Administration Guide

BlackBerry Professional Software for Microsoft Exchange

Version 4.1 SP4

Contents

Managing user accounts

Add a user account

You must set up user accounts on your messaging server before you set up user accounts in the BlackBerry® Professional Software.

When you create a user account, you can assign an IT policy to control settings for the account. You can select one of the preconfigured IT policies, or create your own and select it. For more information about the IT policy rule settings, see the *Policy Reference Guide*.

1. On the server that hosts the BlackBerry Professional Software, on the taskbar, click **Start > BlackBerry Manager**.
2. In the BlackBerry Manager, click the **Home** tab.
3. In the **Account** section, click **Add New Users Wizard**.
4. In the user list, click the name of the user whose BlackBerry Professional Software user account you want to create.
5. Click **Select**.
6. Click **OK**.
7. On the Select IT policy screen, specify the IT policy setting for the user account.
8. On the Device Deployment screen, specify how to activate the BlackBerry device.
9. Click **Done**.

Add a user account manually

1. In the BlackBerry® Manager, click the **Users** tab.
2. In the **Account** section, click **Add Users**.
3. Click **Properties**.
4. Type or select the user account name.
5. Click **OK**.

Change user account information

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account that you want to update.
3. Make your changes.
4. Click **Apply**.

Remove a user account from the BlackBerry Professional Software

When you remove a user account from the BlackBerry® Professional Software, you can retain the BlackBerry configuration and privileges information in the user's mailbox so that you can add the user account again at a later time.

1. In the BlackBerry Manager, click the **Users** tab.
2. Right-click the user account that you want to remove.
3. Click **Yes**.
4. Choose whether to retain the BlackBerry Professional Software user account information in the user’s mailbox.

Managing BlackBerry devices

Change how to load existing email messages on to BlackBerry devices

By default, the BlackBerry® Professional Software loads up to 200 message headers from the previous 5 days on to BlackBerry devices. If you set the BlackBerry Professional Software to load both the email message body and message headers on to a BlackBerry device, the BlackBerry Professional Software can load up to 750 email messages from the previous 14 days for a user.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. In the **Send Headers Only** drop-down list, perform one of the following actions:
   - To load message headers only on to BlackBerry devices, click **True**.
   - To load both the message header and the message body on to BlackBerry devices, click **False**.
5. In the **Prepopulation By Message Age** field, type the number of previous days to load email messages for.
6. In the **Prepopulation By Message Count** field, type the maximum number of email messages to load.
7. Click **OK**.

Options for assigning a BlackBerry device to a user account

When you assign a BlackBerry® device to a user account, you associate the BlackBerry device with that user's messaging account and install service books on the BlackBerry device. You can assign a BlackBerry device to a user account using one of the following methods:

- over a wired connection to the server that hosts the BlackBerry® Professional Software; this option provides you with the greatest control over the timing of each BlackBerry device activation and over wireless network charges
- over the wireless network, using a wireless enterprise activation password; because users do not require a physical connection to your organization's network, this option provides a user with the most flexibility in how to activate the BlackBerry device
- over a wired connection to the BlackBerry® Desktop Manager on the user's computer; with this option, a user can activate the BlackBerry device at a convenient time, but the wireless network is available for use by messaging traffic

Assign a BlackBerry device to a user account using the BlackBerry Manager

You can use this method if you want to assign a BlackBerry® device to a user account and control the activation of the BlackBerry device before distributing it to the user.

1. Connect the BlackBerry device to the server that hosts the BlackBerry® Professional Software.
2. In the BlackBerry Manager, click the **Users** tab.
3. Right-click the user account that you want to assign the BlackBerry device to.
4. Click **Assign device**.
5. Click the BlackBerry device to assign to the user account.

6. Click **OK**.

Assigning a BlackBerry device to a user over the wireless network

You can assign a BlackBerry® device to a user over the wireless network by generating a wireless activation password, assigning the password to a user account, and sending the password to the user in an email message. The user types the password on the BlackBerry device to associate the BlackBerry device with the user's account on the messaging server.

You can use this method to assign either a new or a replacement BlackBerry device without requiring the user to have a wired connection to the network in your organization.

The wireless activation password is specific to a user account. You can customize the password type and length. The password expires after 48 hours by default or if the user types the password unsuccessfully 5 times on the BlackBerry device.

You can customize the default wireless activation message so that the message conforms to your organization's messaging policy. In your message, you can also provide support contact information.

Specify the wireless activation message and password settings

If a user receives a wireless activation password, you cannot generate a new password for the user until the active password expires. The password expires if the BlackBerry® device is not successfully activated in the BlackBerry® Professional Software after 48 hours by default, or if the user unsuccessfully types the password 5 times consecutively.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **General**.
4. Double-click **Custom activation email message**. Type the message.
5. Double-click **Auto-generated password length**. Type the password length.
6. In the **Auto-generated password type** drop-down list, click the password type.
7. Click **OK**.

Create and send a wireless activation message to a user

1. In the BlackBerry® Manager, click the **Users** tab.
2. Right-click a user account.
3. Perform one of the following actions:
   - To generate the password automatically and send it to the user in an email message, click **Generate and email activation password**. You are notified when the password is sent. Click **OK**.
   - To create your own activation password, in the **Set activation password** field, type and confirm the activation password. Provide the password to the user.

Assign a BlackBerry device to a user using the BlackBerry Desktop Manager

When the BlackBerry® Desktop Manager is installed on a user's computer, the user can control the initial activation of a BlackBerry device.

During the activation process, the BlackBerry Desktop Manager prompts the user to associate the BlackBerry device with the user's account on the messaging server and to generate an encryption key.

When the user completes the activation process, the BlackBerry® Professional Software loads messages, address book information, tasks, and memos on to the BlackBerry device.

1. Verify that the BlackBerry Desktop Manager is installed on the user’s computer.
2. Instruct the user to start the BlackBerry Desktop Manager and to connect the BlackBerry device to the computer.

   A message prompts the user to assign the BlackBerry device to the mail account. A second message prompts the user to generate an encryption key.

Protecting lost or stolen BlackBerry devices

You can use IT administration commands to immediately protect your organization's confidential data on BlackBerry® devices over the wireless network.

IT Admin command	Description
Set a Password and Lock Handheld	This command creates a new password and locks a lost BlackBerry device remotely. You can communicate the new password to the user when the user locates the BlackBerry device. When the user unlocks the BlackBerry device, the BlackBerry device prompts the user to accept or reject the password change.
Erase Data and Disable Handheld	This command remotely erases all user information and application data that the BlackBerry device stores. You can use this command to prepare a BlackBerry device for transfer between users in your organization or to protect a stolen BlackBerry device.

Protect a lost BlackBerry device

If a user misplaces a BlackBerry® device, you can help protect the data on the BlackBerry device by issuing commands to lock the BlackBerry device or to make it unavailable.

1. In the BlackBerry Manager, click the **Users** tab.
2. Right-click a user account.
3. Click **Set Password and Lock Handheld**.
4. In the **New Password** and **New Password Again** fields, type and confirm a password that is between 4 and 14 characters long.

   Warning: Do not use special characters when you create the password in case the BlackBerry device does not accept special characters.

5. To display owner information on the BlackBerry device, select the **Set user information also** check box. Type the required owner name and information.
6. Click **OK**.

Protect a stolen BlackBerry device

Contact your wireless service provider to turn off wireless service for the BlackBerry® device only after you send the Erase Data and Disable Handheld command to the BlackBerry device and verify that the BlackBerry device received the command.

1. In the BlackBerry Manager, click the **Users** tab.
2. Right-click a user account.
3. Click **Erase Data and Disable Handheld**.
4. Click **Yes**.

Prepare an existing BlackBerry device for distribution to a new user

To prepare an existing BlackBerry® device for distribution to a new user, delete the previous user's application data from the BlackBerry device and add or remove applications. To remove all applications and data from the BlackBerry device, return the BlackBerry device to its factory default state.

The process of removing all application data from the device can take longer if the Content Protection policy rule in the Security Policy Group is set to a value other than Default. Before you begin, you can turn off content protection. For more information, see the *Policy Reference Guide*.

1. Choose a method to delete the previous user's application data from the BlackBerry device and make the BlackBerry device unavailable to that user before assigning the BlackBerry device to a new user.

Task	Steps
Delete the previous user's application data over a physical connection to the BlackBerry Manager computer.	a. Connect the BlackBerry device to the server that hosts the BlackBerry® Professional Software. b. In the BlackBerry Manager, click the **Local Ports** tab. c. In the **Connection** list, click a connection. d. Click **Wipe Handheld File System**. e. Click **Yes**. f. If prompted, type the BlackBerry device password to complete the task. g. Assign the BlackBerry device to a user.
Return the BlackBerry device to the factory default state.	a. Connect the BlackBerry device to the server that hosts the BlackBerry Professional Software. b. In the BlackBerry Manager, click the **Local Ports** tab. c. In the **Connection** list, click a connection.

d. Click **Nuke Handheld**.

e. Click **Yes**.

f. Click **Load Device (Interactive)**.

g. Click a software configuration.

h. Click **OK**.

i. Complete the application loader wizard.

2. Replace the applications on the BlackBerry device.

   a. Connect the BlackBerry device to the host server for the BlackBerry Professional Software.

   b. In the BlackBerry Manager, click the **Local Ports** tab.

   c. In the **Connection** list, click a connection.

   d. Click **Load Device (Interactive)**.

   e. Click a software configuration.

   f. Click **OK**.

   g. In the Device Software Configuration Screen, clear the check boxes beside the applications that you want to remove, and select the check boxes beside the applications to install.

   h. Complete the application loader wizard.

Configuring organizer data synchronization

Organizer data includes items such as tasks, memos, and contacts. These are also referred to as personal information management items, or PIM items. You can change the settings for organizer data items so that the entries on users' BlackBerry® devices and the entries in the email application on their computers are the same.

You can set synchronization options globally for all user accounts, or you can set synchronization options for a specific user account. By default, wireless synchronization of organizer data for all user accounts is turned on. If you change the global settings, the new settings apply to any new user accounts that you set up. The new global settings are not applied to existing user accounts.

Customizing address book synchronization

Customize address book synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Address Book** section, in the **Synchronization Type** drop-down list, click one of the following synchronization options:
    - To synchronize address book data from the BlackBerry® Professional Software to the BlackBerry device only, click **Server to Device**.
    - To synchronize address book data from the BlackBerry device to the BlackBerry Professional Software only, click **Device to Server**.
    - To synchronize address book data from the BlackBerry device to the BlackBerry Professional Software and from the BlackBerry Professional Software to the BlackBerry device, click **Bidirectional**.
5. If you choose bidirectional synchronization, in the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
    - To specify that the BlackBerry Professional Software information overrules the BlackBerry device information, click **Server Wins**.
    - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off address book synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Address Book** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customize address book synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Address Book** section, in the **Synchronization Type** drop-down list, click one of the following synchronization options:
   - To synchronize address book data from the BlackBerry® Professional Software to the BlackBerry device only, click **Server to Device**.
   - To synchronize address book data from the BlackBerry device to the BlackBerry Professional Software only, click **Device to Server**.
   - To synchronize address book data from the BlackBerry device to the BlackBerry Professional Software and from the BlackBerry Professional Software to the BlackBerry device, click **Bidirectional**.
5. If you choose bidirectional synchronization, in the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
   - To specify that the BlackBerry Professional Software information overrules the BlackBerry device information, click **Server Wins**.
   - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off address book synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Address Book** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customizing task synchronization

Customize task synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Tasks** section, in the **Synchronization Type** drop-down list, click one of the following synchronization options:
   - To synchronize task data from the BlackBerry® Professional Software to the BlackBerry device only, click **Server to Device**.

- To synchronize task data from the BlackBerry device to the BlackBerry Professional Software only, click **Device to Server**.
- To synchronize task data from the BlackBerry device to the BlackBerry Professional Software and from the BlackBerry Professional Software to the BlackBerry device, click **Bidirectional**.

5. If you choose bidirectional synchronization, in the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
    - To specify that the BlackBerry Professional Software information overrules the BlackBerry device information, click **Server Wins**.
    - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off task synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Tasks** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customize task synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Tasks** section, in the **Synchronization Type** drop-down list, click one of the following synchronization options:
    - To synchronize task data from the BlackBerry® Professional Software to the BlackBerry device only, click **Server to Device**.
    - To synchronize task data from the BlackBerry device to the BlackBerry Professional Software only, click **Device to Server**.
    - To synchronize task data from the BlackBerry device to the BlackBerry Professional Software and from the BlackBerry Professional Software to the BlackBerry device, click **Bidirectional**.
5. If you choose bidirectional synchronization, in the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
    - To specify that the BlackBerry Professional Software information overrules the BlackBerry device information, click **Server Wins**.
    - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off task synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Tasks** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customizing memo synchronization

Customize memo synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Memos** section, in the **Synchronization Type** drop-down list, click one of the following synchronization options:
   - To synchronize memo data from the BlackBerry® Professional Software to the BlackBerry device only, click **Server to Device**.
   - To synchronize memo data from the BlackBerry device to the BlackBerry Professional Software only, click **Device to Server**.
   - To synchronize memo data from the BlackBerry device to the BlackBerry Professional Software and from the BlackBerry Professional Software to the BlackBerry device, click **Bidirectional**.
5. If you choose bidirectional synchronization, in the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
   - To specify that the BlackBerry Professional Software information overrules the BlackBerry device information, click **Server Wins**.
   - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off memo synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Memos** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customize memo synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Memos** section, in the **Synchronization Type** drop-down list, click one of the following synchronization options:
    - To synchronize memo data from the BlackBerry® Professional Software to the BlackBerry device only, click **Server to Device**.
    - To synchronize memo data from the BlackBerry device to the BlackBerry Professional Software only, click **Device to Server**.
    - To synchronize memo data from the BlackBerry device to the BlackBerry Professional Software and from the BlackBerry Professional Software to the BlackBerry device, click **Bidirectional**.
5. If you choose bidirectional synchronization, in the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
    - To specify that the BlackBerry Professional Software information overrules the BlackBerry device information, click **Server Wins**.
    - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off memo synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Memos** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customizing message filter synchronization

Customize message filter synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Message Filters** section, in the **Synchronization Type** drop-down list, accept the **Bidirectional** option.
5. In the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:

- To specify that the BlackBerry® Professional Software information overrules the BlackBerry device information, click **Server Wins**.
- To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.

6. Click **Apply**.

Turn off message filter synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Message Filters** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customize message filter synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Message Filters** section, in the **Synchronization Type** drop-down list, accept the **Bidirectional** option.
5. In the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
   - To specify that the BlackBerry® Professional Software information overrules the BlackBerry device information, click **Server Wins**.
   - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off message filter synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Message Filters** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customizing message setting synchronization

Customize message setting synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Message Settings** section, in the **Synchronization Type** drop-down list, accept the **Bidirectional** option.
5. In the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
    - To specify that the BlackBerry® Professional Software information overrules the BlackBerry device information, click **Server Wins**.
    - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off message setting synchronization for all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Global PIM Sync**.
4. In the **Message Settings** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Customize message setting synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Message Settings** section, in the **Synchronization Type** drop-down list, accept the **Bidirectional** option.
5. In the **Conflict Resolution** drop-down list, click one of the following conflict resolution options:
    - To specify that the BlackBerry® Professional Software information overrules the BlackBerry device information, click **Server Wins**.
    - To specify that the BlackBerry device information overrules the BlackBerry Professional Software information, click **Device Wins**.
6. Click **Apply**.

Turn off message setting synchronization for a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click the user account.
3. In the left pane, click **PIM Sync**.
4. In the **Message Settings** section, in the **Synchronization Enabled** drop-down list, click **False**.
5. Click **Apply**.

Turn off synchronization for contact pictures on a user account

By default, pictures that users add to contact entries in their address books are synchronized between their BlackBerry® devices and the email application on their computers. Users can add, delete, and change pictures in the email application on their computers or on their BlackBerry devices.

1. In the BlackBerry Manager, click the **Users** tab.
2. Click a user account.
3. In the **Service Control & Customization** section, click **Edit PIM Sync Field Mapping**.
4. In the **Desktop Field** column, click **Picture**.
5. In the **Device Field** column, in the drop-down list, click **<Clear>**.
6. Click **OK**.

Managing the wireless backup and recovery of organizer data

Automatic wireless backup is designed to back up user account settings and data from BlackBerry® devices to the BlackBerry® Professional Software automatically. You can use the automatic wireless backup feature to synchronize organizer data to new BlackBerry devices without affecting the performance of the messaging server. Automatic wireless backup is turned on by default when you add a user account to the BlackBerry Professional Software.

Turn off the wireless backup of organizer data for a user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click a user account.
3. In the left pane, click **PIM Sync**.
4. Click **Automatic Wireless Backup Enabled**.
5. In the drop-down list, click **False**.
6. Click **OK**.

Remove a user’s organizer data from the BlackBerry Professional Software

If the BlackBerry® Professional Software is not writing a user’s organizer data from the BlackBerry device to the BlackBerry Configuration Database correctly, the existing organizer data in the BlackBerry Professional Software might be corrupted. You can delete the existing organizer data from the BlackBerry Professional Software. This action forces the user's BlackBerry device to synchronize the user's current organizer data with the BlackBerry Professional Software over the wireless network.

1. In the BlackBerry Manager, click the **Users** tab.
2. Click a user account.
3. In the **Service Control & Customization** section, click **Clear PIM Sync Backup Data**.
4. Click **OK**.

Mapping address book fields

The fields for address book contacts can be customized in the email application on users' computers or on users' BlackBerry® devices. You can map up to four of these custom fields between BlackBerry devices and the email application on users' computers. You can create both global field mappings that apply to all user accounts and user field mappings that apply to specific user accounts.

When users request a remote address lookup in the global address list, the fields that you configure display on BlackBerry devices.

Map an address book field from the email application to an address book field on all BlackBerry devices

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Service Control & Customization** section, click **Edit PIM Sync Global Field Mapping**.
3. In the **Desktop Field** column, click a field.
4. In the **Device Field** column, in the drop-down list, click the address book field that you want to map to a field on BlackBerry devices.
5. Click **OK**.

Map user-defined address book fields to address book fields on all BlackBerry devices

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Service Control & Customization** section, click **Edit PIM Sync Global Field Mapping**.
3. In the **Desktop Field** column, click **User Defined String 1**.
4. In the **Device Field** column, in the drop-down list, click the address book field that you want to map to a field on BlackBerry devices.
5. Click **OK**.

Map an address book field in the email application to an address book field on a specific BlackBerry device

1. In the BlackBerry® Manager, click the **Users** tab.

2. Click a user account.
3. In the **Service Control & Customization** section, click **Edit PIM Sync Field Mapping**.
4. In the **Desktop Field** column, click a field.
5. In the **Device Field** column, in the drop-down list, click the address book field that you want to map to a field on the BlackBerry device.
6. Click **OK**.

Map user-defined address book fields to address book fields on a specific BlackBerry device

You can map up to four address book fields that users define in the email application to a specific field on the BlackBerry® device.

1. In the BlackBerry Manager, click the **Users** tab.
2. Click a user account.
3. In the lower pane, click **Service Control & Customization**.
4. Click **Edit PIM Sync Field Mapping**.
5. In the **Desktop Field** column, click **User Defined String 1**.
6. In the **Device Field** column, in the drop-down list, click the address book field that you want to map to a field on the BlackBerry device.
7. Click **OK**.

Configuring message handling

Managing email message filters

Email message filters define which email messages the BlackBerry® Professional Software redirects to BlackBerry devices. When a user receives an email message in the incoming message queue, the BlackBerry Professional Software applies filters to determine how to direct the message: forward, forward with priority, or do not forward to the user's BlackBerry device.

Email message filters that you configure in the BlackBerry Professional Software overrule the email message filters that users define using the BlackBerry® Desktop Manager or their BlackBerry devices.

You can create two types of email message filters in the BlackBerry Professional Software: global filters and user filters.

Global filters apply to all user accounts in the BlackBerry Professional Software. Users cannot view or change global filters. If you define global filters, inform users so that they understand why some of the email message filter rules that they create might not apply to incoming messages. If you change global filters, the BlackBerry Professional Software reads and applies the changes immediately.

User filters apply to specific user accounts in the BlackBerry Professional Software.

Create an email message filter that applies to all user accounts

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Global Filters**.
4. Double-click **Global Filter Definition**.
5. Click **New**.
6. In the **New Message Conditions** section, double-click **Filter Name**.
7. Type a name for the email message filter.
8. Configure the options for the email message filter.
9. Click **Action**.
10. Complete one of the following tasks:

Task	Steps
Create an email message filter that prevents the delivery of messages that satisfy the filter criteria.	In the drop-down list, click **Hold**.
Create an email message filter that forwards messages that satisfy the filter criteria.	a. In the drop-down list, click **Forward**. b. Double-click **Forwarding Options**. c. Perform one of the following actions: • To forward only the message headers to BlackBerry devices, select the **Header Only** check box.

- To forward messages to BlackBerry devices with priority status, select the **Level1 Notification** check box.
- To forward only the message headers of messages with priority status, select both the **Header Only** and **Level1 Notification** check boxes.

11. Click **OK**.
12. In the **Filter Name** list, click the email message filter that you created.
13. Click **Move Up** or **Move Down** to move the filter higher or lower in the list.

    The BlackBerry® Professional Software applies email message filters based on the order in which they appear. Organize the email message filters from the least restrictive to the most restrictive.
14. Click **OK**.

Turn on an email message filter that applies to all user accounts

The BlackBerry® Professional Software applies email message filters based on the order in which they appear.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Global Filters**.
4. Double-click **Global Filter Definition**.
5. In the **Filter Name** list, click an email message filter.
6. Click **Properties**.
7. In the **New Message Conditions** section, set **Enabled** to **True**.
8. Click **OK**.

Create an email message filter that applies to a specific user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click a user account.
3. In the left pane, click **Filters**.
4. Double-click **Filter Rules**.
5. Click **New**.
6. In the **New Message Conditions** section, double-click **Filter Name**.
7. Type a name for the new email message filter.
8. Configure the options for the email message filter.
9. Click **Action**.
10. Complete one of the following tasks:

Task	Steps
Create an email message filter that prevents the delivery of messages that satisfy the filter criteria.	In the drop-down list, click **Hold**.
Create an email message filter that forwards messages that satisfy the filter criteria.	a. In the drop-down list, click **Forward**. b. Double-click **Forwarding Options**. c. Perform one of the following actions: • To forward only the message headers to BlackBerry devices, select the **Header Only** check box. • To forward messages to BlackBerry devices with priority status, select the **Level1 Notification** check box. • To forward only the message headers of messages with priority status, select both the **Header Only** and **Level1 Notification** check boxes.

11. Click **OK**.
12. In the **Filter Name** list, click the email message filter that you created.
13. Click **Move Up** or **Move Down** to move the filter higher or lower in the list.

    The BlackBerry® Professional Software applies email message filters based on the order in which they appear. Organize the email message filters from the least restrictive to the most restrictive.

14. Click **OK**.

Turn on an email message filter that applies to a specific user account

The BlackBerry® Professional Software applies email message filters based on the order in which they appear.

1. In the BlackBerry Manager, click the **Users** tab.
2. Double-click a user account.
3. In the left pane, click **Filters**.
4. Double-click **Filter Rules**.
5. In the **Filter Name** list, click an email message filter.
6. Click **Properties**.
7. In the **New Message Conditions** section, set **Enabled** to **True**.
8. Click **OK**.

Managing how messages are forwarded to a user account

You can configure how the BlackBerry® Professional Software forwards email messages from the email application on users' computers to their BlackBerry devices. You can also manage individual user accounts, provide support to users, and control the size of the message queue and the load on the BlackBerry Messaging Agent to process forwarding requests. By default, email message forwarding is turned on for all user accounts.

Users can configure message forwarding settings on their BlackBerry devices or by using the BlackBerry® Desktop Manager. The settings that you define override the settings that users define.

Forward unfiltered email messages to a BlackBerry device

You can configure the BlackBerry® Professional Software to deliver incoming email messages to a user’s BlackBerry device when email message filter rules do not apply.

1. In the BlackBerry Manager, click the **Users** tab.
2. Double-click a user account.
3. In the left pane, click **Filters**.
4. In the **Default Action** section, set **Forward messages to BlackBerry device** to **True**.
5. Click **OK**.

Forward email messages from inbox subfolders to a BlackBerry device

You can specify the subfolders in the email application on a user's computer that the BlackBerry® Professional Software can forward email messages from. By default, the BlackBerry Professional Software forwards email messages from the inbox only.

1. In the BlackBerry Manager, click the **Users** tab.
2. Click a user account.
3. In the **Service Access** section, click **Choose Folders for Redirection**.
4. Click **Redirect the following selected folders**.
5. Select the check boxes beside the folders that you want to forward messages from.
6. Click **OK**.

Turn off synchronization for email messages sent from a BlackBerry device

You can configure email message synchronization so that messages that users send from their BlackBerry® devices are not synchronized in the email application on their computers.

1. In the BlackBerry Manager, click the **Users** tab.
2. Double-click a user account.
3. In the left pane, click **Redirection**.
4. In the **Message Forwarding** section, set **Do Not Save Sent Messages** to **True**.
5. Click **OK**.

Turn off email message forwarding to a BlackBerry device

You can prevent the BlackBerry® Professional Software from forwarding email messages to a BlackBerry device temporarily; for example, if a user is on vacation and does not want to receive messages during that time. When you turn off message forwarding for a user account, the user can send email messages but cannot receive them on the BlackBerry device. The user can later turn on message forwarding on the BlackBerry device manually.

1. In the BlackBerry Manager, click the **Users** tab.
2. Click a user account.
3. In the **Service Access** section, click **Disable Redirection**.

Managing wireless message reconciliation

Wireless message reconciliation synchronizes message status changes between the BlackBerry® device and the email application on users' computers. The BlackBerry® Professional Software reconciles message moves, deletions, and indicators for read and unread email messages. By default, wireless message reconciliation is turned on in the BlackBerry Professional Software and scheduled to occur every 15 minutes.

If you are concerned about high volumes of wireless network traffic, you can recommend that users limit their use of the Reconcile Now menu item in the message list on the BlackBerry device.

Turn off wireless message reconciliation

To reduce wireless network traffic or to manage individual user accounts, you can prevent the reconciliation of messages between BlackBerry® devices and the email application on users' computers. Users can reconcile their messages by connecting the BlackBerry device to the BlackBerry® Desktop Manager.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, in the **Wireless Message Reconciliation Enabled** drop-down list, click **False**.
5. Click **OK**.

Turn on reconciliation for permanently deleted email messages

Users can permanently delete email messages from the email application on their computers by pressing SHIFT+DELETE. If you want to remove permanently deleted email messages from users' BlackBerry® devices, you can turn on reconciliation for these messages. This feature also deletes from BlackBerry devices any email messages that users move into personal folders or archive in the email application on their computers.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, in the **Hard Deletes Reconciliation** drop-down list, click **True**.
5. Click **OK**.

6. On the server that hosts the BlackBerry® Professional Software, in the Microsoft® Windows® Services, restart the BlackBerry Dispatcher.

Managing message signatures and disclaimers

Add a signature to all messages sent from a specific user’s BlackBerry device

Users can change their message signatures either directly from their BlackBerry® devices or by using the BlackBerry® Desktop Manager. To enforce any signature format policies in your organization, you can add a signature to your organization's corporate disclaimer.

1. In the BlackBerry Manager, click the **Users** tab.
2. Double-click a user account.
3. In the left pane, click **Redirection**.
4. In the **Auto Signature** section, double-click the **Signature** field.
5. Type the signature that you want to appear in the messages that the user sends from the BlackBerry device.
6. Click **OK**.

Add a disclaimer to all messages sent from all BlackBerry devices

Users cannot change the disclaimers that you define.

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, perform one of the following actions:
    - To add a disclaimer before the message body, double-click **Prepended Disclaimer Text**.
    - To add a disclaimer after the user signature, double-click **Appended Disclaimer Text**.
5. Type the disclaimer.
6. Click **OK**.

Add a disclaimer to all messages sent from a specific user’s BlackBerry device

The user cannot change the disclaimers that you define.

1. In the BlackBerry® Manager, click the **Users** tab.
2. Double-click a user account.
3. Perform one of the following actions:
    - To add a disclaimer before the message body, in the **Messaging Options** section, double-click **Prepended Disclaimer Text**.
    - To add a disclaimer after the user signature, in the **Messaging Options** section, double-click **Appended Disclaimer Text**.
4. Type the disclaimer.
5. Click **OK**.

Specify conflict rules for multiple disclaimers

If you add different disclaimers for a single user and for all users, you can specify conflict rules to control how the BlackBerry® Professional Software applies the disclaimers.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, perform one of the following actions:
   - To specify conflict rules for prepended disclaimers, click **Prepended Disclaimer Conflict Rule**.
   - To specify conflict rules for appended disclaimers, click **Appended Disclaimer Conflict Rule**.
5. In the drop-down list, click a rule.
6. Click **OK**.

Sending notification messages to users

You can use the BlackBerry® Manager to send a notification message to an individual user or to all users. You can send notifications as email messages or as PIN messages. Because the messaging server does not process PIN messages, PIN notifications are useful for informing users about messaging server outages. BlackBerry devices do not apply filters to PIN messages.

When a user replies to a notification email message, the reply is addressed and sent to the account that you used to install the BlackBerry® Professional Software (for example, besadmin).

Send a notification message to all users

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Account** section, click **Send Message**.
3. Specify the message type.
4. Click **Next**.
5. Complete the instructions on the screen.

Send a notification message to specific users

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Account** section, click **Send Message**.
3. Specify the message type.
4. Click **Next**.
5. Select **Send to Selected Users**.
6. Click **Next**.
7. Select the check box for each user that you want to send the message to.
8. Click **Next**.

9. Complete the instructions on the screen.

Managing the incoming message queue

The incoming message queue stores incoming email messages that the BlackBerry® Professional Software will process and send to BlackBerry devices.

Delete messages for a specific user from the incoming message queue

To manage the size of the incoming message queue and to manage user accounts with high pending message counts, you can delete email messages for a specific user from the incoming message queue.

When you delete pending messages from the incoming message queue, the BlackBerry® Professional Software does not send the messages to the user's BlackBerry device. Messages still appear in the email application on the user's computer.

1. In the BlackBerry Manager, click the **Users** tab.
2. Click a user account.
3. In the **Service Control & Customization** section, click **Purge Pending Data Packets**.

If wireless calendar synchronization is turned on, the BlackBerry Professional Software deletes pending calendar messages from the incoming message queue and re-sends them later. The BlackBerry Professional Software does not delete IT policies and IT administration commands from the incoming message queue.

Monitoring messages sent from BlackBerry devices

If your organization requires you to retain a copy of all messages that users send from their BlackBerry® devices, use the auto BCC option in the BlackBerry® Professional Software to send copies of all messages to a specified recipient.

The auto BCC option populates the BCC field of the original message so that the message sender is aware of the blind carbon copy.

Configure a blind carbon copy on all messages

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. In the **Messaging Options** section, double-click **Auto BCC Addresses**.
5. Type the email addresses that you want to BCC on all messages. Separate email addresses with a semi-colon (;).
6. Click **OK**.

Configuring support for attachments

Configuring support for attachment file formats

The BlackBerry® Attachment Service in the BlackBerry® Professional Software uses distillers to convert attachments in supported file formats for display on the BlackBerry device. By default, all supported distillers are turned on.

You can add or turn off support for attachment file formats.

File formats that the BlackBerry Attachment Service supports

Format	Extension
Adobe® Acrobat® Versions 1.1, 1.2, 1.3, and 1.4	.pdf
ASCII text	.txt
audio	.amr, .wav, .mp3, .wma
WordPerfect® Versions 6.0, 7.0, 8.0, 9.0 (2000) and 10.0	.wpd
HTML	.htm, .html
images	.bmp, .gif, .jpeg, .jpg, .png, .tif, .tiff, .wmf
Microsoft® Excel® Versions 97, 2000, 2003 and XP	.xls
Microsoft® PowerPoint® Versions 97, 2000, 2003 and XP	.pps, .ppt
Microsoft® Word Versions 97, 2000, 2003 and XP	.doc, .dot
Rich Text Format	.rtf
ZIP archives	.zip

Turn off support for an attachment file format

Turn off a distiller to prevent users from viewing attachments in specific file formats. For example, if you turn off the .pdf distiller, users can no longer view .pdf file attachments on their BlackBerry® devices.

1. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start** > **BlackBerry Server Configuration**.
2. Click the **Attachment Server** tab.
3. In the **Distiller Settings** section, clear the check boxes beside the file formats that you want to turn off.
4. Click **OK**.
5. On the server that hosts the BlackBerry Professional Software, in the Microsoft® Windows® Services, restart the BlackBerry Attachment Service and the BlackBerry Dispatcher.

Add support for attachment file formats

If your email server connects to a document management system that renames file format extensions, add the extensions to the list of file formats to support arbitrary extensions.

1. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start > BlackBerry Server Configuration**.
2. Click the **Attachment Server** tab.
3. In the **Configuration Option** drop-down list, click **Connector Configuration**.
4. In the **Format Extension** field, type the file format extensions that you want to add.
5. Click **OK**.
6. On the server that hosts the BlackBerry Professional Software, in the Microsoft® Windows® Services, restart the BlackBerry Dispatcher.

Controlling the size of attachments that users can receive on their BlackBerry devices

By default, the BlackBerry® Attachment Service in the BlackBerry® Professional Software does not limit the file size of an attachment that is embedded in a message or retrieved through a link . The BlackBerry Professional Software sends data to the BlackBerry device in packets that are no larger than 64 KB; however, the BlackBerry Professional Software can send an unlimited number of packets.

To control attachment file size, you can specify a maximum file size for attachments. You can also configure the maximum dimension for images.

Suggested file sizes for attachments

File format	Suggested size
Adobe® Acrobat® Versions 1.1, 1.2, 1.3, and 1.4	less than 2000 KB
Microsoft® Excel® Versions 97, 2000, 2003, 2007, and XP	less than 2000 KB
Microsoft® PowerPoint® Versions 97, 2000, 2003, 2007, and XP	less than 2000 KB
Microsoft® Word Versions 97, 2000, 2003, 2007, and XP	less than 2000 KB
Corel® WordPerfect® Versions 6.0, 7.0, 8.0, 9.0 (2000), and 10.0	less than 2000 KB
ASCII text	less than 100 KB
HTML	less than 100 KB
ZIP archives	less than 2000 KB
images	less than 2000 KB
audio	less than 2000 KB
MP3	less than 2000 KB
Rich Text Format	less than 2000 KB

Configure the maximum file size for attachments

You can change the maximum file size of attachment file formats to control the amount of memory that the BlackBerry® Attachment Service in the BlackBerry® Professional Software uses during the attachment conversion process.

Consider changing the default configuration if the BlackBerry Attachment Service must respond to multiple users who request conversions for large or complex attachments (especially .pdf files and ASCII text files that are larger than 2 MB), or if it must respond to multiple users who request large or complex documents within the same period of time (0 to 10 minutes) while the BlackBerry Attachment Service processes large conversions.

1. On the server that hosts the BlackBerry Professional Software, on the taskbar, click **Start > BlackBerry Server Configuration**.
2. Click the **Attachment Server** tab.
3. In the **Distiller Settings** section, in the **Max. File Size (Kb)** column, click the value for the distiller that you want to change.
4. Type a value in kilobits.
5. Click **OK**.

Configure the maximum dimensions of image attachments that can display on BlackBerry devices

You can control the dimensions of image attachments that users can view on their BlackBerry® devices. By default, the BlackBerry Attachment Service sets a maximum width of 5000 pixels and a maximum height of 4000 pixels for image attachments.

1. On the server that hosts the BlackBerry® Professional Software, open the Registry Editor. On the taskbar, click **Start > Run**. Type **regedit**.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Research In Motion\BBAttachEngine\Distillers\LoadImageDistiller.
3. Right-click **MaxWidth**.
4. Click **Modify**.
5. Change the value to the maximum width in pixels.
6. Click **OK**.
7. Right-click **MaxHeight**.
8. Click **Modify**.
9. Change the value to the maximum height in pixels.
10. Click **OK**.
11. In the Microsoft® Windows® Services, restart the BlackBerry Attachment Service.

Change the maximum file size of attachments that users can send

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **Messaging**.
4. To change the maximum file size for a single attachment that users can send, in the **Messaging Options** section, in the **Maximum Upload Attachment Size** field, type a value that is between 1 and 3072.

5. To change the maximum file size for multiple attachments that users can send at one time, in the **Messaging Options** section, in the **Maximum Upload Total Attachment Size** field, type a value that is between 1 and 5120 and that is greater than the Maximum Upload Attachment Size.
6. Click **OK**.

Optimize the handling of file attachments

You can optimize the performance of the BlackBerry® Attachment Service by controlling how it retrieves, distills, and converts attachment data. Every attachment conversion process allocates memory when it starts, uses memory on conversion, and locally caches the Document Object Model, also referred to as the DOM. A larger cache size means that more memory is allocated to each running conversion process. The maximum file size of attachments affects the cached memory that the BlackBerry Attachment Service uses.

When the BlackBerry® Professional Software receives an attachment, the BlackBerry Attachment Service converts the attachment into a DOM and caches the DOM locally. By default, the BlackBerry Attachment Service maintains the cache for 25 minutes or until a new request exceeds the cache limit for that process. If the cache limit is exceeded, the BlackBerry Attachment Service deletes the document with the oldest time stamp in the cache. When users request to view an attachment on their BlackBerry devices, the BlackBerry Attachment Service accesses the DOM to process the request. The BlackBerry Attachment Service keeps all cached data in memory only and never caches the original document.

1. On the server that hosts the BlackBerry Professional Software, on the taskbar, click **Start > BlackBerry Server Configuration**.
2. Click the **Attachment Server** tab.
3. In the **Configuration Option** drop-down list, click **Attachment Server**.
4. Perform any of the following tasks:

Task	Steps
Prevent multiple requests for the same attachment from using the first cached copy of the attachment DOM in a conversion process for a user.	In the **Concurrent Caching** drop-down list, click **Disabled**. By default, the BlackBerry Attachment Service maintains the cache for 25 minutes or until a new request exceeds the cache limit for that process. If the cache limit is exceeded, the BlackBerry Attachment Service deletes the document with the oldest time stamp in the cache.
Configure the maximum number of converted documents that can be located in the document cache as DOM for an individual conversion process.	In the **Document Cache Size (docs)** field, type a value between 1 and 128.
Configure the number of conversion requests that the BlackBerry Attachment Service can process concurrently. Configure the value in relation to the available memory and competing services on the computer.	In the **Conversion Processes** field, type a value between 1 and 64.

Configure the number of documents that the BlackBerry Attachment Service can convert concurrently in a single conversion process. Use this setting to control thread saturation and to manage the BlackBerry Attachment Service workload with the Busy Threshold (seconds) setting.	In the **Max. Threads Per Process** field, type a value between 2 and 32.
Configure a limit for the time in which an application conversion process can reuse system resources to reclaim space and prevent failed processes from keeping memory.	In the **Recycle Time(s) (seconds)** field, type a time between 300 and 3600 seconds.
Configure the threshold to determine whether the BlackBerry Attachment Service is busy with conversions and should not accept new requests.	In the **Busy Threshold(s) (seconds)** field, type a time between 60 and 270 seconds.

5. Click **OK**.
6. On the server that hosts the BlackBerry Professional Software, in the Microsoft® Windows® Services, restart the BlackBerry Attachment Service.

Controlling BlackBerry device behavior using IT policy

You can use one or more IT policies to customize and control the functionality of BlackBerry® devices and the BlackBerry® Desktop Software. You can customize the settings in the IT policy rules for your environment. For more information, see the *Policy Reference Guide*.

Preconfigured IT policies in the BlackBerry Professional Software

The BlackBerry® Professional Software provides preconfigured IT policies that you can apply when you set up a user account. You can configure additional IT policy rules in these IT policies or change any settings that are shown in the following table.

IT policy rule	Default IT policy	Basic password security IT policy	Medium password security IT policy	Medium password security (disallow application download) IT policy	Advanced security IT policy	Advanced security (disallow application downloads) IT policy
Device-Only Items policy group						
Password Required	False	True	True	True	True	True
User Can Disable Password	True	False	False	False	False	False
Maximum Security Timeout	–	30 min.	10 min.	10 min.	10 min.	10 min.
Maximum Password Age	–	60 days	30 days	30 days	30 days	30 days
User Can Change Timeout	True	True	True	True	True	True
Password Pattern Checks	0	0	at lease 1 alpha and 1 numeric character	at lease 1 alpha and 1 numeric character	at lease 1 alpha and 1 numeric character	at lease 1 alpha and 1 numeric character
Enable Long-term Timeout	–	–	True	True	True	True
Password policy group						
Maximum Password History	–	–	6	6	6	6

IT policy rule	Default IT policy	Basic password security IT policy	Medium password security IT policy	Medium password security (disallow application download) IT policy	Advanced security IT policy	Advanced security (disallow application downloads) IT policy
Security policy group						
Disallow Third Party Application Download	—	—	—	True	True	True
Force Lock When Holstered	—	—	True	True	True	True
Content Protection Strength	—	—	—	—	Strong	Strong
Disable USB Mass Storage	—	—	—	—	True	True
External File System Encryption level	—	—	—	—	Encrypt to user password (excluding multimedia directories)	Encrypt to user password (excluding multimedia directories)
Bluetooth policy group						
Disable Serial Port Profile	—	—	—	—	True	True
Disable Discoverable Mode	—	—	True	True	True	True
Disable Address Book Transfer	—	—	—	—	True	True
Disable File Transfer	—	—	—	—	True	True
Require LED Connection Indicator	—	—	—	—	True	True
WLAN policy group						
WLAN Allow Handheld Changes	—	False	False	False	False	False

Enforcing IT policy changes over the wireless network

If your BlackBerry® Device Software supports it, you can immediately enforce IT policy rule additions, deletions, or modifications on BlackBerry devices. When the BlackBerry device receives an updated default IT policy or a new IT policy, the BlackBerry device and BlackBerry® Desktop Software apply the configuration changes.

The BlackBerry® Professional Software resends the IT policy to the BlackBerry device to update the BlackBerry device and BlackBerry Desktop Software behavior over the wireless network. By default, the BlackBerry Professional Software resends the IT policy to the appropriate BlackBerry devices within a short period of time after you update the IT policy.

You can also resend an IT policy to a BlackBerry device manually. You can configure the BlackBerry Professional Software to resend IT policies to BlackBerry devices at a scheduled interval, regardless of whether you have changed the IT policies.

Changing the default behavior of BlackBerry devices and BlackBerry Desktop Software in your organization

You can use either of the following methods to change the default behavior of BlackBerry® devices and BlackBerry® Desktop Software in your organization:

- set the values of IT policy rules in the default IT policy
- create a new IT policy, set its IT policy rule values, and assign one or more users or user groups to the new IT policy

When you set an IT policy rule to a True or False value, you prevent the user from selecting another value for a corresponding field on the BlackBerry device.

When you type a string that simultaneously turns on an IT policy rule and provides the parameters for its use, the user cannot change the value of a corresponding field on the BlackBerry device.

When you select a predefined, permitted value to assign to an IT policy rule, you restrict the values that the user can set for a corresponding field on the BlackBerry device.

A lock icon next to a field on the BlackBerry device indicates that its setting is controlled by the IT policy and the user cannot change it.

You can add a standard IT policy rule to, remove a standard IT policy rule from, or change the assigned value of a standard IT policy rule in an IT policy. You cannot add, remove, or change the values for a standard IT policy rule. You also cannot delete the standard IT policy rules.

You can add a new IT policy rule to, remove a new IT policy rule from, or change the assigned value of a new IT policy rule in an IT policy the same way that you change a standard IT policy rule in an IT policy.

Reverting to the default behavior of BlackBerry devices and BlackBerry Desktop Software

To revert to the default behavior that an IT policy rule customizes or controls, you can set that IT policy rule to Default, if that setting is available, or delete the value that you previously set.

If you assign users to a new IT policy, you can delete that IT policy to revert those users to the default behavior for all functionality on the BlackBerry® device and the BlackBerry® Desktop Software. The BlackBerry® Professional Software automatically reassigns the users to the Default IT policy and resends the default IT policy to the BlackBerry device, enforcing the settings in the Default IT policy.

Create an IT policy

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Common** section, click **Create IT Policy**.
3. Click **New**.
4. Double-click **IT Policy Name**.
5. Type a name for the new IT policy.
6. In the left pane, click a policy group.
7. In the right pane, double-click the IT policy rule.
8. Specify a value for the IT policy rule.
9. Continue with the remaining policy groups that you want to configure.
10. Click **Apply**.

Create an IT policy based on an existing IT policy

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Common** section, click **Create IT Policy**.
3. In the list of policies, click the IT policy that you want to base the new IT policy on.
4. Click **New Copy**.
5. Double-click **IT Policy Name**.
6. Type a name for the new IT policy.
7. In the left pane, click a policy group.
8. In the right pane, double-click the IT policy rule.
9. Specify a value for the IT policy rule.
10. Continue with the remaining policy groups that you want to configure.
11. Click **Apply**.

Change an IT policy rule setting in an IT policy

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Common** section, click **Create IT Policy**.
3. In the list of policies, click the IT policy that you want to change.
4. Click **Properties**.
5. In the left pane, click a policy group.

6. In the right pane, click the IT policy rule.
7. Specify a value for the IT policy rule.
8. Click **Apply**.

Assign an IT policy to a user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Click a user acount.
3. In the **IT Admin** section, click **Assign IT Policy**.
4. In the **IT Policy** list, select the IT policy that you want to assign.
5. Click **Next**.
6. Click **OK**.

Import IT policy definitions

The IT policy definitions file is an .xml file that adds new or updated IT policy rules to your existing set of IT policy rules. The downloaded file might include IT policy rules that control features or services that are not included in your version of the BlackBerry® Professional Software. Do not edit the IT policy definitions file.

1. Download the .xml file that contains IT policy rule definitions from www.blackberry.com .
2. Unzip the file to a temporary folder.
3. In the BlackBerry Manager, click the **Home** tab.
4. In the **Service Control & Customization** section, click **Import IT Policy Definitions**.
5. Click the .xml file that you downloaded.
6. Click **Open**.
7. Click **OK**.

Delete an IT policy

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **IT Policy**.
4. In the **IT Policy Administration** section, double-click **IT Policies**.
5. Click the IT policy that you want to delete.
6. Click **Remove**.
7. Click **Yes**.
8. Click **OK**.

Resend an IT policy to a BlackBerry device manually

1. In the BlackBerry® Manager, click the **Users** tab.
2. Click the user account that you want to resend the IT policy to.
3. In the **IT Admin** section, click **Resend IT Policy**.
4. Click **OK**.

Resend an IT policy to a BlackBerry device automatically

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **IT Admin**.
4. Double-click **Policy Resend Interval**.
5. Type the interval, in hours, for the automatic resends to occur.
6. Click **Apply**.

Customizing wireless access to enterprise applications

Specify the central push server

You can configure the BlackBerry® MDS Connection Service as a central push server. The central push server acts as a single host that receives content push requests from server-side applications that reside on a corporate application server, web server, or database. The central push server handles push requests and delivers data and updates from a server-side application to BlackBerry devices.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. In the **Common** section, click **Set as Push Server**.

Configuring how BlackBerry devices authenticate with content servers

If you configured the content servers in your environment to use an authentication protocol to authenticate the sources of data requests that they receive, you can specify how BlackBerry® devices authenticate with those content servers to obtain application data and updates.

Configure whether BlackBerry devices authenticate with content servers directly, or whether the BlackBerry MDS Connection Service authenticates with content servers on behalf of BlackBerry devices. If you configure BlackBerry devices to authenticate directly with content servers, users are prompted to provide login credentials every 30 minutes on their authenticated BlackBerry devices. If you do not configure an authentication method for BlackBerry MDS Connection Service connections, users are prompted only if the connection to the content server persists for more than 30 minutes.

Configure how BlackBerry devices authenticate with content servers

1. In the BlackBerry® Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **HTTP**.
4. Click **Support HTTP Authentication**.
5. In the drop-down list, perform one of the following actions:
   - If you want BlackBerry devices to authenticate with content servers directly, click **False**.
   - If you want the BlackBerry MDS Connection Service to store authentication information and perform HTTP authentication on behalf of BlackBerry devices, click **True**.
6. Double-click **Authentication Timeout**.
7. Type the length of time, in milliseconds, that you want authentication information for BlackBerry devices to remain valid on the content server. By default, the authentication timeout limit is 1 hour.
8. Click **Apply**.
9. If you set **Support HTTP Authentication** to **True**, configure the BlackBerry MDS Connection Service to authenticate on behalf of BlackBerry devices with content servers that use NTLM, Kerberos™, LTPA, or RSA® Authentication Manager.

Configure the BlackBerry MDS Connection Service to authenticate on behalf of BlackBerry devices with content servers that use NTLM

1. Navigate to <*drive*:>\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\<*Instance*>\config.
2. Configure the MdsLogin.conf file.

   For more information about the Java® Authentication and Authorization Service configuration file, visit http://java.sun.com/javase/6/docs/technotes/guides/security/jgss/tutorials/LoginConfigFile.html .

Configure the BlackBerry MDS Connection Service to authenticate on behalf of BlackBerry devices with content servers that use Kerberos

1. Navigate to <*drive*:>\Program Files\Research In Motion\BlackBerry Enterprise Server\MDS\Servers\<*Instance* >\config.
2. Configure the krb5.conf file.

   For more information about the Kerberos™ 5 configuration file, visit web.mit.edu/kerberos/www/krb5-1.3/krb5-1.3.3/doc/krb5-admin.html#krb5.conf .

Configure the BlackBerry MDS Connection Service to authenticate on behalf of BlackBerry devices with content servers that use LTPA

Turn on HTTP cookie storage to allow the BlackBerry® MDS Connection Service to authenticate with content servers that use LTPA authentication technology.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **HTTP**.
4. Click **Support HTTP Cookie Storage**.
5. In the drop-down list, click **True**.
6. Click **Apply**.

Configure the BlackBerry MDS Connection Service to authenticate on behalf of BlackBerry devices with the RSA Authentication Manager

When you turn on RSA® authentication, users must type their login credentials on their BlackBerry® devices before they can access intranet or Internet content. After the user is authenticated, if proxy authentication is configured, the BlackBerry device prompts the user to authenticate with the proxy server. By default, the BlackBerry device is authenticated for 24 hours, and an inactive BlackBerry device remains connected for 60 minutes.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **RSA Authentication**.
4. Click **Enable RSA Authorization Support**.

5. In the drop-down list, click **True**.
6. To specify the length of time that an authenticated BlackBerry device can remain connected to your organization's network before the user must log in again, double-click **RSA Authentication Timeout**.
7. Type a value, in minutes.
8. To specify the length of time that an inactive BlackBerry device can remain connected to your organization's network before the user must log in again, double-click **RSA Inactivity Timeout**.
9. Type a value, in minutes.
10. Click **Apply**.

Allowing push applications on external web servers to make trusted connections to the BlackBerry MDS Connection Service

You can configure the BlackBerry® MDS Connection Service to allow push applications on untrusted web servers to push content and updates to BlackBerry devices. If you want to establish trusted connections between external web servers and the BlackBerry MDS Connection Service, you must initialize a key store file (webserver.keystore) on the computer on which the BlackBerry MDS Connection Service is installed. This allows the BlackBerry MDS Connection Service to accept HTTPS connections from push applications on external web servers.

Your organization can trust a web server that hosts push applications but is external to your environment if the BlackBerry® Professional Software stores a certificate for it in the key store file. To trust external web servers, you can configure BlackBerry devices to use the BlackBerry MDS Connection Service to retrieve certificate information for web servers that host push applications, and then use the Java® keytool to install the certificates on the computer on which the BlackBerry MDS Connection Service is installed. Push applications can then use the trusted certificates to authenticate with the BlackBerry MDS Connection Service.

The BlackBerry MDS Connection Service supports LDAP and OCSP for certificate and certificate status retrieval, and SSL/TLS for authenticated connections using trusted certificates.

Permit BlackBerry devices to connect to untrusted external web servers

You can permit BlackBerry® devices to connect to untrusted web servers that push application content to BlackBerry devices.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **TLS/HTTPS**.
4. Perform one of the following actions:
   - To allow outgoing requests from the BlackBerry device that the BlackBerry MDS Connection Service encrypts with HTTPS, in the **Allow Untrusted HTTPS Connections** drop-down list, click **True**.
   - To allow outgoing requests from the BlackBerry device that the BlackBerry MDS Connection Service encrypts with TLS, in the **Allow Untrusted TLS Connections** drop-down list, click **True**.
5. Click **Apply**.

Configure the BlackBerry MDS Connection Service to retrieve certificates for web servers

Define a user name and password for the BlackBerry® MDS Connection Service to authenticate with LDAP servers on behalf of BlackBerry devices.

Do not change the default LDAP port parameters unless there is a port conflict with another service on the same computer. If you change port or host information, you must stop and restart the BlackBerry MDS Connection Service to reload the configuration information.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **LDAP**.
4. Set the LDAP server settings.
5. Click **Apply**.
6. Next, you configure the BlackBerry MDS Connection Service to retrieve the status of certificates for web servers.

Configure the BlackBerry MDS Connection Service to retrieve the status of certificates for web servers

You can configure the BlackBerry® MDS Connection Service to use the Online Certificate Status Protocol, which is also referred to as OCSP, to obtain the revocation status of digital security certificates.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **OCSP**.
4. Perform any of the following tasks:

Task	Steps
Set the BlackBerry MDS Connection Service to accept OCSP servers (responders) that the BlackBerry device specifies.	a. Click **Use Device Responders**. b. In the drop-down list, click **True**.
Set the OCSP handler to use the OCSP responder extension in a certificate.	a. If a certificate is present, click **Use Certificate Extension Responders**. b. In the drop-down list, click **True**.
Set the default URL of the OCSP responder.	a. Double-click **Default Responder URL**. b. Type the URL of the OCSP responder.
Set the URL of the server on which the certificate revocation list, or CRL, is located.	a. Double-click **Default CRL Server URL**. b. Type the URL of the CRL server.

5. Click **Apply**.
6. Next, you install retrieved certificates for web servers.

Install retrieved certificates for web servers

Use the Java® keytool to add a certificate for a web server to the BlackBerry® Professional Software key store and permit connections to the trusted web server. For more information about using the Java keytool, visit java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html .

1. Copy the certificate from a secure web site to a .cer file.
2. At a command prompt, browse to <*drive:*>\Program Files\Java\<*JRE version*>\bin.
3. Type **keytool -import -trustcacerts -alias <*alias_name*> -file <*cert_filename*> -keystore cacerts**.
4. Type the key store password.
5. At the prompt, click **Yes** to add the certificate to the key store.

Restricting user access to web content

You can create pull rules to restrict the web servers that users can access from applications on their BlackBerry® devices. You can use one of the following methods to specify which web servers you want users to be able to access:

- Turn on the pull authorization access control to restrict access to all types of web content, and then create pull rules to allow users to access certain web servers.
- Create pull rules to specify which web servers users cannot access from their BlackBerry devices.

Restrict web content requests from BlackBerry devices

Turn on pull authorization for the BlackBerry® MDS Connection Service to prevent users from accessing web content on their BlackBerry devices. If you want to provide access to certain web servers, you can create URL patterns and assign a pull rule that allows a user to access specified web servers.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **Access Control**.
4. Click **Pull Authorization**.
5. In the drop-down list, click **True**.
6. Click **Apply**.

Create URL patterns

You can create pull rules that specify the web servers that users can access from applications on their BlackBerry® devices. To create a pull rule, you must first create URL patterns that specify web servers. You assign these URL patterns to a pull rule that you create. You can then specify whether users are permitted or denied access to the specified web servers. After you create a pull rule, you must assign it to a user.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Access Control**.

4. Double-click **URL Patterns**.
5. Click **New**.
6. Double-click **URL pattern**.
7. Type the URL pattern of the web server that the pull rule will control access to.
8. Click **Service Name**.
9. In the drop-down list, click the service that the URL pattern is bound to.
10. Click **OK**.
11. Next, you create a URL pattern for each web server that you want to allow users to access. You then create a pull rule.

Create a pull rule

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Pull Rules**.
5. Click **New**.
6. Double-click **Name**.
7. Type a name for the pull rule.
8. Click **Apply**.
9. Next, you assign URL patterns to the pull rule.

Assign URL patterns to a pull rule

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **URL Pattern Rules**.
5. In the left pane, click the pull rule you created.
6. In the right pane, perform any of the following actions:
    - To prevent users from accessing a specified URL pattern, select the **Deny** check box.
    - To allow users to access a specified URL pattern, select the **Allow** check box.
7. Click **Apply**.
8. Next, you assign the pull rule to a user.

Assign a pull rule to a specific user

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.

3. In the left pane, click **Access Control**.
4. Double-click **User Rules**.
5. In the left pane, click a pull rule.
6. In the right pane, click a user.
7. Click **Apply**.

Restricting user access to media content

Using standard definitions for MIME media types, you can restrict the types of media—for example, audio and video—that the BlackBerry® MDS Connection Service can deliver to applications on the BlackBerry device.

For more information about MIME media types, visit www.iana.org .

Prevent users from accessing certain types of media

You can configure the BlackBerry® MDS Connection Service to prevent users from accessing every format of a media type (for example, video), or a specific format of a media type (for example, mp4), from the applications on the BlackBerry device.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. Click **Media Content Management**.
4. Double-click **Media Content Types**.
5. Click **New**.
6. In the **Media Content Type** field, type the media type and, optionally, a subtype, using standard definitions for MIME media types. Use the format *type/subtype*.
7. In the **Disallow content** drop-down list, click **True**.
8. Click **OK**.

Configure a size restriction for certain types of media

You can configure the BlackBerry® MDS Connection Service to prevent users from accessing certain types of media that exceed a maximum file size.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. Click **Media Content Management**.
4. Double-click **Media Content Types**.
5. Click **New**.
6. In the **Media Content Type** field, type the media type and, optionally, a subtype, using standard definitions for MIME media types. Use the format *<type>/<subtype>*.
7. In the **Maximum KB/Connection** field, type the maximum file size.
8. In the **Disallow content** drop-down list, click **False**.

9. Click **OK**.

Configuring how the BlackBerry MDS Connection Service manages web requests

The BlackBerry® MDS Connection Service handles requests for web content from applications on BlackBerry devices. You can configure how the BlackBerry MDS Connection Service manages these requests.

Configure the BlackBerry MDS Connection Service to manage HTTP cookie storage

By default, the BlackBerry® MDS Connection Service does not manage HTTP cookie storage. If the BlackBerry device requires JavaScript® support in its HTTP requests, cookies are processed on the BlackBerry device.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **HTTP**.
4. Click **Support HTTP Cookie Storage**.
5. In the drop-down list, click **True**.
6. Click **OK**.

Configure the timeout interval for HTTP connections with BlackBerry devices

You can specify the length of time, in milliseconds, that the BlackBerry® MDS Connection Service waits for a BlackBerry device to send data before it closes the HTTP connection with the BlackBerry device. The default interval is 120,000 milliseconds (2 minutes).

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **HTTP**.
4. Double-click **HTTP Device Connection Timeout**.
5. Type a number, in milliseconds.
6. Click **Apply**.

Configure the timeout interval for HTTP connections with web servers

You can specify the length of time, in milliseconds, that the BlackBerry® MDS Connection Service waits for a web server to send data before it closes the HTTP connection with the web server. The default interval is 120,000 milliseconds (2 minutes).

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **HTTP**.
4. Double-click **HTTP Server Connection Timeout**.
5. Type a number, in milliseconds.
6. Click **Apply**.

Configure the maximum number of HTTP redirections the BlackBerry MDS Connection Service supports

HTTP redirections occur when an application on the BlackBerry® device requests a web page from a web server and the web server returns a redirection status code that indicates a new URL for the web page. The default value is five redirections.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **HTTP**.
4. Double-click **Maximum Number of Redirects**.
5. Type a number.
6. Click **Apply**.

Restricting the push content that users can receive on their BlackBerry devices

By default, the BlackBerry® MDS Connection Service delivers all push requests from server-side push applications to applications on BlackBerry devices. As a result, users are able to receive application data and updates without having to request the content.

If you want to configure your environment so that only certain server-side push applications can send push requests to BlackBerry devices, you can turn on push authentication to restrict the BlackBerry MDS Connection Service from delivering push requests, then you can create push initiators that specify which server-side applications are permitted to send push requests to BlackBerry devices. You can also create and assign push rules to users to specify which users can receive push requests.

Restrict push applications from sending data to BlackBerry devices

You can turn on push authentication to allow only authenticated push applications to send push requests to applications on BlackBerry® devices.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **Access Control**.
4. Click **Push Authentication**.
5. In the drop-down list, click **True**.
6. Click **Apply**.
7. Next, to authenticate and allow certain server-side push applications to send push requests to BlackBerry devices, create push initiators.

Create a push initiator for a push application

A push initiator specifies which server-side push application is authenticated and allowed to send push requests to applications on BlackBerry® devices when you have push authentication turned on for the BlackBerry MDS Connection Service. Depending on your development environment, you can configure multiple server-side push applications to use the same push initiator (that is, to use the same push principal name and password).

1. In the BlackBerry Manager, click the **Home** tab.

2. Click **Edit Global Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Initiators**.
5. Click **New**.
6. Double-click **Push Principal Name**.
7. Type the name of the server-side application that you want to allow to send push requests to BlackBerry devices.
8. Double-click **Credentials**.
9. Type the password for the server-side push application.

   Make sure that the value of the authorization HTTP header in a push request from a server-side push application matches the push principal name and password that you specified for the push initiator.
10. Click **Apply**.
11. Next, you create a push initiator for each server-side push application that you want to allow to send push requests to BlackBerry devices. If you want to restrict which users can receive push requests from authenticated push applications, turn on push authorization.

Turn on push authorization

After you turn on push authentication and create push initiators to specify which push applications can send push requests, you can create pull rules to specify which users are allowed to receive push requests. Turn on push authorization for the BlackBerry® MDS Connection Service to allow the BlackBerry MDS Connection Service to apply the push rules that you create.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **Access Control**.
4. Click **Push Authorization**.
5. In the drop-down list, click **True**.
6. Click **Apply**.
7. Next, you create a push rule.

Create a push rule

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Rules**.
5. Click **New**.
6. Double-click **Name**.
7. Type a name for the push rule.
8. Click **Apply**.
9. Next, you assign push initiators to the push rule.

Assign push initiators to a push rule

Before you begin, you must create push initiators to authenticate certain push applications.

1. In the BlackBerry® Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. In the left pane, click **Access Control**.
4. Double-click **Push Initiator Rules**.
5. In the left pane, click a push rule.
6. In the right pane, select the push initiators for the applications that you want to assign to the push rule.
7. Click **Apply**.
8. Next you, assign the push rule to each user account.

Assign a push rule to a specific user account

Before you begin, create a push rule and assign push initiators to the push rule.

1. In the BlackBerry® Manager, click **Edit Global Properties** .
2. In the left pane, click **Access Control**.
3. Double-click **User Rules**.
4. In the left pane, click a push rule.
5. In the right pane, click a user account.
6. Click **OK**.

Encrypt push requests that push applications send to BlackBerry devices

You can configure the BlackBerry® MDS Connection Service to encrypt the push requests that server-side push applications send to BlackBerry devices using SSL or TLS. By default, the BlackBerry MDS Connection Service does not encrypt the push requests that server-side push applications send.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **Access Control**.
4. Click **Push Encryption**.
5. In the drop-down list, click **True**.
6. Click **Apply**.

Managing push application requests

The BlackBerry® MDS Connection Service receives push application requests from server-side push applications, then delivers these requests to applications on BlackBerry devices. You can control how the BlackBerry MDS Connection Service processes, stores, and delivers push application requests.

Specify device ports for application-reliable push requests

Application developers can design custom BlackBerry® Java® Applications to handle application-reliable push requests. When a BlackBerry Java Application receives an application-reliable push request, it returns a delivery confirmation to the BlackBerry MDS Connection Service, which delivers the confirmation to the server-side push application. The application's developer or the application's documentation can provide information about the ports that are defined for BlackBerry Applications that support application-reliable push requests. You can then specify the device ports that each BlackBerry Java Application uses to listen for application-reliable push requests.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **Push/PAP**.
4. Double-click **Device Ports Enabled for Reliable Pushes**.
5. Type the device port number. Use commas to separate multiple port numbers.
6. Click **Apply**.
7. Click **Restart Service**.

Store push application requests in the BlackBerry Configuration Database

To manage memory and system resources in your environment, you can configure the BlackBerry® MDS Connection Service to store Password Authentical Protocol and RIM® push requests in the BlackBerry Configuration Database. You can configure storage settings for the BlackBerry Configuration Database.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **Push/PAP**.
4. Click **Store Push Submissions**.
5. In the drop-down list, click **True**.
6. Click **Apply**.
7. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start > Administrative Tools > Services**.
8. Right-click **BlackBerry MDS Connection Service**.
9. Click **Restart**.
10. Next, you configure storage settings for push requests stored in the BlackBerry Configuration Database.

Configure storage settings for push requests stored in the BlackBerry Configuration Database

You can manage your system resources by configuring storage settings for push requests stored in the BlackBerry® Configuration Database.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Global Properties**.
3. Click **Push Control**.
4. Double-click **Maximum Stored Push Messages**.
5. Type the maximum number of push requests that can be stored in the BlackBerry Configuration Database.

6. Double-click **Maximum Push Message Age**.
7. Type the maximum length of time, in minutes, to store a push request before the BlackBerry® Professional Software purges it from the BlackBerry Configuration Database.
8. Click **Apply**.
9. On the server that hosts the BlackBerry Professional Software, on the taskbar, click **Start > Administrative Tools > Services**.
10. Right-click **BlackBerry MDS Connection Service**.
11. Click **Restart**.

Configure the maximum number of active connections that the BlackBerry MDS Connection Service can process

You can configure the maximum number of push connections that the BlackBerry® MDS Connection Service can process at the same time. When this limit is reached, the BlackBerry MDS Connection Service queues the remaining push connections.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **Push/PAP**.
4. Double-click **Maximum number of Active Connections**.
5. Type a number.
6. Click **OK**.
7. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start > Administrative Tools > Services**.
8. Right-click **BlackBerry MDS Connection Service**.
9. Click **Restart**.

Configure the maximum number of queued connections that the BlackBerry MDS Connection Service can process

The BlackBerry® MDS Connection Service queues push connections when the number of connections reaches the limit that you specify. You can configure the maximum number of push connections that the BlackBerry MDS Connection Service can queue. When this limit is reached, the BlackBerry MDS Connection Service sends a "service unavailable" message to BlackBerry devices that receive push requests.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. Click **Push/PAP**.
4. Double-click **Maximum number of Queued Connections**.
5. Type a number.
6. Click **OK**.
7. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start > Administrative Tools > Services**.
8. Right-click **BlackBerry MDS Connection Service**.
9. Click **Restart**.

Clear the push request queue manually on a Microsoft SQL Server

An automated process runs daily to clear the push request queue on a Microsoft® SQL Server™. You can also clear the push request queue manually by running the RIMPurgeMDSMsg<*database_name*> process from your Microsoft SQL Server management console.

1. Perform one of the following actions:
   - If you are using Microsoft SQL Server Enterprise Manager, navigate to Console Root\Microsoft SQL Servers\SQL Server Group\<*BlackBerry Configuration Database server*>\Management\SQL Server Agent\Jobs.
   - If you are using Microsoft SQL Server Management Studio, navigate to SQL Server Agent\Jobs.
2. Start the RIMPurgeMDSMsg<*database_name*> process.

Configuring how the BlackBerry MDS Connection Service connects to BlackBerry devices

Specify the maximum amount of data that the BlackBerry MDS Connection Service can send to BlackBerry devices

1. In the BlackBerry® Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **General**.
4. Double-click **Maximum KB/Connection**.
5. Type a number, in kilobytes.
6. Click **Apply**.

Specify the BlackBerry MDS Connection Service flow control timeout limit

You can specify how long the BlackBerry® MDS Connection Service waits for acknowledgement from a BlackBerry device before it discards pending content for that BlackBerry device.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **General**.
4. Double-click **Flow Control Timeout**.
5. Type a number, in milliseconds.
6. Click **Apply**.

Specify the thread pool size of the BlackBerry MDS Connection Service

Make sure there is adequate system memory to support the thread pool size that you want to specify. You can specify the maximum number of threads that the BlackBerry® MDS Connection Service can process at the same time before it rejects processing requests.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **General**.

4. Double-click **Thread Pool Size**.
5. Type a number between 100 and 1000.
6. Click **Apply**.

Specify the maximum number of persistent socket connections

Make sure there is adequate system memory to support the value that you want to specify. You can specify the maximum number of persistent socket connections that can be open at the same time between BlackBerry® devices and the BlackBerry MDS Connection Service. The BlackBerry MDS Connection Service rejects processing requests from BlackBerry devices when the number of persistent socket connections reaches the maximum number that you specify.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **General**.
4. Double-click **Maximum Simultaneous Persistent Sockets**.
5. Type a number between 100 and 3500.
6. Click **Apply**.

Specify the port on which the web server listens for push application requests

You can specify the port on which the web server listens for HTTP and HTTPS requests from server-side push applications. Change the default port parameters only if there is a port conflict with another service on the same computer.

1. In the BlackBerry® Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **General**.
4. Perform one of the following actions:
   - To specify the port for HTTP requests from push applications, double-click **Web Server Listen Port**.
   - To specify the port for HTTPS requests from push applications, double-click **Web Server SSL Listen Port**.
5. Type the port number.
6. Click **Apply**.
7. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start** > **Administrative Tools** > **Services**. Right-click **BlackBerry MDS Connection Service**. Click **Restart**.
8. Notify any push application developer in your environment that you have changed the port number.

Specify how often the BlackBerry MDS Connection Service polls for configuration information

You can specify how often the BlackBerry® MDS Connection Service polls the BlackBerry Configuration Database for changes to the BlackBerry MDS Connection Service administrative settings. The default interval is 5 minutes.

1. In the BlackBerry Manager, click the **Connection Service** tab.
2. Click **Edit Connection Service Properties**.
3. In the left pane, click **General**.
4. Double-click **Admin Configuration Cycle Timer**.

5. Type a number, in minutes.
6. Click **Apply**.

Managing BlackBerry Device Software and wireless applications

Making BlackBerry Device Software or applications available to users

You can make BlackBerry® Device Software or applications available to users in the following ways:

- install BlackBerry Device Software on or add applications to a BlackBerry device that is connected to the server that hosts the BlackBerry® Professional Software
- make the BlackBerry Device Software and applications available so that a user can install the software and add applications using the application loader tool

You must make the BlackBerry Device Software and applications available in a shared network location.

You can create a software configuration to define how the BlackBerry Professional Software delivers the applications to BlackBerry devices, and optionally, which applications can be added to certain BlackBerry devices.

Share the network folder

1. On the server that hosts the BlackBerry® Professional Software, navigate to the following location: *drive:*>\Program Files\Common Files\Research In Motion.
2. Right-click the **Research In Motion** folder.
3. Click **Sharing and Security**.
4. On the **Sharing** tab, select **Share this folder**.
5. Click **Permissions**.
6. Set the **Read** permission to **Allow**.
7. Click **OK**.
8. Create the following network path: **<*drive:*>\Program Files\Common Files\Research In Motion\Shared\Applications**.
9. Next, you add the required applications to the shared network folder.

Install the BlackBerry Device Software files in the shared network folder

1. Obtain the BlackBerry® Device Software installation file from your wireless service provider.
2. Copy the BlackBerry Device Software installation file to the shared network folder.
3. In the folder, double-click the .exe file.
4. Complete the installation.
5. Verify that the files are located in <*drive*:>\Program Files\Common Files\Research In Motion\Shared\Loader Files.
6. Next, you add any additional applications to the shared network folder and then index the applications.

Add the application files to the shared network folder

Add only .alx and .cod files to the shared network folder.

1. Navigate to *drive*:>\Program Files\Common Files\Research In Motion\Shared\Applications.
2. Copy the .alx and .cod files for the application to an application folder in the **Applications** folder, preserving the structure of the application.
3. Next, you index the application files.

Indexing applications on a network drive

You create a software index for the applications that you add to the network drive so that the application loader tool and software configurations can locate the applications that are available to add to BlackBerry® devices. When you create a software index, the BlackBerry® Professional Software creates a specification.pkg file and a PkgDBCache.xml index file for each application.

The index files are created automatically for recent versions of the BlackBerry® Device Software. Check your application folder for the .xml file and .pkg files.

Create a software index for the applications in the shared network folder

1. Open a command prompt window. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start > Run**. Type **cmd**.
2. At the command prompt, type **cd <*drive*>:\Program Files\Common Files\Research In Motion\Apploader** .
3. Type **loader.exe /index**.

   The application loader tool builds the software index structure in the network drive and adds any missing index files.
4. Type **exit**.
5. Verify that the folder for the application now contains the following two files: .xml file and .pkg file.
6. Next, you create the new software configuration.

Reindex the applications in the shared network folder

If you change an .alx file after you create an index for the applications in the shared network folder, you must reindex the applications.

1. At the command prompt, navigate to **<*drive*>:\Program Files\Common Files\Research In Motion\Apploader**.
2. Type **loader.exe /reindex**.

   The application loader updates the software index structure in the shared network folde and adds any missing index files.
3. Next, you create a software configuration.

Defining software configurations

A software configuration points to the shared network location of the BlackBerry® Device Software and applications that you plan to install on a specific BlackBerry device model. Using a software configuration, you can remotely add and remove third-party applications using the application loader tool on BlackBerry devices that are connected to computers running the BlackBerry® Desktop Manager.

You create a software configuration for each BlackBerry device model in your organization. When you create a software configuration, you can define application control policies to specify the resources that applications can access on BlackBerry devices from behind your organization's firewall. You can also use application control policies to monitor the installed applications and to make sure that certain applications remain installed on, or are removed from, BlackBerry devices.

After you create a software configuration and define any application control policies, you assign the software configuration to a user account to apply the configuration attributes.

Create a software configuration

If you have more than one BlackBerry® device model in your organization, you must create a different software configuration for each model.

1. In the BlackBerry Manager, click the **Software Configurations** tab.
2. In the **Common** section, click **Add New Configuration**.
3. Verify that you completed the prerequisite tasks outlined in the Add New Configuration screen. Click **OK**.
4. In the **Configuration Name** field, type a name.
5. In the **Configuration Description** field, type a description.
6. Click **Change**.
7. Type the location of the BlackBerry® Device Software or applications.
8. Click **OK**.
9. In the **Application Name** list, select the check box beside the BlackBerry device models that you want to configure the BlackBerry Device Software or applications for.
10. Select or clear the check box for each application that you want to install or remove.
11. In the **Delivery** drop-down list, click the delivery method.
12. In the **Policy** list, click the Application Control policy rule for the application.

    You can click **Policies** to define new application control policy rules for an application.
13. Click **OK**.

Create a software configuration based on an existing software configuration

1. In the BlackBerry® Manager, click the **Software Configurations** tab.
2. Click a software configuration.
3. Click **Copy Configuration**.
4. Double-click the copied software configuration.
5. In the **Configuration Name** field, rename the software configuration.
6. Change the software configuration properties as necessary.
7. Click **OK**.

Applying application control policies

After you create a software configuration, you can configure an application control policy to control or change the behavior of an application on the BlackBerry® device. For example, you can use an application control policy to specify that an application is required on the BlackBerry device.

For more information about application control policies, see the *Policy Reference Guide*.

Define an application control policy

1. In the BlackBerry® Manager, click the **Software Configurations** tab.
2. In the **Common** section, click **Manage Application Policies**.
3. Click **New**.
4. Type a new policy name.
5. Customize the application control policy rules.
6. Click **Apply**.
7. Next, you assign the application control policy to an application.

Assign an application control policy to an application

1. In the BlackBerry® Manager, click the **Software Configurations** tab.
2. In the **Configuration Name** list, click a software configuration.
3. In the **Common** section, click **Edit Configuration**.
4. Click the application that you want to assign the application control policy to.
5. In the **Policy** drop-down list, click an application control policy.
6. Perform one of the following actions:
   - To assign an application control policy to all applications that are not currently assigned to an application control policy, click an application control policy at the application software level.
   - To assign the application control policy that is assigned at the application software level, click **<default>**. An asterisk is added to the policy name.
   - To assign the default application control policy rules that are preconfigured on the BlackBerry device, click **<none>**.
7. Click **Apply**.

Assign a software configuration to a user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Right-click the user account that you want to assign the software configuration to.
3. Click **Assign Software Configuration**.
4. Click the software configuration that you want to assign.

5. Click **OK**.

Send an application to a BlackBerry device over the wireless network

The wireless download to BlackBerry® devices can take up to four hours to start.

1. In the BlackBerry Manager, click the **Software Configurations** tab.
2. Click a software configuration.
3. Click **Edit Configuration**.
4. Click the application that you want to send over the wireless network.
5. In the **Delivery** drop-down list, click **Wireless**.
6. To make sure that the application remains installed on a BlackBerry device, set the **Disposition** to **Required**.
7. Click **OK**.

Load the BlackBerry Device Software or applications on to a BlackBerry device using the BlackBerry Manager

If you want to install BlackBerry® Device Software or applications on BlackBerry devices before you distribute the BlackBerry devices to users, you can use the BlackBerry Manager to complete the installation process.

1. Connect the BlackBerry device to the server that hosts the BlackBerry® Professional Software.
2. In the BlackBerry Manager, click the **Software Configurations** tab.
3. Click a software configuration.
4. Click **Edit Configuration**.
5. Click the application that you want to install.
6. In the **Delivery** drop-down list, click **Wireline only**.
7. To make sure that the application remains installed on a BlackBerry device, set the **Disposition** to **Required**.
8. Click **OK**.

Managing applications on BlackBerry devices

Change an application control policy

1. In the BlackBerry® Manager, click the **Software Configurations** tab.
2. Click **Manage Application Policies**.
3. Click the application control policy.
4. Click **Properties**.
5. Change the properties of the application control policy.
6. Click **OK**.

Remove applications from BlackBerry devices over the wireless network

You can remove applications from BlackBerry® devices over the wireless network. The BlackBerry® Professional Software might take up to four hours to remove an application from a BlackBerry device.

1. In the BlackBerry Manager, click the **Software Configurations** tab.
2. Click **Manage Application Policies**.
3. Double-click an application control policy.
4. In the **Disposition** drop-down list, click **Disallowed**.
5. Click **OK**.

Upgrade an application on a BlackBerry device over the wireless network

You can upgrade applications on BlackBerry® devices over the wireless network. The BlackBerry® Professional Software might take up to four hours to upgrade an application on a BlackBerry device. If the **Disposition** is set to **Required** in the application control policy, the application upgrade is also sent over the wireless network.

1. In the network drive, add or upgrade the application.
2. Reindex the application.

Remove a software configuration from a user account

1. In the BlackBerry® Manager, click the **Users** tab.
2. Right-click the user account that you want to delete the software configuration from.
3. Click **Assign Software Configuration** .
4. Click **<none>**.
5. Click **OK**.

Controlling the BlackBerry environment

Protecting BlackBerry device data in transit

From the time that the user sends data (for example, an email message) from the BlackBerry® device until the BlackBerry® Professional Software receives the data, and from the time that the BlackBerry Professional Software receives and forwards data to the user until the user receives the data on the BlackBerry device, standard BlackBerry encryption uses a symmetric algorithm to protect the data.

By default, the BlackBerry Professional Software uses both the Triple Data Encryption Standard (Triple DES or 3DES) and the Advanced Encryption Standard (AES) algorithms to encrypt all communication with BlackBerry devices.

Encryption algorithm	Description	Notes
Triple DES	enables the use of the Triple DES algorithm to encrypt and decrypt all data communication between the BlackBerry Professional Software and all BlackBerry devices	provides Triple DES encryption only on BlackBerry devices
AES	enables the use of the AES algorithm to encrypt and decrypt all data communication between the BlackBerry Professional Software and all BlackBerry devices	• uses a longer encryption key, which is designed to provide a better combination of security and performance than Triple DES • helps to protect user data and encryption keys from traditional and side-channel attacks
Triple DES and AES	provides Triple DES encryption on BlackBerry device that do not support AES (BlackBerry devices that run BlackBerry® Device Software versions earlier than 4.0)	provides the default encryption method

Change the encryption algorithm

If you change the encryption algorithm, you must reactivate all of the BlackBerry® devices in your organization to enable users to send and receive messages on their BlackBerry devices again.

1. In the BlackBerry Manager, click the **Home** tab.
2. Click **Edit Server Properties**.
3. In the left pane, click **General**.
4. In the **Security** section, click **Encryption Algorithm**.
5. In the drop-down list, click the encryption type that you want to use.
6. Click **OK**.

Managing client access license keys

Client access license keys, or CAL keys, control the number of user accounts that can exist in the BlackBerry® Professional Software at the same time. If you exceed the number of permitted user accounts, the BlackBerry Manager notifies you that you require more CAL keys.

The BlackBerry Professional Software supports a maximum of 30 user accounts, regardless of the number of user accounts that your CAL key or combination of CAL keys supports.

Add a CAL key

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Account** section, click **License Management**.
3. Type the new information for the CAL key.
4. Click **Add License**.
5. Click **Close**.

Copy a CAL key to a text file

1. In the BlackBerry® Manager, click the **Home** tab.
2. In the **Account** section, click **License Management**.
3. Right-click the CAL key that you want to copy.
4. Click **Copy Key**.
5. Open a text editor.
6. Paste the CAL key into the file.
7. Save the file.

Remove a CAL key

You can remove a CAL key only if you have more than one. You must have a CAL key that supports the BlackBerry® Professional Software user accounts in your organization.

1. In the BlackBerry Manager, click the **Home** tab.
2. In the **Account** section, click **License Management**.
3. Right-click the CAL key that you want to delete.
4. Click **Remove License Key**.

Removing the BlackBerry Professional Software from the host server

Remove the BlackBerry Professional Software from the host server

1. On the server that hosts the BlackBerry® Professional Software, on the taskbar, click **Start** > **Settings** > **Control Panel** > **Add/ Remove Programs**.
2. Click **BlackBerry Professional Software**.
3. Click **Remove**.
4. Click **Yes**.

Remove the registry entries from the host server

1. On the server that you removed the BlackBerry® Professional Software from, open the Registry Editor. On the taskbar, click **Start** > **Run**. Type **regedit**.
2. Delete the following registry keys:

Location	Key
HKEY_LOCAL_MACHINE\SOFTWARE	Research In Motion
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services	BBAttachServer and any keys starting with “BES” or “BlackBerry”
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services	BBAttachServer and any keys starting with “BlackBerry”
HKEY_LOCAL_MACHINE\SYSTEM \ControlSet00n\Services	BBAttachServer and any keys starting with “BlackBerry”
HKEY_CURRENT_USER\SOFTWARE	Research In Motion
HKEY_CURRENT_USER\SOFTWARE \Microsoft\Windows NT\ CurrentVersion\Windows Messaging SubSystem\Profiles	any keys named BlackBerryServer, BlackBerry Manager, or listed as the name of your BlackBerry Professional Software
HKEY_USERS\.DEFAULT\SOFTWARE	Research In Motion
HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows \CurrentVersion\App Paths	BESManmmc.dll

Legal notice

The BlackBerry device and/or associated software are protected by copyright, international treaties, and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D445,428; D433,460; D416,256. Other patents are registered or pending in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

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

This document might contain references to third-party sources of information, hardware or software, products or services and/or third-party web sites (collectively the "Third-Party Information"). RIM does not control, and is not responsible for, any Third-Party Information, including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third-Party Information. The inclusion of Third-Party Information in this document does not imply endorsement by RIM of the Third-Party Information or the third party in any way. Installation and use of Third-Party Information with RIM's products and services may require one or more patent, trademark, or copyright licenses in order to avoid infringement of the intellectual property rights of others. Any dealings with Third-Party Information, including, without limitation, compliance with applicable licenses and terms and conditions, are solely between you and the third party. You are solely responsible for determining whether such third-party licenses are required and are responsible for acquiring any such licenses relating to Third-Party Information. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use Third-Party Information until all such applicable licenses have been acquired by you or on your behalf. Your use of Third-Party Information shall be governed by and subject to you agreeing to the terms of the Third-Party Information licenses. Any Third-Party Information that is provided with RIM's products and services is provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the Third-Party Information and RIM assumes no liability whatsoever in relation to the Third-Party Information even if RIM has been advised of the possibility of such damages or can anticipate such damages.

Document ID: 15443227 Version 5

Last modified: November 2, 2007

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

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada