



Erasing file systems on BlackBerry devices

Technical Overview

Contents

Types of file storage systems on BlackBerry devices	2
User data that the BlackBerry device stores	2
Types of remote BlackBerry device wipes	4
Erasing data from BlackBerry device memory and making the BlackBerry device unavailable (standard security wipe)	5
Resetting a BlackBerry device to factory default settings	6
Unbinding the smart card from the BlackBerry device	6
Actions that the BlackBerry device performs during BlackBerry device wipe processes	7

Types of file storage systems on BlackBerry devices

Type of memory	Description
flash memory (internal to device)	<p>Flash memory is a file system that stores application and user data on the BlackBerry® device. It cannot be physically removed from the BlackBerry device. Sections of flash memory can store files that the user downloads or saves manually to device memory.</p> <p>An NV store (non-volatile store) persists in flash memory and can only be overwritten by the BlackBerry device operating system. Third-party application code cannot write to the NV store. The device erases flash memory during a device wipe only.</p>
memory card file system (external or internal to device)	<p>Stores files that the user saves manually on the BlackBerry device. The user might save files to an external memory file system (for example, a removable media card) or to internal device memory that the BlackBerry device treats and exposes like an external memory file system. The BlackBerry device erases internal 'memory card' file systems during a device wipe.</p> <p>External memory file systems can be installed, accessed, and encrypted on the BlackBerry device. The BlackBerry device does not erase external memory file systems during a device wipe.</p>

User data that the BlackBerry device stores

The BlackBerry device stores user data items, including the following:

Item	Description
AutoText	all text that automatically replaces the text a BlackBerry device user types
BlackBerry® Browser	<ul style="list-style-type: none"> content that web sites or third-party applications push to the BlackBerry device web sites that the user saves on the BlackBerry device browser cache
calendar	<ul style="list-style-type: none"> subject location organizer attendees notes included in the appointment or meeting request
contacts (in the address book)	<p>all information except the contact title and category</p> <p>Note: 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.</p>
email	<ul style="list-style-type: none"> subject email addresses message body attachments

Item	Description
memo list	<ul style="list-style-type: none">• title• information included in the body of the note
RSA SecurID® Library	the contents of the .sdtid file seed stored in flash memory
tasks	<ul style="list-style-type: none">• subject• information included in the body of the task
third-party application data	all data associated with third-party applications that are installed on the BlackBerry device

Types of remote BlackBerry device wipes

The BlackBerry device wipe process is designed to delete all data in internal memory and overwrite that memory with zeroes.

Type	Description
factory default device wipe	This method of removing BlackBerry device data is initiated by the BlackBerry® Enterprise Server administrator remotely using the Remote Wipe Reset to Factory Defaults IT policy rule. See "Resetting a BlackBerry device to factory default settings" on page 6 for more information.
security wipe of data (standard security wipe)	This method of removing BlackBerry device data is initiated by the BlackBerry Enterprise Server administrator remotely, or by the BlackBerry device user locally on the BlackBerry device. See "Erasing data from BlackBerry device memory and making the BlackBerry device unavailable" on page 5 for more information.
security wipe of data and third-party applications (standard security wipe with Include third party applications option selected on device)	This method of removing BlackBerry device data is initiated by the BlackBerry device user locally on the BlackBerry device. The BlackBerry Enterprise Server administrator can achieve the same result by performing a factory default device wipe. See "Removing third-party applications during a user-initiated security wipe" on page 5 for more information.
security wipe of data on a content-protected device (standard security wipe on a content-protected device)	If content protection is turned on, during a security wipe the BlackBerry device uses a memory scrub process to overwrite the BlackBerry device flash memory file system. The BlackBerry memory scrub process complies with United States government requirements for clearing sensitive user data, including <i>Department of Defense directive 5220.22-M</i> and <i>National Institute of Standards and Technology Special Publication 800-88</i> .

The BlackBerry device performs the following actions, depending on the method used to wipe the internal device memory:

BlackBerry device action	Description
deletes user data	The BlackBerry device permanently deletes all user data in memory.
deletes corporate PIN-to-PIN encryption key	The BlackBerry device permanently deletes its references to the corporate peer-to-peer, or PIN-to-PIN, encryption key in memory.
deletes the master encryption key	The BlackBerry device permanently deletes its references to the master encryption key in memory.
unbinds the smart card (if applicable)	The BlackBerry device permanently deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.
unbinds the IT policy	The BlackBerry device permanently deletes the IT policy public key from its NV store so that it can receive a new IT policy and IT policy public key from a BlackBerry Enterprise Server.
password history	The BlackBerry device permanently deletes its references to past BlackBerry device password hashes in memory.
stored BlackBerry MDS device policy	The BlackBerry device permanently deletes its BlackBerry® Mobile Data System device policy from its NV store.
deletes stored IT policy	The BlackBerry device permanently deletes its stored IT policy.
deletes third-party applications	The BlackBerry device permanently deletes all third-party applications stored on the BlackBerry device.

BlackBerry device action	Description
overwrites BlackBerry device memory if content protection is turned on	The BlackBerry device uses a memory scrub process to overwrite the BlackBerry device flash memory file system.

For more information, see "Appendix D: BlackBerry device wipe process" in the *BlackBerry Enterprise Solution Security Technical Overview*.

Erasing data from BlackBerry device memory and making the BlackBerry device unavailable (standard security wipe)

A BlackBerry device that is not physically connected to a computer is designed to permanently delete its user and application data when any of the following events occur:

- The user clicks Wipe Handheld (in the Security Options) on the BlackBerry device.
- The user types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows on the BlackBerry device. (The default is ten attempts.)
- The BlackBerry Enterprise Server administrator sends the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Manager.
- The BlackBerry Enterprise Server administrator sends the Erase Data and Disable Handheld IT administration command with a delay (in hours, up to 168 hours) to the BlackBerry device from the BlackBerry Manager.

A BlackBerry device is designed to erase its user and application data and all applications when it is physically connected to a computer and any of the following events occur:

- The BlackBerry device user runs the application loader tool in the BlackBerry® Desktop Software and types the password incorrectly more times than the Set Maximum Password Attempts IT policy rule allows in the application loader tool prompt. (The default is ten attempts.)
The BlackBerry device user can also use the application loader tool in the BlackBerry Desktop Software to erase all user and application data on the BlackBerry device, but choose not to erase the BlackBerry device applications.
- The BlackBerry Enterprise Server administrator clicks Wipe Handheld File System in the BlackBerry Manager. This option deletes all data and applications from the BlackBerry device even if the service books do not exist on the BlackBerry device (in other words, if there is no connection between the BlackBerry Enterprise Server and the BlackBerry device).

Removing third-party applications during a user-initiated security wipe

When the user clicks Wipe Handheld (in the Security Options) on the BlackBerry device, the user can select the Include third party applications option at the same time. If the user selects this option, when the BlackBerry device permanently deletes its stored user data during the device wipe, it will also remove all of its third-party applications and application data.

Requiring a delay on remote BlackBerry device wipes

The BlackBerry Enterprise Server administrator can set the following IT policy rules to require that the remote BlackBerry device automatically delete its user and application data.

IT policy rule	Description
Secure Wipe Delay After IT Policy Received	Set this IT policy rule to a period of time, in hours, after which, if the BlackBerry device has not successfully received IT policy updates or IT administration commands, the BlackBerry device permanently deletes its user and application data.
Secure Wipe Delay After Lock	Set this IT policy rule to a period of time, in hours, after which, if the user has not unlocked the BlackBerry device, the BlackBerry device permanently deletes its user and application data.

IT policy rule	Description
Secure Wipe if Low Battery	Set this IT policy rule to require that, if the BlackBerry device battery power is insufficient to receive IT policy updates or IT administration commands, the BlackBerry device permanently deletes its user and application data.

Resetting a BlackBerry device to factory default settings

The BlackBerry Enterprise Server administrator can use the Remote Wipe Reset to Factory Defaults IT policy rule to require the BlackBerry device to return to factory default settings when it receives the Erase Data and Disable Handheld IT administration command over the wireless network. When the BlackBerry Enterprise Server administrator sets this rule to True and sends the Erase Data and Disable Handheld IT administration command to the BlackBerry device from the BlackBerry Manager, or the BlackBerry Enterprise Server administrator clicks Nuke Handheld in the BlackBerry Manager, the BlackBerry device reverts to its factory default settings and permanently deletes all of the following items:

- user data
- corporate PIN-to-PIN encryption key
- master encryption key
- smart card binding information
- password history
- stored BlackBerry MDS device policy
- record of time elapsed since the BlackBerry device was last turned on
- stored IT policy
- third-party applications and application data

When the BlackBerry device reverts to its factory default settings, it overwrites BlackBerry device internal memory and, if content protection is turned on, performs a scrub of BlackBerry device memory.

Unbinding the smart card from the BlackBerry device

When the BlackBerry Enterprise Server administrator or the user starts a BlackBerry device wipe, causing the BlackBerry device to erase its stored user and application data, the BlackBerry device permanently deletes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.

The BlackBerry Enterprise Server administrator can permanently delete the smart card binding information from the BlackBerry device manually in the following ways.

- Send the Erase Data and Disable Handheld IT administration command to the BlackBerry device to permanently delete the binding between a user's current smart card and the BlackBerry device.
- When the user turns off two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and permanently deletes the smart card binding information from the BlackBerry device.

Actions that the BlackBerry device performs during BlackBerry device wipe processes

When the BlackBerry device permanently deletes its stored user and application data, it performs specific actions, depending on the type of device wipe performed:

Device wipe actions:	Type of device wipe		
	Standard security wipe		Factory default wipe
	with Include third party applications option turned off	with Include third party applications option turned on	
deletes user data	✓	✓	✓
deletes corporate PIN-to-PIN encryption key	✓	✓	✓
deletes master encryption key	✓	✓	✓
unbinds IT policy	✓	✓	✓
unbinds smart card	✓	✓	✓
deletes password history			✓
deletes stored BlackBerry MDS device policy			✓
deletes record of time elapsed since the BlackBerry device was last turned on			✓
deletes stored IT policy			✓
deletes third-party applications		✓	✓
overwrites BlackBerry device memory	✓	✓	✓
performs a scrub of BlackBerry device memory if content protection is turned on	✓	✓	✓

For more information about performing a scrub of BlackBerry device memory, see "Appendix D: BlackBerry device wipe process" in the *BlackBerry Enterprise Solution Security Technical Overview*.

Part number: 21625041 Version 1

©2008 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.

RSA SecurID is a trademark of RSA Security. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners.

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