

BlackBerry Device Software

Securing Devices for Personal Use and
Work Use

Version: 6.0

[Security Note](#)



Contents

1	Securing devices in your organization's environment for personal use and work use.....	2
2	New features in this release.....	3
3	System requirements.....	4
4	How a device classifies what data and applications are for work use or personal use.....	5
	Data and applications that a device classifies for work use.....	5
	Data and applications that a device classifies for personal use.....	6
5	Preventing a user from compromising work data on a device.....	7
	Preventing a user from pasting work data into a personal application.....	7
	Preventing a user from forwarding work data using personal channels.....	8
	Prevent a user from using the work contact list in personal email accounts and personal calendars.....	8
	Controlling the browsing traffic in the BlackBerry Browser.....	8
	Preventing a user from backing up work data that is stored on a device.....	9
	Protecting work data on a media card.....	9
6	Deleting only work data from a device.....	11
	Delete only work data from a device.....	12
7	Managing third-party applications on a device that a user uses for personal purposes.....	13
8	Managing add-on applications on a device that a user uses for personal purposes.....	14
9	IT policy rules that apply to devices that users use for personal purposes.....	15
10	Known issues.....	16
11	Related resources.....	17
12	Document revision history.....	18
13	Glossary.....	19
14	Provide feedback.....	21
15	Legal notice.....	22

Securing devices in your organization's environment for personal use and work use

1

Your organization might want to permit BlackBerry® device users to use BlackBerry devices for both personal use and work use. For example, your organization might want to permit users to activate personal devices on a BlackBerry® Enterprise Server or permit users to use devices that your organization purchases for personal use.

If devices are running a BlackBerry® Device Software version that can distinguish between personal data and work data, security features and options on the devices allow the devices to treat your organization's data and applications differently from personal data and applications. The features and options have the following benefits:

- permit your organization to control access to your organization's data and applications on the devices
- help prevent your organization's data from being compromised
- provide a unified experience for users when they access personal data and work data
- permit your organization to delete your organization's data and applications from personal devices when users are no longer a part of your organization

New features in this release

2

Feature	Description
ability to delete your organization's data and leave personal data intact	You can delete only your organization's data on a personal BlackBerry® device and remove the device from the BlackBerry® Enterprise Server. This feature does not delete personal data, so a BlackBerry device user can continue to use their personal device even after the user is no longer a part of your organization.
ability to prevent a user from pasting your organization's data into personal applications	You can prevent a user from unintentionally compromising your organization's data by preventing the user from pasting your organization's data into personal applications. For example, you can prevent a user from copying information from a work email message to a personal email account.
ability to control which applications can access your organization's data	You can configure which third-party applications and add-on applications developed by Research In Motion® are authorized by your organization to access your organization's data. This feature makes sure that you can control which applications can access your organization's data and permits personal applications and work applications to coexist on the same device.
ability to prevent a user from forwarding your organization's data using personal channels	To maintain control over your organization's data, you can prevent a user from forwarding data using personal channels (for example, the BlackBerry® Internet Service). This feature is designed to make sure that the device can send your organization's data using a work channel only (for example, a BlackBerry Enterprise Server), and not a personal channel.

Related topics

[Deleting only work data from a device, 11](#)

[Preventing a user from pasting work data into a personal application, 7](#)

[Preventing a user from forwarding work data using personal channels, 8](#)

[Data and applications that a device classifies for work use, 5](#)

[Data and applications that a device classifies for personal use, 6](#)

System requirements

3

To help secure BlackBerry® devices for personal use in your organization's environment, you must use either BlackBerry® Enterprise Server for Microsoft® Exchange (5.0 SP3 or later), BlackBerry® Enterprise Server for IBM® Lotus® Domino® (5.0 SP3 or later), or BlackBerry® Enterprise Server Express (5.0 SP3 or later) and one of the following devices that is running BlackBerry® 6:

- BlackBerry® Torch™ 9800 smartphone (bundle 1478 or later)
- BlackBerry® Bold™ 9780 smartphone (bundle 1478 or later)
- BlackBerry® Bold™ 9700 smartphone (bundle 1478 or later)
- BlackBerry® Curve™ 9300 smartphone (bundle 1478 or later)
- BlackBerry® Pearl™ 9100 smartphone (bundle 1478 or later)
- BlackBerry® Curve™ 9330 smartphone (bundle 1830 or later)
- BlackBerry® Bold™ 9650 smartphone (bundle 1830 or later)
- BlackBerry® Style™ 9670 smartphone (bundle 1830 or later)

How a device classifies what data and applications are for work use or personal use

To control what happens to your organization's data and applications on a BlackBerry® device, you can configure a device to distinguish between data and applications that are for personal use and data and applications that are for work use. You must set the Enable Separation of Work Content IT policy rule to Yes before the device can distinguish between work data and personal data.

By default, after you configure the Enable Separation of Work Content IT policy rule, core applications can access work data, personal data, or both. For example, the email application can access both work data and personal data because a BlackBerry device user can use the email application to manage the work email account and personal email accounts. To determine whether a third-party application or an add-on application developed by Research In Motion® can access work data, you must configure the "Is access to the corporate data API allowed" application control policy rule. The device checks this rule to determine which applications can access work data.

After you configure the Enable Separation of Work Content IT policy rule, the following events can occur:

- the device and BlackBerry® Enterprise Server do not synchronize personal organizer data
- an application can determine whether it can access work data
- after applications that can access work data register with the device, the applications can delete work data without deleting personal data when the device notifies the applications that they must delete work data

To help a device determine which data is work data, you can provide the device with domain information for your organization. You can specify a list of domain names, email address domains, and certificate server domains that are specific to your organization in the Work Domains IT policy rule. For example, if a user sends an email message to a contact that is not in the contact list on the device, the device can use the domain information in the Work Domains IT policy rule to determine whether the contact is a work contact.

Data and applications that a device classifies for work use

A BlackBerry® device classifies the following data and applications for work use:

- email messages and attachments that are sent to the BlackBerry device user's work email account and the email messages and attachments that the user sends from the work email account
- draft email messages that the user creates using their work email account
- calendar entries that the user creates using their work calendar
- contacts that the BlackBerry® Enterprise Server synchronizes with the user's work email account
- organizer data, such as tasks and memos
- applications that you send to the device from a BlackBerry Enterprise Server, and that have the "Is access to the corporate data API allowed" application control policy rule set to Allow
- files that the user accesses and downloads from your organization's network using the Files application
- files on media cards that are created by applications that can access work data (except for media applications)

The BlackBerry device classifies email addresses in the user's contact list as work email addresses using the domains that you specify in the Work Domains IT policy rule.

After the device classifies data for work use, the user cannot reclassify the data for personal use. For example, if a user selects a work email account in the Send Using field of a draft email message and starts typing a message in the body, the user cannot change the selected work email account to a personal email account. However, the user can reclassify personal data as work data. For example, if the user selects a personal email account in the Send Using field of a draft email message, the user can change the selected personal email account to a work email account even after they start typing a message in the body of the email.

Data and applications that a device classifies for personal use

A BlackBerry® device classifies the following data and applications for personal use:

- email messages and attachments that a BlackBerry device user sends from any email account (for example, a personal email account) except for the work email account
- contacts that the device synchronizes with personal email accounts (for example, Google Mail™ contacts)
- phone data (phone data is considered to be personal data but the call history and call logs are deleted when you delete work data)
- instant messages that a user sends or receives using BlackBerry® Messenger
- text messages that a user sends or receives using PIN messaging, SMS text messaging, or MMS messaging
- applications that have the "Is access to the corporate data API allowed" application control policy rule set to Deny
- content that is stored for the BlackBerry® Browser (the BlackBerry Browser is a personal application but the cache is deleted when you delete work data)
- maps
- media application data (for example, the camera, video, music, or voice recorder)
- passwords that the Password Keeper encrypts

Preventing a user from compromising work data on a device

5

A BlackBerry® device is designed to separate work data from personal data so that you can help prevent a BlackBerry device user from compromising your organization's data by using personal channels to unintentionally send work data. You can configure several features to help prevent a user from compromising your organization's data on a device:

- prevent a user from pasting work data into a personal application
- prevent a user from forwarding work data using a personal channel
- prevent a user from using the work contact list in personal email accounts and personal calendars
- prevent a user from backing up work data
- control the browser traffic in BlackBerry® Browser
- protect the work data that a user stores on a media card

Preventing a user from pasting work data into a personal application

To help prevent a BlackBerry® device user from pasting work data into a personal application, you can set the Enable Separation of Work Content IT policy rule to Yes so that the following guidelines apply to the user:

- a user can cut, copy, and paste work data from a work application to another work application
- a user cannot cut, copy, and paste work data from a work application to a personal application
- a user can cut, copy, and paste personal data from a personal application to a work application or another personal application

If a user tries to paste work data to a personal application, the BlackBerry device displays a warning message.

By default, the Enable Separation of Work Content IT policy rule is set to No. The device does not distinguish between work data and personal data.

If you set the Enable Separation of Work Content IT policy rule to Yes, a user can select a work email account in the Send Using field of a draft email message, paste work data into the body of the email message, and then change the selected work email account in the Send Using field to a personal email account before the user sends the email message. If you would like to prevent the user from changing the work email account to a personal email account, you should also set the Require Work Resources For Conducting Work Activities IT policy rule to Yes. By default, the Require Work Resources For Conducting Work Activities IT policy rule is set to No.

Preventing a user from forwarding work data using personal channels

To help prevent a BlackBerry® device user from forwarding work data using personal channels, you can set the Disable Forwarding of Work Content Using Personal Channels IT policy rule to Yes. Personal channels include the BlackBerry® Internet Service, SMS text messages, MMS messages, PIN messages, and BlackBerry® Messenger. When you set the Disable Forwarding of Work Content Using Personal Channels IT policy rule to Yes, the device permits the user to follow these guidelines:

- a user can forward work email messages, contacts, calendar entries, tasks, or memos using a work email account
- a user cannot forward work email messages, contacts, calendar entries, tasks, or memos using personal channels

If the user tries to forward work email messages, contacts, calendar entries, tasks, or memos using personal channels, the device is designed to display a warning message and does not permit the user to complete the task.

By default, the Disable Forwarding of Work Content Using Personal Channels IT policy rule is set to No. The device does not distinguish between work data and personal data when users forward data.

Prevent a user from using the work contact list in personal email accounts and personal calendars

By default, a BlackBerry® device does not prevent a BlackBerry device user from using personal email accounts or personal calendars to send email messages or calendar appointments to email addresses in the work contact list. For example, a user can send email messages to work email addresses using a personal email account and create meetings with work email addresses in a personal calendar.

To help prevent a user from using personal email accounts or personal calendars to send email messages or calendar appointments to email addresses in the work contact list, you can set the Require Work Resources For Conducting Work Activities IT policy rule to Yes. When you set this rule to Yes, a user must use the work email account to send email messages to work email addresses and the work calendar to send calendar invites to work email addresses.

Controlling the browsing traffic in the BlackBerry Browser

A BlackBerry® device user can use the BlackBerry® Browser to browse the Internet and your organization's intranet. The device does not consider the BlackBerry Browser to be a work application. You can change the behavior of the BlackBerry Browser depending on the IT policies that you configure in your organization's environment:

- If you do not want users to browse using the Internet Browser, set the Allow IBS Browser IT policy rule to No.
- If you do not want users to browse using Wi-Fi® hotspots, set the Allow Hotspot Browser IT policy rule to No.
- If you do not want users to browse using WAP, set the Enable WAP Config IT policy rule to No.
- If you want users to browse using only the BlackBerry® Enterprise Server, set the Allow Other Browser Services IT policy rule to No.
- If you do not want users to browse using the BlackBerry Enterprise Server, set the Allow Browser IT policy rule to No.

You can also configure pull rules to prevent a user from accessing specific web servers using the BlackBerry Browser. For more information about configuring pull rules, see the *BlackBerry Enterprise Server Administration Guide*.

BlackBerry® 6 permits you to control the browser transport selection for the BlackBerry Browser. For more information about browser transport selection, see the *Selecting Browser Transport Technical Note*.

Preventing a user from backing up work data that is stored on a device

By default, if your organization's environment includes BlackBerry® Enterprise Server for Microsoft® Exchange (5.0 SP3 or later) or BlackBerry® Enterprise Server for IBM® Lotus® Domino® (5.0 SP3 or later), a BlackBerry® device user can back up both work data and personal data on a computer using the BlackBerry® Desktop Software and BlackBerry® Web Desktop Manager. The user can restore the data to the device that the user backed up after the BlackBerry® Device Software is updated or when issues occur that require the user to restore the information.

In rare circumstances, when a user restores work data, a device might not be able to recognize the data as work data and might treat it as personal data. For example, if a user restores data from an existing device to a new device that the user did not activate on the BlackBerry® Enterprise Server and that has the radio turned off, the new device might not recognize the data as work data.

If you want to prevent the user from backing up work data, you can change the value of the Desktop Backup IT policy rule to No organizational databases. When you set the rule to No organizational databases, the device does not back up the following information:

- organizer data such as tasks or memos
- work contacts
- work calendar entries

Protecting work data on a media card

By default, a BlackBerry® device stores all data in unencrypted format on a media card. When you set the Enable Separation of Work Content IT policy rule to Yes, the device automatically encrypts all work data on a media card using a device key.

You can perform any of the following actions to further protect the work data on a media card:

- Prevent a user from storing any data on media cards by setting the Disable External Memory IT policy rule to Yes.
- Prevent a user from transferring data to a media card over a USB connection by setting the Disable USB Mass Storage IT policy rule to Yes.
- Permit the user to store data on media cards, but specify that the device must encrypt all data and not just work data. To configure this option, set the External File System Encryption Level IT policy rule to one of the following values:
 - Encrypt to User Password (excluding multi-media directories)
 - Encrypt to User Password (including multi-media directories)
 - Encrypt to Device Key (excluding multi-media directories)

- Encrypt to Device Key (including multi-media directories)
- Encrypt to User Password and Device Key (excluding multi-media directories)
- Encrypt to User Password and Device Key (including multi-media directories)

Deleting only work data from a device

6

To help secure your organization's data on a personal BlackBerry® device, you can permit your organization to delete work data from a device when a user no longer works at your organization. You can use the BlackBerry Administration Service to require that a personal device remove only work data when the device receives the Delete only the organization data and remove device IT administrative command over the wireless network. All personal data remains on the device. A BlackBerry device user cannot use the device or make emergency calls while the device deletes the work data.

The device permanently deletes the following work data:

Item	Description
email messages	<ul style="list-style-type: none"> email messages that are sent to the user's work email account and the email messages that the user sends from the work email account draft email messages that the user creates using their work email account
attachments	attachments that are sent to the user's work email account and the attachments that the user sends from the work email account
calendar entries	calendar entries that the user creates using their work calendar
contacts	contacts that the BlackBerry® Enterprise Server synchronizes with the user's work email account
memos	all memos
tasks	all tasks
call history	although the device defines phone data for personal use, the call history entries are deleted when you delete work data
call logs	although the device classifies phone data as personal data, the call log files are deleted when you delete work data
the BlackBerry® Browser cache	although the device specifies the BlackBerry Browser for personal use, the BlackBerry Browser cache is deleted when you delete work data
files	<ul style="list-style-type: none"> files that the user accesses and downloads from your organization's network using the Files application files on media cards that are created by applications that can access work data (except for media applications) work data is not deleted from the media card if the media card is not available when the device deletes work data, however the user cannot access work data on the media card after the device removes work data
IT policy	IT policy that is associated with your organization
PIN encryption key	references to your organization's PIN encryption key
device transport key	references to the device transport key which prevents the device from communicating with the BlackBerry Enterprise Server

Item	Description
work service books	service books on the device that the device classifies for work use

Delete only work data from a device

Before you begin: If you want to remove your organization's applications from the BlackBerry® device, create a software configuration that includes the applications and set the disposition of all work applications to Disallowed in the software configuration. Assign the software configuration to the user account to send it to the device. For more information, see the *BlackBerry Enterprise Server Administration Guide*.

1. In the BlackBerry Administration Service, on the **BlackBerry solution management** menu, expand **User**.
2. Click **Manage users**.
3. Search for a user account.
4. In the search results, click the PIN for the user account.
5. In the **Device activation** list, click **Delete only the organization data and remove device**.
6. Optionally, in the **Removing users and devices** section, in the **Actions** drop-down list, perform one of the following actions:
 - To delete a user account from the BlackBerry® Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Delete the user**.
 - In a Microsoft® Exchange environment, to delete a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Delete the user and remove BlackBerry information from the user's messaging system**.
 - In an IBM® Lotus® Domino® environment, to delete a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Delete the user and remove the profile document and the state database**.
 - To disable a user account from the BlackBerry Enterprise Server but retain the BlackBerry Enterprise Server information in the user's mailbox, click **Disable as BlackBerry user**.
 - In a Microsoft® Exchange environment, to disable a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Disable the user and remove BlackBerry information from the user's messaging system**.
 - In a Lotus Domino environment, to disable a user account from the BlackBerry Enterprise Server and remove the BlackBerry Enterprise Server information from the user's mailbox, click **Disable the user and remove the profile document and the state database**.
7. Click **Yes - Delete only the organization data and remove device**.

Managing third-party applications on a device that a user uses for personal purposes

7

By default, a BlackBerry® device classifies all third-party applications as work applications that can access work data.

After you set the Enable Separation of Work Content IT policy rule to Yes, if you do not want specific third-party applications to access work data such as work contacts, you can consider performing any of the following actions:

- Create a software configuration for all unlisted applications and set the "Is access to the corporate data API allowed" application control policy rule to Deny. This prevents all third-party applications from accessing work data. If you want to allow specific third-party applications to access work data, you can create a software configuration that allows only third-party applications that you specify to access work data.
- Create a software configuration for each application that you want to prevent from accessing work data and set the "Is access to the corporate data API allowed" application control policy rule to Deny. This prevents third-party applications that you specify from accessing work data and allows all third-party applications that you do not specify to access work data.
- Create a software configuration and set the disposition for unlisted applications to Disallowed. This prevents a BlackBerry device user from installing any third-party applications on the device that you did not specifically list in the software configuration.
- Create a software configuration that lists specific applications and set the disposition to Disallowed. This prevents a user from installing the third-party applications that you listed in the software configuration.

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

Managing add-on applications on a device that a user uses for personal purposes 8

By default, a BlackBerry® device classifies all add-on applications developed by Research In Motion® as work applications that can access work data.

After you set the Enable Separation of Work Content IT policy rule to Yes, if you do not want add-on applications to access work data such as work contacts, you can use existing IT policy rules to prevent the applications from accessing work data. For example, you can set the Disable Organizer Data Access for Social Networking Applications IT policy rule to Yes to prevent add-on applications such as Facebook® for BlackBerry® smartphones and MySpace® for BlackBerry® smartphones from accessing the work calendar and work contact list.

The Enable Separation of Work Content IT policy rule has some effect on add-on applications. For example, if you set the Enable Separation of Work Content IT policy rule to Yes, the Facebook application prevents users from pasting work data.

To prevent add-on applications developed by RIM from accessing work data, the "Is access to the corporate data API allowed" application control policy rule for the applications must be set to Deny. If this application control policy rule is not set to Deny, users can copy and paste work data into the applications.

For more information about which applications are add-on applications developed by RIM, browse to www.blackberry.com/support to read KB24317.

IT policy rules that apply to devices that users use for personal purposes

9

The following IT policy rules apply to BlackBerry® devices that BlackBerry device users use for personal purposes:

IT policy group	IT policy rule
Browser	<ul style="list-style-type: none">• Allow Hotspot Browser• Allow IBS Browser
Device Only	Enable WAP Config
Global	Allow Browser
Personal Devices	<ul style="list-style-type: none">• Disable Forwarding of Work Content Using Personal Channels• Enable Separation of Work Content• Require Work Resources for Conducting Work Activities• Work Domains
Security	<ul style="list-style-type: none">• Desktop Backup• Disable External Memory• Disable USB Mass Storage• External File System Encryption Level

For more information about the IT policy rules, see the *BlackBerry Enterprise Server Policy Reference Guide*.

Known issues

10

When the Require Work Resources For Conducting Work Activities and Enable Separation of Work Content IT policy rules are both set to Yes, and a BlackBerry® device user tries to open Windows Live™ Messenger, the user receives an error message. (DT 1013388)

When the Require Work Resources For Conducting Work Activities IT policy rule is set to No and a user configures a personal email account to Auto BCC a work email account, when the user creates an email message using the personal email account, the BlackBerry device uses a work email service record to send the email to the work email account. (DT 960873)

If a user receives a work email message with an attachment, the user is not prevented from forwarding the attachment using a personal email account over a Bluetooth® connection. (DT 893098)

Workaround: You can set the Disable Bluetooth IT policy rule to Yes to turn off support for Bluetooth technology on a device.

Personal applications that use the Accessibility API can still access work data. (DT 880284)

Personal applications can still view the file names and the file properties for work files. (DT 880246)

The Screenshot API allows third-party applications to take screen shots of the data on the device when it displays work data. (DT 879346)

Workaround: You can set the Allow Screen Shot Capture IT policy rule to No to prevent the device from allowing applications, including third-party applications, to take screen shots.

Related resources

11

Resource	Description
<i>BlackBerry Enterprise Server Administration Guide</i>	<ul style="list-style-type: none">• generating and changing device transport keys• configuring extended messaging encryption• managing security• protecting lost or stolen BlackBerry® devices
<i>BlackBerry Enterprise Server Policy Reference Guide</i>	<ul style="list-style-type: none">• understanding BlackBerry® Enterprise Server IT policy rules and application control policy rules• using IT policies and application control policies
<i>BlackBerry Enterprise Server Security Technical Overview</i>	<ul style="list-style-type: none">• understanding how the BlackBerry Enterprise Server is designed to help protect data that is in transit between a device and a BlackBerry Enterprise Server or your organization's LAN• managing security settings for all devices
<i>Enforcing Encryption of Internal and External File Systems on BlackBerry Devices Technical Overview</i>	<ul style="list-style-type: none">• understanding which data items devices encrypt by default• using encryption to protect stored files in the built-in media storage and media cards
<i>Protecting the BlackBerry device platform against malware</i>	<ul style="list-style-type: none">• understanding the default behavior of the device• understanding malware vulnerabilities on the device• managing the risk of malware attacks• using IT policy rules, application control rules, and code signing to help contain malware on the device

Document revision history

12

Date	Description
10 December 2010	Updated to include corrections and revisions
17 September 2010	Initial version

Glossary

13

API

application programming interface

BCC

blind carbon copy

BlackBerry device memory

The BlackBerry device memory consists of the NV store, flash memory, RAM, on-board device memory, and BlackBerry device key store.

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.

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.

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.

MMS

Multimedia Messaging Service

NV

nonvolatile

PIN

personal identification number

SMS

Short Message Service

USB

Universal Serial Bus

WAP

Wireless Application Protocol

Provide feedback

14

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

Legal notice

15

©2011 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. Facebook is a trademark of Facebook, Inc. Google Mail is a trademark of Google Inc. IBM, Domino, and Lotus are trademarks of International Business Machines Corporation. Microsoft is a trademark of Microsoft Corporation. MySpace is a trademark of MySpace, Inc. Wi-Fi is a trademark of the Wi-Fi Alliance. Windows Live is a trademark of Microsoft Corporation. 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 Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM 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 web sites (collectively the "Third Party Products and Services"). RIM 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 RIM 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, MERCHANTABLE 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 RIM 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 RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM 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 RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM 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 RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM 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 RIM OR ANY AFFILIATES OF RIM 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 RIM'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 RIM'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 RIM and RIM 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 RIM.

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 RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM 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.

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

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

Published in Canada