



# Enforcing encryption of internal and external file systems on BlackBerry devices

## Technical Overview



## Contents

- Data that BlackBerry devices encrypt by default .....1
- System requirements for file encryption on BlackBerry devices.....1
- Using encryption to protect stored files on BlackBerry devices .....1
- IT policy requirements for encryption of stored files on BlackBerry devices.....3
- Data that the BlackBerry device can encrypt in internal memory .....3
- Protecting user data stored on a locked BlackBerry device .....4
  - Turning on protected storage of BlackBerry device data in internal memory.....4
  - Guidelines for setting the internal memory encryption level.....4
- Protecting files stored in external memory on the BlackBerry device.....5
  - Setting the external memory encryption level .....5
  - Turning on external memory encryption .....5
  - Transferring encrypted media files ..... 6
  - Moving the media card to a different BlackBerry device ..... 6
  - Controlling access to objects in external memory ..... 6
- Protecting device transport encryption keys on a locked BlackBerry device ..... 6



## Data that BlackBerry devices encrypt by default

The BlackBerry® Enterprise Solution encrypts data traffic in transit between the BlackBerry® Enterprise Server and the BlackBerry devices automatically. By default, the BlackBerry Enterprise Solution generates the device transport encryption key and message key that the BlackBerry Enterprise Server and BlackBerry devices use to encrypt and decrypt all data traffic between them.

For more information about how the BlackBerry Enterprise Solution encrypts data traffic in transit, see the *BlackBerry Enterprise Solution Security Technical Overview*.

## System requirements for file encryption on BlackBerry devices

Internal files	External files	Device transport encryption keys
Java® based BlackBerry devices that run BlackBerry® Device Software Version 4.0 or later	<ul style="list-style-type: none"> <li>BlackBerry Enterprise Server Version 4.0 SP6 or later</li> <li>Java based BlackBerry devices that support external file storage using a media card (BlackBerry devices that run BlackBerry Device Software Version 4.2 or later)</li> </ul>	<ul style="list-style-type: none"> <li>BlackBerry Enterprise Server Version 4.0 SP3 or later</li> <li>Java based BlackBerry devices that run BlackBerry Device Software Version 4.1 or later</li> </ul>

## Using encryption to protect stored files on BlackBerry devices

You can configure the following options on the BlackBerry Enterprise Server to turn on encryption of stored files on supported BlackBerry devices.

Internal files	External files	Device transport encryption keys
To require BlackBerry devices on the organization's BlackBerry Enterprise Servers to encrypt user and application data that the BlackBerry devices store in internal memory using content protection, turn on the content protection process on BlackBerry devices using the Content Protection Strength IT policy rule in the BlackBerry Administration Service.	To require BlackBerry devices to encrypt files stored on media cards, turn on encryption on the external memory cards using the External File System Encryption Level IT policy rule.	To require BlackBerry devices to encrypt the device transport encryption keys that they use to encrypt data stored in internal file systems, set the Force Content Protection of Master Keys IT policy rule.  <b>Note:</b> When you turn on content protection of device transport encryption keys, the BlackBerry device uses the same encryption key strength that it uses to encrypt internal file systems when encrypting the device transport encryption keys.

Users can configure the following options to turn on encryption of stored files on their supported BlackBerry devices.

Internal files	External files	Device transport encryption keys
<p>Turn on the Content Protection option (<b>Options &gt; Security Options &gt; General Settings</b>).</p>	<ol style="list-style-type: none"> <li>1. Turn on Media Card Support (<b>Options &gt; Media Card</b> or <b>Options &gt; Memory &gt; Media Card Support</b>).</li> <li>2. Set the encryption mode for the external file system. The BlackBerry device encrypts files stored on the media card.</li> <li>3. Choose whether to encrypt media files in external memory only on the device. <ul style="list-style-type: none"> <li>• BlackBerry Device Software version 4.7 or later: If you set the <b>Encrypt Media Files</b> option to <b>Yes</b>, the BlackBerry device encrypts all files that have an audio, image, or video MIME type, excluding OMA DRM file types (.dcf, .odf, .o4a and .o4v).</li> <li>• BlackBerry Device Software version earlier than 4.7: If you set the <b>Encrypt Media Files</b> option to <b>Yes</b>, the BlackBerry device encrypts files according to the folders they are stored in on the media card (/BlackBerry/videos/, /BlackBerry/music/, /BlackBerry/pictures/, /BlackBerry/ringtones/ and /BlackBerry/voicenotes/).</li> </ul> <p><b>Note:</b> The BlackBerry device does not encrypt files transferred using USB while the Mass Storage Mode Support option is turned on, or OMA DRM files. OMA DRM files are protected using the OMA DRM standard.</p> </li> </ol>	<p>This option is not available for control by BlackBerry device users.</p>

For more information about how BlackBerry devices can encrypt stored data, see the *BlackBerry Enterprise Solution Security Technical Overview*.

## IT policy requirements for encryption of stored files on BlackBerry devices

Internal files	External files	Device transport encryption keys
Set the Content Protection Strength IT policy rule to the minimum strength level required. The user can set the Content Protection Strength option to a higher level on the BlackBerry device.	<ul style="list-style-type: none"> <li>Set the External File System Encryption Level IT policy rule to the minimum encryption level required. The user can set the Encryption Mode option to a higher level on the BlackBerry device.</li> <li>Set the Disable USB Mass Storage IT policy rule to True to prevent the user from turning on Mass Storage Mode on the BlackBerry device. The BlackBerry device does not encrypt external file on the media card when mass storage mode is turned on.</li> </ul> <p><b>Note:</b> The Disable External Memory IT policy rule should be unchanged from the default value, or explicitly set to False.</p>	Set the Force Content Protection of Master IT policy rule to the minimum strength level required.

See the *Policy Reference Guide* for more information about using IT policy rules.

## Data that the BlackBerry device can encrypt in internal memory

When you or BlackBerry device users turn on content protection on BlackBerry devices, the BlackBerry devices encrypt the following user data items:

Item	Description
AutoText	all text that automatically replaces the text a BlackBerry device user types
BlackBerry Browser	<ul style="list-style-type: none"> <li>content that web sites or third-party applications push to the BlackBerry device</li> <li>web sites that the user saves on the BlackBerry device</li> <li>browser cache</li> </ul>
calendar	<ul style="list-style-type: none"> <li>subject</li> <li>location</li> <li>organizer</li> <li>attendees</li> <li>notes included in the appointment or meeting request</li> </ul>

Item	Description
contacts (in the address book)	all information except the contact title and category <b>Note:</b> Set the Force Include Address Book In Content Protection IT policy rule to True to prevent the BlackBerry device user from turning off the Include Address Book option on the BlackBerry device. The BlackBerry device permits the Caller ID and Bluetooth Address Book transfer features to work when content protection is turned on and the BlackBerry device is locked.
email	<ul style="list-style-type: none"> <li>subject</li> <li>email addresses</li> <li>message body</li> <li>attachments</li> </ul>
memo list	<ul style="list-style-type: none"> <li>title</li> <li>information included in the body of the note</li> </ul>
OMA DRM applications	a key identifying the BlackBerry device and a key identifying the SIM card (if available) that the BlackBerry device adds to DRM forward-locked applications
RSA SecurID Library	the contents of the .sdtid file seed stored in flash memory
tasks	<ul style="list-style-type: none"> <li>subject</li> <li>information included in the body of the task</li> </ul>

## Protecting user data stored on a locked BlackBerry device

If content protection is turned on, on BlackBerry devices, user data that the BlackBerry devices store is always protected with the 256-bit AES encryption algorithm. Content protection of BlackBerry device user data is designed to perform the following actions:

- use a 256-bit AES content protection key to encrypt stored data when the BlackBerry device is locked
- use an ECC public key to encrypt data that the BlackBerry device receives when it is locked

## Turning on protected storage of BlackBerry device data in internal memory

You turn on protected storage of data on the BlackBerry device by setting the Content Protection Strength IT policy rule. You should choose a strength level that corresponds to the desired ECC key strength.

If a BlackBerry device user turns on content protection on the BlackBerry device, in the BlackBerry device Security Options, the BlackBerry device user can set the content protection strength to the same levels that you can set using the Content Protection Strength IT policy rule.

## Guidelines for setting the internal memory encryption level

When the content-protected BlackBerry device decrypts a message that it received while locked, the BlackBerry device uses the ECC private key in the decryption operation. The longer the ECC key, the more time the ECC decryption operation adds to the BlackBerry device decryption process. Choose a content protection strength level that optimizes either the ECC encryption strength or the decryption time.

If you set the content protection strength to Stronger (to use a 283-bit ECC key) or to Strongest (to use a 571-bit ECC key), consider setting the Minimum Password Length IT policy rule to enforce a minimum BlackBerry device password length of 12 characters or 21 characters, respectively. These password lengths

maximize the encryption strength that the longer ECC keys are designed to provide. The BlackBerry device uses the BlackBerry device password to generate the ephemeral 256-bit AES encryption key that the BlackBerry device uses to encrypt the content protection key and the ECC private key. A weak password produces a weak ephemeral key.

## Protecting files stored in external memory on the BlackBerry device

The BlackBerry device is designed to prevent a third-party device from using the media card by encrypting multimedia data that it stores on an external memory device according to the External File System Encryption Level IT policy rule setting, or the corresponding BlackBerry device setting.

The BlackBerry device is designed to support the following features:

- external file encryption by encrypting specific files on the external memory device using AES
  - Note:** The external file system encryption does not apply to files that the BlackBerry device user manually transfers to external memory (for example, from a USB mass storage device).
- access control to objects on the external memory device using code signing with 1024-bit RSA

The external memory device stores encrypted copies of the file keys that the BlackBerry device is designed to use to decrypt and encrypt files on the external memory device. The BlackBerry device is designed to use a randomly generated device key stored in the NV store in BlackBerry device RAM, the BlackBerry device password, or both to encrypt the external memory file keys.

## Setting the external memory encryption level

The administrator can use the External File System Encryption Level IT policy rule to enforce a minimum level of encryption for the external file system. If the IT policy rule is set, the BlackBerry device user can set the encryption mode to any encryption level stronger than the minimum.

Encryption mode	Description
Device	The BlackBerry device uses a randomly generated device key to encrypt the external file system to encrypt the external file system.
Security Password	The BlackBerry device uses the BlackBerry device password to encrypt the external file system. Turning on this option turns on the password prompt on the BlackBerry device automatically. The BlackBerry device then requires the user to set a BlackBerry device password if one does not exist already.
Security Password & Device	The BlackBerry device uses the randomly generated device key and the BlackBerry device password to encrypt the external file system. Turning on this option requires the user to set a BlackBerry device password if one does not exist already.

## Turning on external memory encryption

When the BlackBerry device user stores a file in external memory for the first time after the BlackBerry Enterprise Server administrator turns on or the BlackBerry device user turns on mass storage mode, the BlackBerry device decrypts the external memory file encryption key and uses it to automatically encrypt the stored file.

## Transferring encrypted media files

The user can connect the BlackBerry device to the computer to transfer files between the device and the computer, or use Bluetooth® technology to send media files to or receive media files from a Bluetooth enabled device.

Turning on the mass storage mode option on the BlackBerry device allows the user to transfer files quickly over a USB connection between the media card and the computer without using the media manager tool of the BlackBerry Desktop Manager. When the user transfers files to the media card using mass storage mode, the device does not encrypt the transferred files using mass storage mode even if the BlackBerry device is set to encrypt files stored on the media card. If the user transfers encrypted files from the media card using mass storage mode, the computer cannot decrypt the transferred files using mass storage mode.

## Moving the media card to a different BlackBerry device

If the user removes the media card from the BlackBerry device and places it in a new BlackBerry device, the new BlackBerry device cannot decrypt any files that the first BlackBerry device encrypted on the media card using a randomly generated device key. If the first BlackBerry device encrypted the files on the media card using the BlackBerry device password, when the user removes the media card from the BlackBerry device and places it in a new BlackBerry device, the new BlackBerry device prompts the user for the password used on the first BlackBerry device to access the files on the new device.

## Controlling access to objects in external memory

The BlackBerry device is designed to permit code signing keys in the header information of each encrypted file on the external memory device. The BlackBerry device is designed to check the code signing keys when the BlackBerry device opens the input or output streams of the encrypted files.

The BlackBerry device, any computer platform, and other devices that use the external memory device can modify encrypted files (for example, truncate files) on the external memory device. The BlackBerry device is not designed to perform integrity checks on the encrypted file data.

## Protecting device transport encryption keys on a locked BlackBerry device

If you turn on content protection of device transport encryption keys, the BlackBerry device uses the principal encryption key to encrypt the device transport encryption keys stored in flash memory and encrypts the principal encryption key using the content protection key. When the BlackBerry device receives data encrypted with a device transport encryption key while it is locked, it uses the decrypted principal encryption key to decrypt the required device transport encryption key in flash memory, and uses the decrypted device transport encryption key to decrypt and receive the data.

The BlackBerry device stores the decrypted device transport encryption keys and the decrypted principal encryption key in RAM only. When you, the BlackBerry device user, or a set password timeout locks the BlackBerry device, the wireless transceiver remains on and the BlackBerry device does not clear the RAM associated with these keys. The BlackBerry device is designed to prevent the decrypted principal encryption keys and the decrypted device transport encryption keys from appearing in flash memory.

Part number: 20993644 Version 4

©2010 Research In Motion Limited. All Rights Reserved. The BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, BlackBerry, "Always On, Always Connected" and the "envelope in motion" symbol are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries.

Java is a trademark of Sun Microsystems, Inc. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

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

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