Service sends the acceptance message, in encrypted and compressed format, through the BlackBerry Dispatcher to the device, and creates a cache of the connectivity information to maintain the instant messaging session.

The BlackBerry Collaboration Service receives events that the server initiates from the Microsoft Office Communicator Web Access server using an HTTP GET or HTTPS GET request, and sends the events to the collaboration client over the session. The BlackBerry Collaboration Service sends events that the BlackBerry device initiates to the Microsoft Office Communicator Web Access server using an HTTP POST or HTTPS POST request.

Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Communications Server 2007



1. A user logs in to a collaboration client on a BlackBerry device.
2. The device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
 - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
 - If no idle sessions exist, the BlackBerry Collaboration Service sends a Server Busy status message to the 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 HTTP persistent connection supports, the BlackBerry Collaboration Service sends a Failed status message to the device and rejects the login request.

The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and tries to authenticate the user using Integrated Windows Authentication. If the authentication is not successful, the BlackBerry Collaboration Service tries a forms-based login process instead. The BlackBerry Collaboration Service sends a login request in XML format to the Microsoft Office Communicator Web Access server.

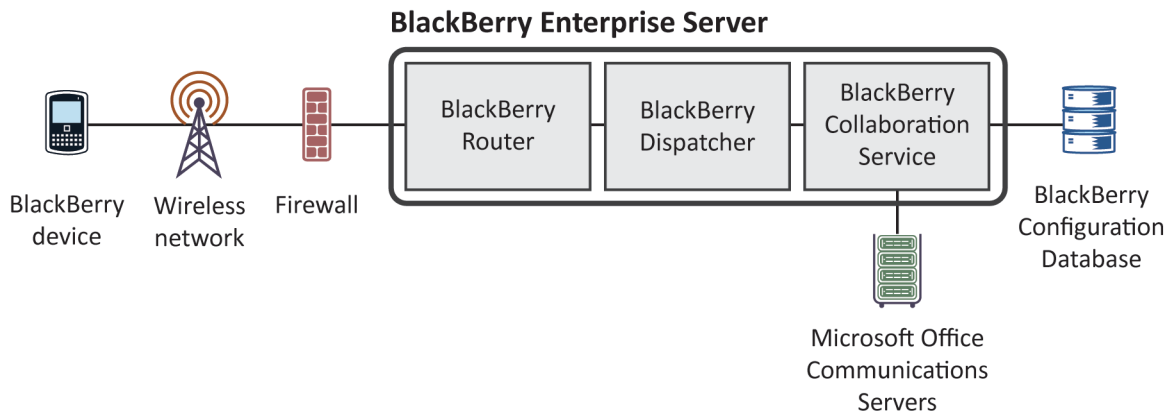
The BlackBerry Collaboration Service opens the connection using HTTPS over port 443. You can also configure the connection to use HTTP, the transport protocol that the AJAX service uses, or a custom port number.

5. The Microsoft Office Communicator Web Access server formats the request using a Microsoft API and sends the request to the Microsoft Office Communications Server 2007 over an MTLS connection.
6. The Microsoft Office Communications Server 2007 accepts the request, processes the login information, and sends the acceptance to the Microsoft Office Communicator Web Access server.

7. The Microsoft Office Communicator Web Access server sends the acceptance to the BlackBerry Collaboration Service.
8. The BlackBerry Collaboration Service sends the acceptance message, in encrypted and compressed format, through the BlackBerry Dispatcher to the device, and creates a cache of the connectivity information to maintain the instant messaging session.

The BlackBerry Collaboration Service receives events that the server initiates from the Microsoft Office Communicator Web Access server using an HTTP GET or HTTPS GET request, and sends the events to the collaboration client over the session. The BlackBerry Collaboration Service sends events that the device initiates to the Microsoft Office Communicator Web Access server using an HTTP POST or HTTPS POST request.

Process flow: Starting an instant messaging session using the BlackBerry Client for use with Microsoft Office Communications Server 2007 R2 or Microsoft Lync Server 2010



1. A BlackBerry device user logs in to a collaboration client on a BlackBerry device.
2. The device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions was reached, and performs one of the following actions:

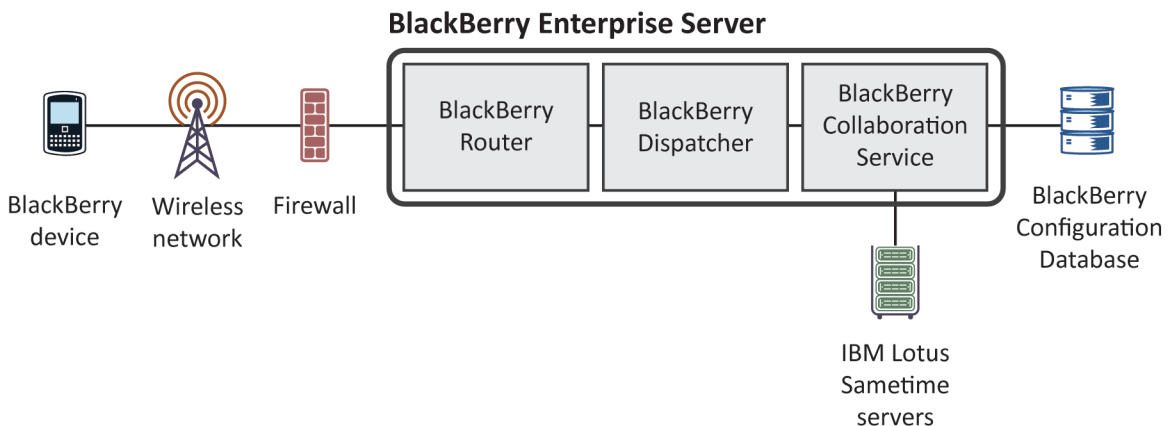
- If the maximum number of sessions was reached and you configured a timeout limit, the BlackBerry Collaboration Service logs out any instant messaging sessions on devices that are outside of a wireless coverage area, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
- If no idle sessions exist, the BlackBerry Collaboration Service sends a Server Busy status message to the device and rejects the login request.
- If you did not configure a maximum number of sessions and the number of sessions equals the total number that the HTTP persistent connection supports, the BlackBerry Collaboration Service sends a Failed status message to the device and rejects the login request.

The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and tries to authenticate the user using Integrated Windows authentication. The BlackBerry Collaboration Service sends a login request in SIP format to the Microsoft Communication server and, for Microsoft Office Communications Server 2007 R2, sends a login request to Microsoft Active Directory directly.

The BlackBerry Collaboration Service opens the connection using TLS over port 5061. You can also configure the connection to use TCP for Microsoft Office Communications Server 2007 R2.

5. The BlackBerry Collaboration Service formats the request using a Microsoft API and sends the request to the Microsoft Communication server over an MTLN connection.
6. The Microsoft Communications Server accepts the request, processes the login information, and sends the acceptance to the BlackBerry Collaboration Service.
7. The BlackBerry Collaboration Service sends the message that contains the acceptance through the BlackBerry Dispatcher to the device in encrypted and compressed format, and creates a cache of the connectivity information to maintain the instant messaging session.

Process flow: Starting an instant messaging session using the BlackBerry Client for IBM Sametime



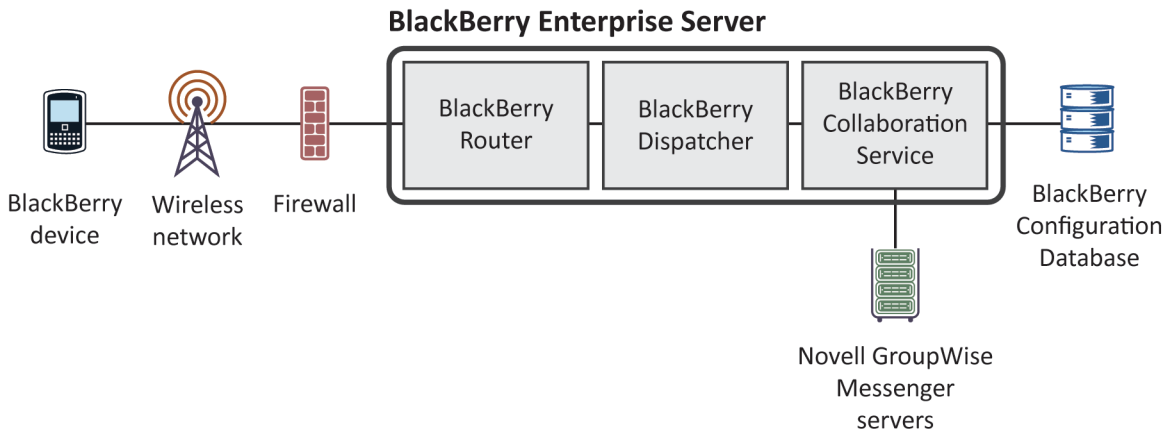
1. A user logs in to a collaboration client on a BlackBerry device.
2. The BlackBerry device compresses and encrypts the user ID and password, and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
 - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on BlackBerry devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
 - If no idle sessions exist, the BlackBerry Configuration Database sends a Server Busy 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 IBM Sametime API supports, the BlackBerry Configuration Database sends a Failed status message to the BlackBerry device and rejects the login request.

The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and connects to the IBM Sametime server. The BlackBerry Collaboration Service starts an encrypted proxy connection over TCP/IP using the IBM Sametime API, reformats the request from the RIM proprietary protocol format into one that the IBM Sametime API supports, and sends the request.

By default, the BlackBerry Collaboration Service starts the connection over port 1533 unless you specify a custom port number.

5. The IBM Sametime server accepts the login request from the BlackBerry device, starts a dedicated TCP/IP connection for the session, and listens for requests from the BlackBerry device for the session.
6. The BlackBerry Collaboration Service sends the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device, and creates a cache of the connectivity information to maintain the instant messaging session.

Process flow: Starting an instant messaging session using the BlackBerry Client for Novell GroupWise Messenger



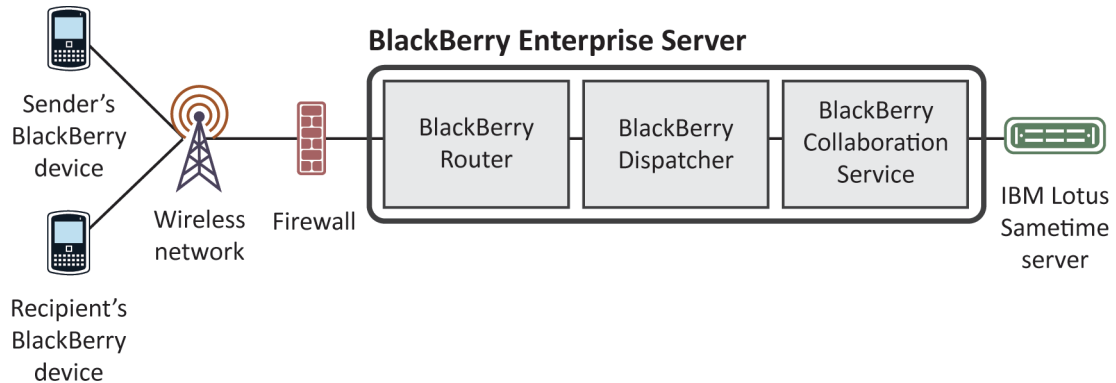
1. A user logs in to a collaboration client on a BlackBerry device.
2. The BlackBerry device compresses and encrypts the user ID and password and sends them through the BlackBerry Router to the BlackBerry Dispatcher over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry Collaboration Service over port 3200. If the BlackBerry Collaboration Service is located on a remote computer, the request remains encrypted using a Research In Motion proprietary protocol.
4. The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to find out if the maximum number of sessions has been reached, and performs one of the following actions:
 - If the maximum number of sessions has been reached and a timeout limit is set, the BlackBerry Collaboration Service logs out any instant messaging sessions on BlackBerry devices that are out of coverage, and any instant messaging sessions that are no longer sending status messages to the BlackBerry Collaboration Service.
 - If there are no idle sessions, the BlackBerry Configuration Database sends a Server Busy 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 Novell GroupWise protocol supports, the BlackBerry device sends a Failed (300) status message to the BlackBerry device and rejects the login request.

The BlackBerry Collaboration Service checks the BlackBerry Configuration Database to verify that the user has permission to use the collaboration client, and connects to the Novell GroupWise Messenger server.

The BlackBerry Collaboration Service starts an encrypted proxy (SSL) connection using the Novell GroupWise protocol and sends the request. By default, the BlackBerry Collaboration Service opens the connection over port 8300, but it can also open the connection over a custom port number.

5. The Novell GroupWise Messenger server accepts the login request from the BlackBerry device, opens a dedicated SSL connection for the session, and listens for requests from the BlackBerry device.
6. The BlackBerry Collaboration Service sends the acceptance, in encrypted and compressed format, through the BlackBerry Dispatcher to the BlackBerry device, and creates a cache of the connectivity information to maintain the instant messaging session.

Process flow: Sending a file to a contact using the BlackBerry Client for IBM Sametime



1. A user opens a conversation with a contact, clicks Send File on the menu, and selects a file to send to the contact.
2. The BlackBerry Client for IBM Sametime creates an invitation request and sends it to the BlackBerry Collaboration Service.
3. The BlackBerry Collaboration Service checks the size of the file to verify that it does not exceed the maximum file size that you configure on the BlackBerry Enterprise Server, associates the file extension and the conversation ID with the invitation request, and sends the request to the IBM Sametime server.
4. The IBM Sametime server checks the file size to verify that it does not exceed the maximum file size that you configured on the IBM Sametime server (by default, 1 MB), associates the file with the conversation that is open between the sender and recipient, and sends the request to the BlackBerry Collaboration Service.
5. The BlackBerry Collaboration Service converts the request into an instant messaging invitation and sends it to the client on the recipient's BlackBerry device.
6. In the conversation window on the recipient's client, the recipient receives a request to accept or decline the file. The recipient can also select an option to optimize the file for viewing on the BlackBerry device.

The BlackBerry Collaboration Service can optimize files for viewing on the BlackBerry device only if it has access to the BlackBerry Attachment Service in your organization's environment.

7. The recipient accepts the request.

If the recipient selected the optimize option, the file will be downloaded to the memory of the BlackBerry device. If the recipient did not select the optimize option, the client prompts the recipient to save the file to a location in the file system on the BlackBerry device.

8. The recipient's client sends a content request packet to the BlackBerry Collaboration Service.

9. The BlackBerry Collaboration Service requests the file size from the IBM Sametime server, and sends data to the IBM Sametime server to begin the file transfer process.

By default, the media transfer state on the BlackBerry Collaboration Service is set to transfer.

10. The sender's client sends the data for the file in content message packets to the BlackBerry Collaboration Service.
11. The BlackBerry Collaboration Service checks the order of the content message packets and sends them to the recipient's client using a BlackBerry instant messaging protocol.
12. The recipient's client receives the first content message packet, sends an acknowledgement message to the BlackBerry Collaboration Service, and requests the next content message packet from the BlackBerry Collaboration Service. This continues until the client receives all of the content message packets.

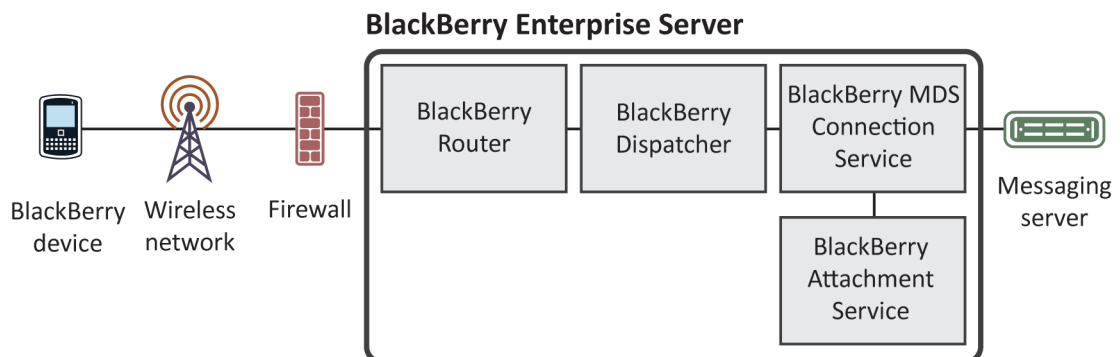
If the recipient selected the option to optimize the file for viewing, the BlackBerry Attachment Service converts the file into a format that is optimized for viewing on the BlackBerry device.

13. When the BlackBerry Collaboration Service receives an acknowledgement message for the last content message packet from the recipient's client, it changes its media transfer state to done and stops the file transfer process on the IBM Sametime server.
14. In the conversation window, the client notifies the recipient that the file has been received.

The recipient can open the file from the conversation window or from the file system on the BlackBerry device. The BlackBerry device uses the BlackBerry Browser to render supported files. If the recipient selected the option to optimize the file for viewing, the recipient can open and view supported files in the attachment viewer on the BlackBerry device. The recipient can also save the optimized file to a location in the file system on the BlackBerry device.

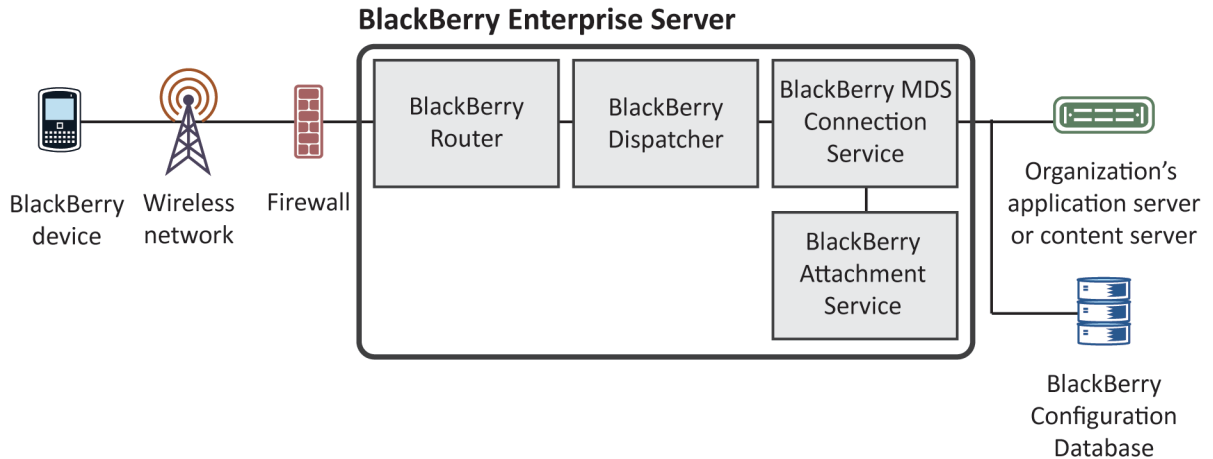
Message attachment process flows

Process flow: Viewing a message attachment



1. A user receives a message with an attachment on a BlackBerry device.
2. The BlackBerry Messaging Agent verifies that the format of the attachment is valid for conversion.
If the format is not valid and the user's BlackBerry device is based, the Open Attachment menu item does not appear on the user's BlackBerry device.
3. The user clicks the Open Attachment menu item to view the attachment on the BlackBerry device.
4. The attachment viewer sends the request to the BlackBerry Messaging Agent.
5. The BlackBerry Messaging Agent connects to the BlackBerry Attachment Service over port 1900.
6. The BlackBerry Attachment Service retrieves the attachment in binary format from the user's message store using the BlackBerry Messaging Agent link to the messaging server.
The BlackBerry Attachment Service distills the attachment and extracts the content, layout, appearance, and navigation information from the attachment.
The BlackBerry Attachment Service organizes, stores, and links the information in a proprietary DOM in a binary XML style.
The BlackBerry 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).
The BlackBerry Attachment Service sends the UCS data to the BlackBerry Messaging Agent using a TCP/IP connection over port 1900.
7. The BlackBerry Messaging Agent sends the converted attachment to the BlackBerry Dispatcher.
8. The BlackBerry Dispatcher compresses the first portion of the attachment, encrypts it using the device transport key of the BlackBerry device, and sends the first portion of the attachment to the BlackBerry Router.
9. The BlackBerry Router sends the first portion of the attachment to the wireless network over port 3101.
10. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network.
11. The wireless network delivers the attachment to the BlackBerry device.
12. The BlackBerry device sends a delivery confirmation to the BlackBerry Dispatcher, which sends it to the BlackBerry Messaging Agent. If the BlackBerry Enterprise Server does not receive a delivery confirmation within 4 hours, it sends the attachment data to the wireless network again.
13. The BlackBerry device uses its device transport key to decrypt and decompress the attachment so that the user can view the attachment.
14. The user views the attachment on the BlackBerry device by selecting a section from the table of contents, or by viewing the full attachment. The original formatting of the attachment, including indents, tables, fonts, and bullets, is reflected on the BlackBerry device.

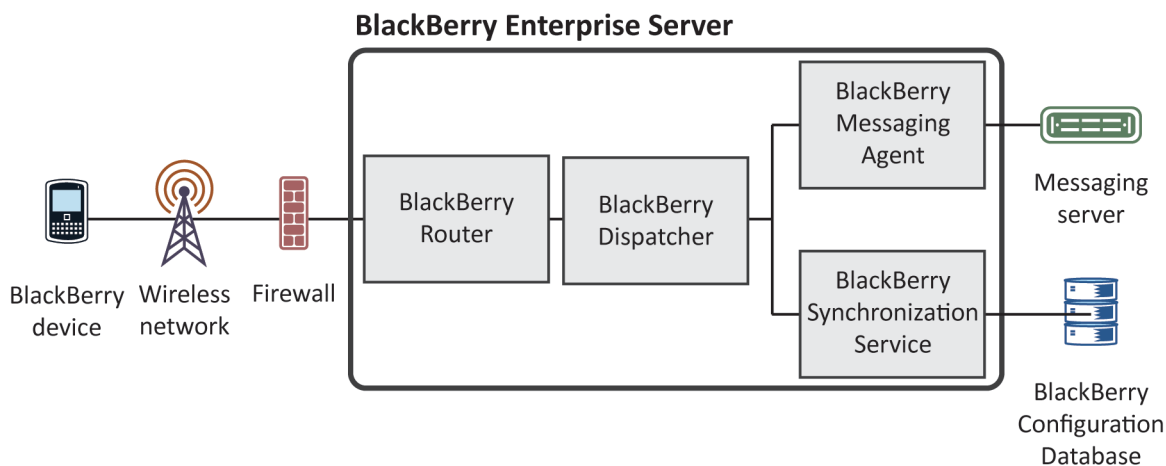
Process flow: Viewing an attachment using a link



1. A user clicks the Get Link menu item to view an attachment on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service creates an HTTP session for the user and sends the request to the web server. The BlackBerry MDS Connection Service retrieves the requested content and sends it to the BlackBerry Attachment Service.
5. The BlackBerry Attachment Service extracts the content, layout, appearance, and navigation information from the attachment and organizes, stores, and links the information in a proprietary DOM in a binary XML style.
6. The BlackBerry 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 BlackBerry Attachment Service sends the converted attachment to the BlackBerry MDS Connection Service using HTTP.
8. The BlackBerry MDS Connection Service sends the first 250 KB of content to the BlackBerry Dispatcher over port 3200.
9. The BlackBerry Dispatcher compresses the content, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
10. The BlackBerry Router sends the encrypted content to the BlackBerry device.
11. The BlackBerry device uses its device transport key to decrypt and decompress the attachment content so that the user can view the attachment.
12. The user views the attachment on the BlackBerry device using the browser plug-in for the attachment viewer. The attachment viewer processes 3 KB at a time.

Organizer data process flows

Process flow: Synchronizing organizer data for the first time on a BlackBerry device



1. A user activates a new BlackBerry device or upgrades an existing BlackBerry device and receives the service book for the BlackBerry Synchronization Service.
2. The BlackBerry device requests the synchronization configuration information from the BlackBerry Synchronization Service.

The configuration information indicates whether wireless data synchronization on the BlackBerry Enterprise Server is turned on, and which database can be synchronized. The configuration information also provides database synchronization types and conflict resolution settings. All data that the BlackBerry device and BlackBerry Enterprise Server send between each other is compressed and encrypted.

3. The BlackBerry Synchronization Service returns the configuration information and synchronizes the databases using that information.

A synchronization agent on the BlackBerry device tracks which databases can be synchronized over the wireless network. If data already exists on both the BlackBerry device and BlackBerry Enterprise Server, the BlackBerry Synchronization Service merges, adds, or updates the records during the synchronization process. If data exists on only the BlackBerry device or BlackBerry Enterprise Server, the BlackBerry Synchronization Service restores the data from

the appropriate location. The BlackBerry device and BlackBerry Enterprise Server do not delete records during the initial synchronization process.

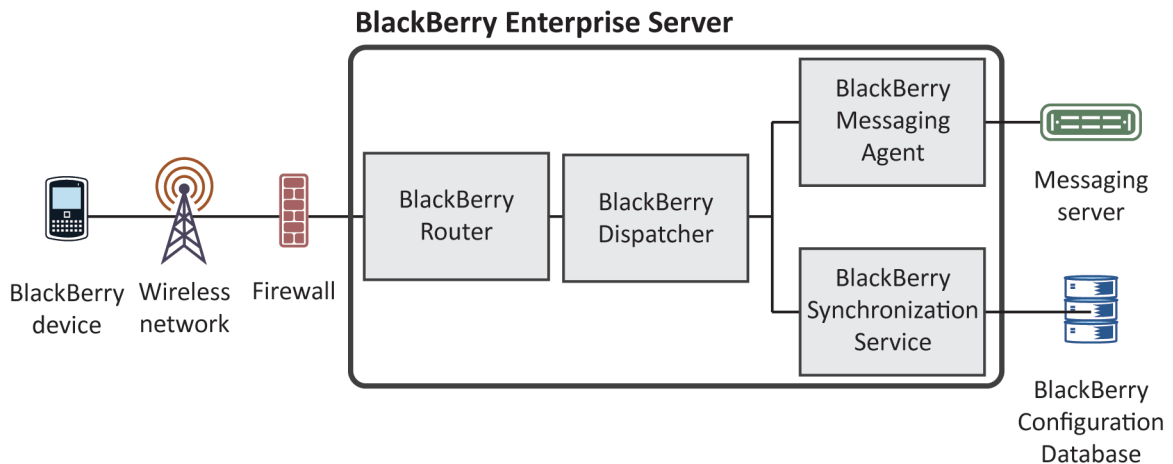
After the BlackBerry Synchronization Service registers a database for wireless data synchronization, it can no longer be synchronized or restored using the BlackBerry Desktop Software.

The initial synchronization process is complete when the data on the BlackBerry device and the data on the BlackBerry Enterprise Server are synchronized. Future changes on the BlackBerry device or BlackBerry Enterprise Server are synchronized over the wireless network.

If the user changes data on the BlackBerry device or in the organizer application on the user's computer during the initial synchronization process, the BlackBerry Synchronization Service synchronizes the changes after the initial synchronization completes.

If the user connects the BlackBerry device to a computer that is running the BlackBerry Device Manager, the initial synchronization process can occur over the connection to the BlackBerry Router instead of over the wireless network.

Process flow: Synchronizing subsequent changes to organizer data



1. A user saves a change to the organizer data or BlackBerry device settings (for example, a new AutoText entry) on a BlackBerry device or in the organizer application on the user's computer.
2. Depending on where the user made the change, the BlackBerry device or the BlackBerry Enterprise Server adds the change to a changelist and sends the changelist to the BlackBerry Synchronization Service.
The changelist includes the target database and record information for the organizer application.
3. The BlackBerry Synchronization Service sends a change to organizer data over the wireless network, along with other entries in the changelist for the user.

The BlackBerry Synchronization Service sends other changes, including BlackBerry device information, time zone information, and backup and restore data, at the batch synchronization interval that is set on the BlackBerry Enterprise Server. By default, the batch synchronization interval is 10 minutes.

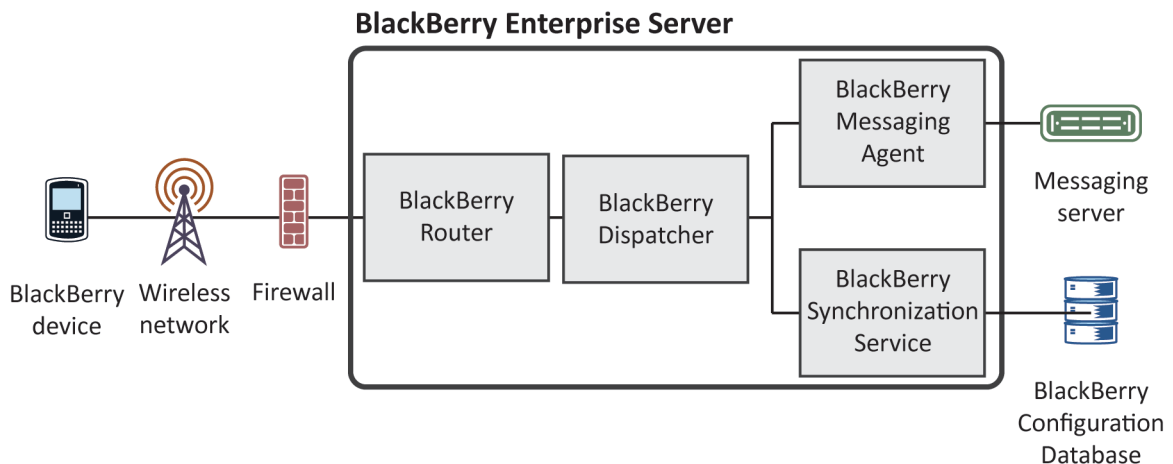
To prevent synchronization errors, the BlackBerry Enterprise Server and BlackBerry device can send only a single changelist at a time for a user account.

The BlackBerry Synchronization Service writes a synchronization request entry to the SyncRequest table of the BlackBerry Configuration Database, and sends the changed records to the BlackBerry Dispatcher.

4. The BlackBerry Dispatcher compresses the content, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router for delivery to the BlackBerry device.
5. The BlackBerry device sends a delivery confirmation to the BlackBerry Synchronization Service for each record that it receives.
6. The BlackBerry Synchronization Service receives delivery confirmations, deletes the corresponding synchronization request entries from the SyncRequest table, and writes an entry to the SyncRecordState table for each delivery confirmation.

Each organizer database record has a unique identifier that is mapped to a corresponding record on the BlackBerry device.

Process flow: Adding a contact picture on a BlackBerry device



1. A user adds a picture to a contact in the address book on a BlackBerry device and saves the change.
2. The BlackBerry device creates a changelist request to synchronize the changed record. The changelist request includes the updated record information and identifies the address book as the target for the update.

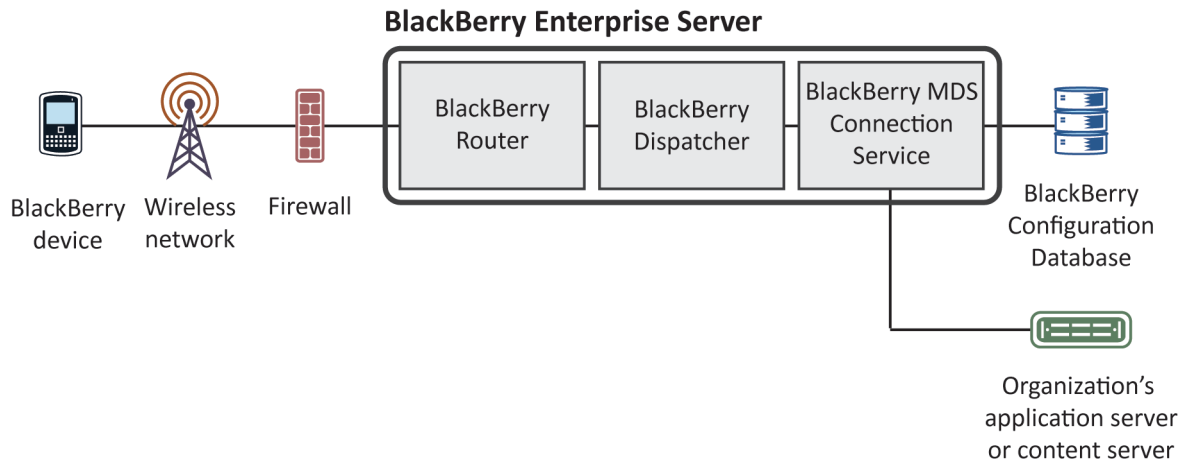
The BlackBerry device compresses and encrypts the request, and sends the request to the BlackBerry Dispatcher over port 3101.

3. The BlackBerry Dispatcher uses the device transport key of the BlackBerry device to decrypt and decompress the request, and sends the request to the BlackBerry Synchronization Service.
4. The BlackBerry Synchronization Service receives the changelist request, writes a synchronization request entry in the SychRequest table of the BlackBerry Configuration Database, and sends the changed record to the BlackBerry Dispatcher.
5. The BlackBerry Dispatcher sends the changed record, in XML format, to the BlackBerry Messaging Agent.
If the file size of the picture exceeds 32 KB, the BlackBerry Messaging Agent rejects the synchronization request.
6. The BlackBerry Messaging Agent sends the changed record to the messaging server.
7. The messaging server updates the user's personal contact list.
8. The BlackBerry Messaging Agent sends a delivery confirmation to the BlackBerry Dispatcher.
9. The BlackBerry Dispatcher sends the delivery confirmation to the BlackBerry Synchronization Service.
10. The BlackBerry Synchronization Service deletes the synchronization request entry from the SyncRequest table, writes an entry in the SyncRecordState table, and sends the delivery confirmation to the BlackBerry Dispatcher.
11. The BlackBerry Dispatcher encrypts the results using the device transport key of the BlackBerry device, compresses them, and sends them to the BlackBerry Router.
12. The BlackBerry Router sends the results to the wireless network over port 3101.
13. The wireless network verifies that the PIN belongs to a valid BlackBerry device and sends the delivery confirmation to the BlackBerry device.

If the BlackBerry device does not receive the delivery confirmation from the wireless network within 20 minutes, it sends the synchronization request to the wireless network again. If the BlackBerry device does not receive the delivery confirmation within 8 hours, it stops resending the synchronization request to the wireless network.

Mobile data process flows

Process flow: Requesting BlackBerry Browser content on a BlackBerry device



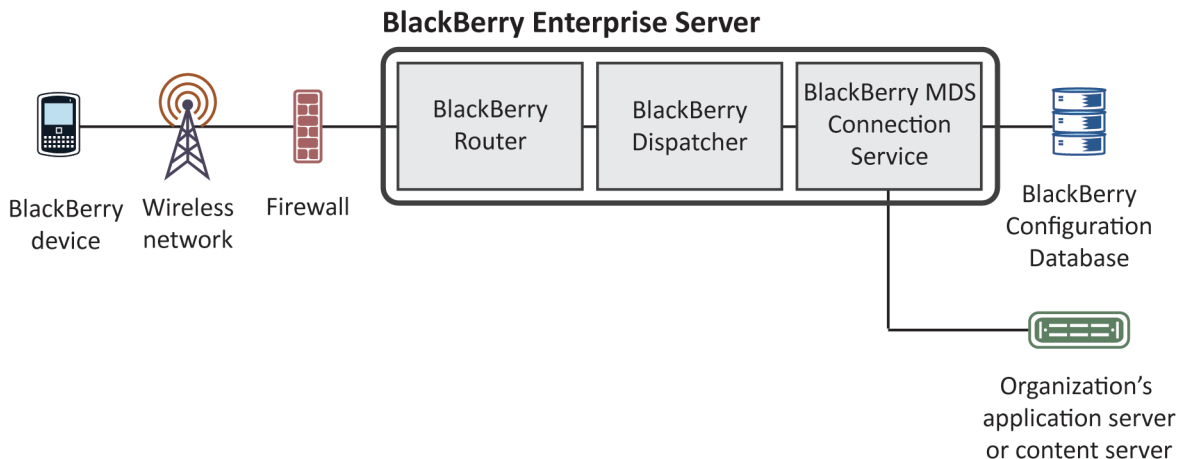
1. A user requests Internet or intranet content from your organization's content server using the BlackBerry Browser on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service creates an HTTP session for the user and retrieves the requested Internet or intranet content from the content server.

The BlackBerry MDS Connection Service converts the content so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.

5. The BlackBerry Dispatcher compresses the content, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
6. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.
7. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network and sends the encrypted content to the BlackBerry device.
8. The BlackBerry device sends a delivery confirmation to the BlackBerry Router, and decrypts and decompresses the content so that the user can view it in the BlackBerry Browser.

If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

Process flow: Requesting BlackBerry Browser content while access control is turned on for the BlackBerry MDS Connection Service

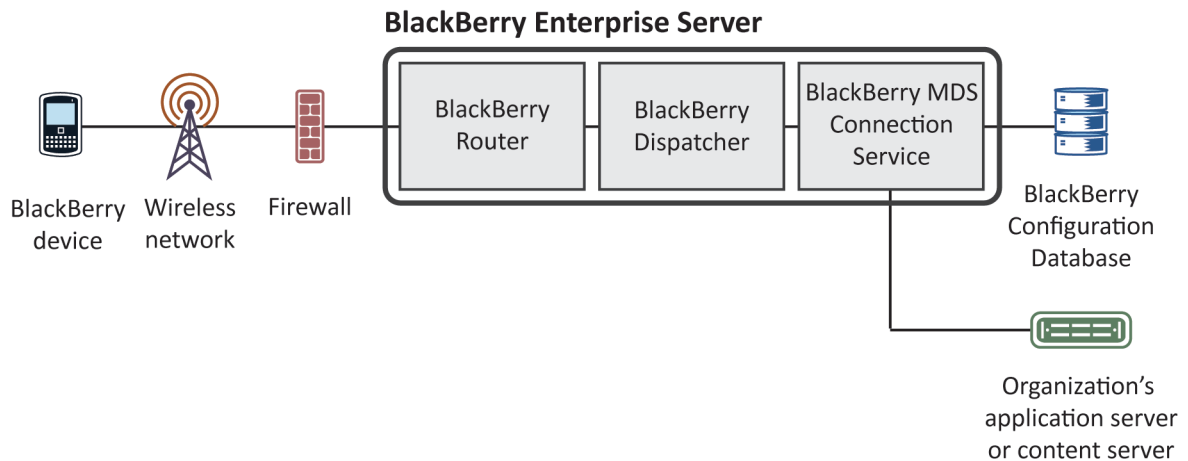


1. A user requests Internet or intranet content from your organization's content server using the BlackBerry Browser on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service checks the BlackBerry Configuration Database to verify whether pull authorization is turned on, and whether the user has permission to pull content from the specified content server.
If the user does not have permission to pull content from the specified content server, the BlackBerry MDS Connection Service rejects the request and sends an error message to the BlackBerry device.
5. The BlackBerry MDS Connection Service creates an HTTP session for the user and sends the user's authentication credentials to the content server. If the user authenticates, the BlackBerry MDS Connection Service sends the HTTP request to the content server. If the user does not authenticate, the BlackBerry Browser displays an HTTP 403 Error message, and prompts the user to type the correct credentials.
6. The BlackBerry MDS Connection Service retrieves the content from the content server, converts it so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.
7. The BlackBerry Dispatcher compresses the content, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
8. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.

9. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network and sends the encrypted content to the BlackBerry device.
10. The BlackBerry device sends a delivery confirmation to the BlackBerry Router, and decrypts and decompresses the content so that the user can view it in the BlackBerry Browser.

If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

Process flow: Requesting BlackBerry Browser content with two-factor authentication turned on



1. A user requests Internet or intranet content from your organization's content server using the BlackBerry Browser on a BlackBerry device.
2. The BlackBerry device sends the request to the BlackBerry Enterprise Server over port 3101.
3. The BlackBerry Dispatcher sends the request to the BlackBerry MDS Connection Service over port 3200.
4. The BlackBerry MDS Connection Service checks whether the user's BlackBerry device is running an authenticated connection that can support the content request.

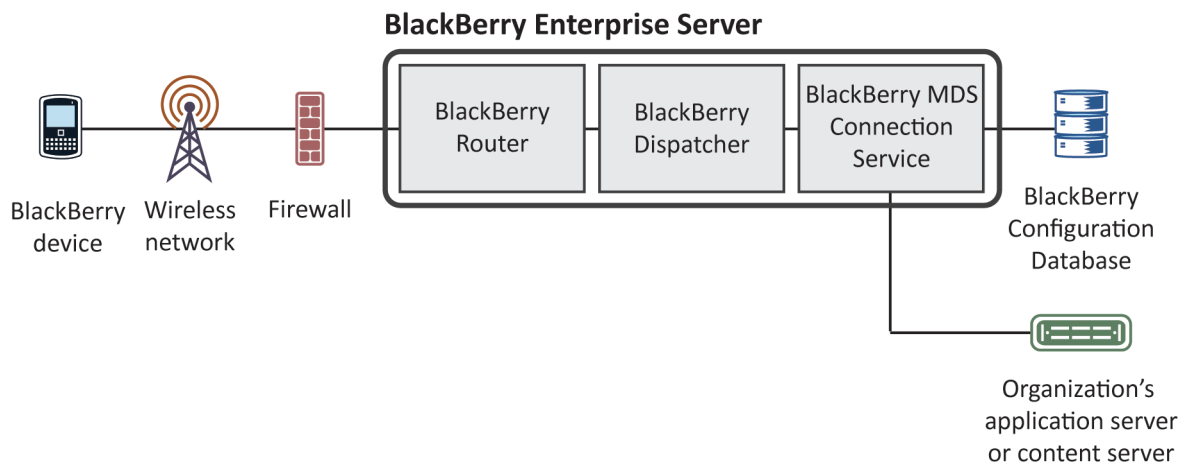
If the BlackBerry device is not running an authenticated connection, the BlackBerry MDS Connection Service redirects the user to a login web page. If the user logs in, using an RSA SecurID user name and passcode, the BlackBerry MDS Connection Service creates a connection to the content server. By default, the BlackBerry device caches the user's information for 24 hours of activity on the authenticated connection, or 60 minutes of inactivity.

The BlackBerry MDS Connection Service creates an HTTP session for the user and retrieves the Internet or intranet content from the content server. The BlackBerry MDS Connection Service converts the content so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.

5. The BlackBerry Dispatcher compresses the content, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
6. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.
7. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network and sends the encrypted content to the BlackBerry device.
8. The BlackBerry device sends a delivery confirmation to the BlackBerry Router, and decrypts and decompresses the content so that the user can view it in the BlackBerry Browser.

If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

Process flow: Pushing application content to a BlackBerry device



1. A push application on an application server or a content server behind your organization's firewall sends an HTTP POST request to a central push server over the listen port for the content server. The default port number is 8080.

You can define one or more instances of the BlackBerry MDS Connection Service in a BlackBerry Domain as a central push server. A push application specifies the BlackBerry Enterprise Server host name and the connection port number that the BlackBerry MDS Connection Service listens on.

2. The central push server checks the BlackBerry Configuration Database for the following information about the intended recipients of the application content: the PINs that are associated with the user accounts, whether the PINs are enabled for the BlackBerry MDS Connection Service, and the active BlackBerry Enterprise Server instances that the users are located on.

User accounts that do not appear in the BlackBerry Configuration Database, or that are pending deletion, cannot receive the push content.

The central push server responds to the push application to acknowledge that it is processing the request, and sends the push content to the BlackBerry MDS Connection Service instances that have active, primary connections to the BlackBerry Enterprise Server instances.

3. The BlackBerry MDS Connection Service converts the content so that the user can view it on the BlackBerry device, and sends the content to the BlackBerry Dispatcher over port 3200.
4. The BlackBerry Dispatcher compresses the content, encrypts it using the device transport key of the BlackBerry device, and sends the encrypted content to the BlackBerry Router.
5. The BlackBerry Router sends the encrypted content to the wireless network over port 3101.

The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network, and sends the encrypted content to the BlackBerry device.

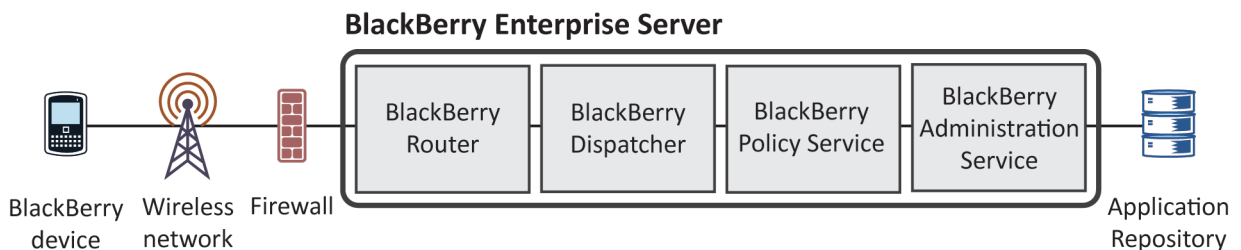
6. The BlackBerry device sends a delivery confirmation to the BlackBerry Router.

If the BlackBerry MDS Connection Service does not receive a delivery confirmation within the flow control timeout limit, it sends a message to the wireless network to delete the pending content.

7. The BlackBerry device decrypts and decompresses the content.

The BlackBerry Application detects the incoming content by listening on a port number that the application developer specified. For example, the BlackBerry Browser listens for push application connections on port 7874. The application displays the content on the BlackBerry device when the user runs the application.

Process flow: Installing a BlackBerry Java Application on a BlackBerry device over the wireless network



1. A developer creates a BlackBerry Java Application using the BlackBerry Java Development Environment or another Java authoring tool. The developer produces an application bundle.

The application bundle contains an .alx file that stores information about the attributes of the BlackBerry Java Application, including the author name, a description of the application, and copyright information.

2. In the BlackBerry Administration Service, you publish the application bundle to the application repository.

3. You create a software configuration and add the BlackBerry Java Application to the software configuration. You specify that the application is required, assign an application control policy to the application, and specify wireless delivery to BlackBerry devices.

You assign the software configuration to a group.

4. The BlackBerry Administration Service creates a deployment job.

A deployment job represents the objects that must be sent to each user's BlackBerry device and consists of multiple tasks. Each task manages the delivery of an object (for example, a BlackBerry Java Application, an access control policy, or an IT policy) to a BlackBerry device.

5. The delivery manager component of the BlackBerry Administration Service receives tasks to send a BlackBerry Java Application to BlackBerry devices.
6. The BlackBerry Administration Service exports the files for the BlackBerry Java Application to a shared network folder.
7. The delivery manager converts the tasks into send module commands, queues send module commands into logical groups for each user, and sends the send module commands to the BlackBerry Policy Service. Separate applications are queued in separate groups.
8. The BlackBerry Policy Service processes the send module commands in the queue in sequence. When the BlackBerry Policy Service processes a group of send module commands, it retrieves the data for the BlackBerry Java Application from the shared network folder, and sends the send module commands with the application data to the BlackBerry Dispatcher.

If the send module commands are less than 56 KB, the BlackBerry Policy Service sends them in one data packet. If the send module commands exceed 56 KB, the BlackBerry Policy Service sends them in multiple data packets.

9. The BlackBerry Dispatcher sends the send module commands to the BlackBerry Router.
10. The BlackBerry Router sends the send module commands to a BlackBerry device over the wireless network.
11. The BlackBerry device installs the BlackBerry Java Application. The BlackBerry device sends an acknowledgement packet for the BlackBerry Java Application to the BlackBerry Router.
12. The BlackBerry Router sends the acknowledgement packet to the BlackBerry Dispatcher.
13. The BlackBerry Dispatcher delivers the acknowledgement packet to the BlackBerry Policy Service.
14. The BlackBerry Policy Service clears the send module commands for the BlackBerry device from the queue and processes the next group of send module commands that are in the queue.
15. The BlackBerry Administration Service displays that the BlackBerry Java Application was delivered to the BlackBerry device.

If the BlackBerry device does not receive all of the send module commands within 4 hours, the BlackBerry device sends a failure acknowledgement packet to the BlackBerry Policy Service. The BlackBerry Administration Service detects the failure acknowledgement packet and displays an installation failure message for the BlackBerry device.

BlackBerry device management process flows

Process flow: Activating a BlackBerry device over the wireless network

A user receives or purchases a new BlackBerry device.

1. The user contacts your organization's IT department to activate the BlackBerry device.
2. You create a temporary activation password for the user account and communicate the password to the user. The password applies to the user account only.
3. To activate the BlackBerry device over the wireless network, the user opens the activation application on the BlackBerry device and types the appropriate email address and activation password.
4. The BlackBerry device sends an activation request message to the email account. The message contains information about the BlackBerry device, such as routing information and the public keys for the BlackBerry device.
5. 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.

The BlackBerry Enterprise Server and BlackBerry device establish a device transport key. The BlackBerry Enterprise Server and BlackBerry device confirm knowledge of the device transport key to each other. If the confirmation is successful, the activation proceeds and further communication between the BlackBerry Enterprise Server and BlackBerry device is encrypted.

The BlackBerry Enterprise Server sends an IT policy to the BlackBerry device. If the BlackBerry device cannot accept the IT policy, the activation process does not complete.

The BlackBerry Enterprise Server sends the appropriate service books (for example, the 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.

6. If the user account is configured for wireless synchronization, and if wireless backup and wireless calendar synchronization on the BlackBerry device are turned on, the BlackBerry Enterprise Server sends user data to the BlackBerry device.

Process flow: Resending an IT policy to a BlackBerry device manually

1. You click a user account, and then click Resend IT Policy.
2. The BlackBerry Policy Service reads the current IT policy settings for the user account from the BlackBerry Configuration Database to determine which IT policy to send to the BlackBerry device.

The BlackBerry Policy Service prepares to send the IT policy using the GME protocol by adding the unique identifier and BlackBerry Enterprise Server version.

The BlackBerry Policy Service adds the unique key that the BlackBerry Domain uses to sign IT policy data packets to the IT policy data packet.

The BlackBerry Policy Service sends the IT policy data packet to the BlackBerry Dispatcher.
3. The BlackBerry Dispatcher encrypts the IT policy data packet using the device transport key of the BlackBerry device, compresses the content, and sends it to the BlackBerry Router for delivery to the BlackBerry device.
4. The BlackBerry Router sends the encrypted IT policy data packet to the wireless network over port 3101. The wireless network verifies that the PIN belongs to a valid BlackBerry device that is registered with the wireless network.

Process flow: Authenticating data on a BlackBerry device without connecting to the BlackBerry Infrastructure

1. A user connects a BlackBerry device to a computer that the BlackBerry Device Manager is running on.
2. The BlackBerry Router uses a unique authentication protocol to verify that the user is a valid BlackBerry device user.

The authentication sequence uses the same authentication information for the BlackBerry Enterprise Server and BlackBerry device that the SRP authentication sequence uses to validate the BlackBerry Enterprise Server before permitting it to connect to the BlackBerry Infrastructure. The BlackBerry Router cannot access the value of the device transport key of the BlackBerry device and BlackBerry Enterprise Server.
3. The BlackBerry device and BlackBerry Router use the BlackBerry Device Manager to send data to each other over the physical connection, behind the firewall. All the data that the BlackBerry device and BlackBerry Enterprise Server send to each other is compressed and encrypted. This data bypasses the wireless network.

The transfer of wireless data over an SRP connection is restored when the user disconnects the BlackBerry device from the computer or closes the BlackBerry Device Manager.

Glossary

10

AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
API	application programming interface
ASCII	American Standard Code for Information Interchange
BlackBerry Domain	A BlackBerry Domain consists of the BlackBerry Configuration Database with its users and any BlackBerry Enterprise Server instances that connect to it.
BlackBerry MDS	BlackBerry Mobile Data System
BlackBerry transport layer encryption	BlackBerry transport layer encryption (formerly known as standard BlackBerry encryption) uses a symmetric key encryption algorithm to help protect data that is in transit between a BlackBerry device and the BlackBerry® Enterprise Server when the data is outside an organization's firewall.
CBC	cipher block chaining
CDMA	Code Division Multiple Access
CMIME	Compressed Multipurpose Internet Mail Extensions
content protection	Content protection helps protect user data on a locked BlackBerry device by encrypting the user data using the content protection key and ECC private key.
DES	Data Encryption Standard
device transport key	The device transport key (formerly known as the master encryption key) is unique to a BlackBerry device. The BlackBerry device and BlackBerry Enterprise Server use the device transport key to encrypt the message keys.
DMZ	A demilitarized zone (DMZ) is a neutral subnetwork outside of an organization's firewall. It exists between the trusted LAN of the organization and the untrusted external wireless network and public Internet.
DNS	A Domain Name System (DNS) is an Internet database that translates domain names that are meaningful and recognizable by people into the numeric IP addresses that the Internet uses.
DOM	Document Object Model
ECC	Elliptic Curve Cryptography
EDGE	Enhanced Data Rates for Global Evolution

Enterprise Service Policy	The Enterprise Service Policy controls which BlackBerry devices can connect to a BlackBerry Enterprise Server.
GAL	Global Address List
GAN	generic access network
GANC	generic access network controller
gateway message envelope	The gateway message envelope protocol is a Research In Motion proprietary protocol that allows the transfer of compressed and encrypted data between the wireless network and BlackBerry devices. The protocol defines a routing layer that specifies the types of message contents allowed and the addressing information for the data. Gateways and routing components use this information to identify the type and source of the BlackBerry device data, and the appropriate destination service to route the data to.
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol over Secure Sockets Layer
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
ISP	Internet service provider
IP	Internet Protocol
IP address	An Internet Protocol (IP) address is an identification number that each computer or mobile device uses when it sends or receives information over a network, such as the Internet. This identification number identifies the specific computer or mobile device on the network.
IT administration command	An IT administration command is a command that you can send over the wireless network to protect sensitive information on a BlackBerry device or delete all BlackBerry device data.
IT policy	An IT policy consists of various IT policy rules that control the security features and behavior of BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager.
IT policy rule	An IT policy rule permits you to customize and control the actions that BlackBerry smartphones, BlackBerry PlayBook tablets, the BlackBerry Desktop Software, and the BlackBerry Web Desktop Manager can perform.
Java ME	Java Platform, Micro Edition
JDBC	Java Database Connectivity
JSON	JavaScript Object Notation

Kerberos protocol	The Kerberos protocol is a Microsoft Active Directory authentication protocol that permits a trusted third-party application to authenticate clients by exchanging encrypted service tickets with Microsoft Active Directory.
LAN	A local area network (LAN) is a computer network shared by a group of computers in a small area, such as an office building. Any computer in this network can communicate with another computer that is part of the same network.
LDAP	Lightweight Directory Access Protocol
LTPA	Lightweight Third-Party Authentication
MAPI	Messaging Application Programming Interface
message keys	The message keys encrypt the data that is sent to and from a BlackBerry device.
messaging server	A messaging server sends and processes messages and provides collaboration services, such as updating and communicating calendar and address book information.
MSDE	Microsoft SQL Server Desktop Engine
MTLS	Mutual Transport Layer Security
NAT	network address translation
NTLM	NT LAN Manager
PIN	personal identification number
principal encryption key	The principal encryption key encrypts the device transport key when a BlackBerry device is locked if content protection is turned on.
RPC	remote procedure call
RTF	Rich Text Format
service books	Service books determine which services are available on BlackBerry devices.
SIP	Session Initiation Protocol
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRP	Server Routing Protocol
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.
Triple DES	Triple Data Encryption Standard

UCS	Universal Content Stream
UMA	Unlicensed Mobile Access
UNC	Universal Naming Convention
USB	Universal Serial Bus
VPN	virtual private network
WAP	Wireless Application Protocol
XML	Extensible Markup Language

Provide feedback

11

To provide feedback on this content, visit www.blackberry.com/docsfeedback.

Legal notice

12

©2013 BlackBerry. All rights reserved. BlackBerry® and related trademarks, names, and logos are the property of BlackBerry Limited and are registered and/or used in the U.S. and countries around the world.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated. Bluetooth is a trademark of Bluetooth SIG. Corel and WordPerfect are trademarks of Corel Corporation. GSM is a trademark of the GSM MOU Association. IBM, Lotus, Domino and Sametime are trademarks of International Business Machines Corporation. IEEE 802.11a, IEEE 802.11b, and IEEE are trademarks of the Institute of Electrical and Electronics Engineers, Inc. Java, JDBC, and JavaScript Kerberos is a trademark of the Massachusetts Institute of Technology. Microsoft, Hyper-V, ActiveX, Active Directory, Excel, PowerPoint, SQL Server, Visual Studio, RSA Authentication Manager, Microsoft Lync Server, Windows, and Windows Server are trademarks of Microsoft Corporation. Novell and GroupWise are trademarks of Novell, Inc. PGP is a trademark of PGP Corporation. RSA and RSA SecurID are trademarks of RSA Security. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE

DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of

separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

Certain features outlined in this documentation require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, and/or BlackBerry Device Software.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Certain features outlined in this documentation might require additional development or Third Party Products and Services for access to corporate applications.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>