

BlackBerry Enterprise Server Express for Microsoft Exchange

Version: 5.0 | Service Pack: 1

Policy Reference Guide

Contents

1	IT policy rules.....	4
	Default IT policy.....	4
2	Descriptions of IT policy rules.....	5
	Common policy group.....	5
	Disable MMS IT policy rule.....	5
	Device Only Items.....	5
	Allow SMS IT policy rule.....	5
	Maximum Password Age IT policy rule.....	6
	Maximum Security Timeout IT policy rule.....	6
	Minimum Password Length IT policy rule.....	7
	Password Pattern Checks IT policy rule.....	7
	Password Required IT policy rule.....	8
	User Can Change Timeout IT policy rule.....	8
	User Can Disable Password IT policy rule.....	9
	Bluetooth policy group.....	9
	Disable Bluetooth IT policy rule.....	9
	Camera policy group.....	10
	Disable Photo Camera IT policy rule.....	10
	Disable Video Camera IT policy rule.....	10
	Email Messaging policy group.....	11
	Confirm External Image Download IT policy rule.....	11
	Disable Manual Download of External Images IT policy rule.....	11
	Disable Rich Content Email IT policy rule.....	12
	Maximum Native Attachment MTH attachment size IT policy rule.....	12
	Maximum Native Attachment MFH attachment size IT policy rule.....	12
	Maximum Native Attachment MFH total attachment size IT policy rule.....	13
	Password policy group.....	13
	Forbidden Passwords IT policy rule.....	13
	Maximum Password History IT policy rule.....	14
	Set Maximum Password Attempts IT policy rule.....	14
	Set Password Timeout IT policy rule.....	15
	Suppress Password Echo IT policy rule.....	15
	Security policy group.....	16

Content Protection Strength IT policy rule.....	16
Disable External Memory IT policy rule.....	17
Disable IP Modem IT policy rule.....	17
Disallow Third Party Application Downloads IT policy rule.....	18
Encryption on On-Board Device Memory Media Files IT policy rule.....	18
External File System Encryption Level IT policy rule.....	19
Force Lock When Holstered IT policy rule.....	19
Required Password Pattern IT policy rule.....	20
S/MIME Application policy group.....	21
S/MIME Allowed Content Ciphers IT policy rule.....	21
S/MIME Force Encrypted Messages IT policy rule.....	21
Wi-Fi policy group.....	22
Disable Wi-Fi IT policy rule.....	22
Wireless Software Upgrades policy group.....	22
Disallow Patch Download Over WAN IT policy rule.....	22
Wired Software Updates policy group.....	23
Allow Web-Based Software Loading IT policy rule.....	23
Cryptographic Services Backup IT policy rule.....	23

3 Descriptions of application control policy rules..... 24

Are Internal Network Connections Allowed application control policy rule.....	24
Are External Network Connections Allowed application control policy rule.....	24
Are Local Connections Allowed application control policy rule.....	25
Can Device Settings be Modified application control policy rule.....	25
Can the Security Timer be Reset application control policy rule.....	25
Disposition application control policy rule.....	26
Is Access to the Browser Filters API Allowed application control policy rule.....	26
Is Access to the Email API Allowed application control policy rule.....	26
Is Access to the Event Injection API Allowed application control policy rule.....	27
Is Access to the File API Allowed application control policy rule.....	27
Is Access to the GPS API Allowed application control policy rule.....	27
Is Access to the Handheld Key Store Allowed application control policy rule.....	28
Is Access to the Interprocess Communication API Allowed application control policy rule.....	28
Is Access to the Phone API Allowed application control policy rule.....	29
Is Access to the Media API Allowed application control policy rule.....	29

Is Access to the Module Management API Allowed application control policy rule.....	30
Is Access to the PIM API Allowed application control policy rule.....	30
Is Access to the Screen, Microphone, and Video Capturing APIs Allowed application control policy rule.....	30
Is Access to the Serial Port Profile for Bluetooth API Allowed application control policy rule.....	31
Is Access to the User Authenticator API Allowed application control policy rule.....	31
Is Access to the Wi-Fi API Allowed application control policy rule.....	32
Is Key Store Medium Security Allowed application control policy rule.....	32
Is Theme Data Allowed application control policy rule.....	33
List of Browser Filter Domains application control policy rule.....	33
List of External Domains application control policy rule.....	34
List of Internal Domains application control policy rule.....	34
4 Glossary.....	35
5 Provide feedback.....	36
6 Legal notice.....	37

IT policy rules

1

You can assign IT policies to BlackBerry® devices to satisfy your organization's security policy requirements and to reflect the needs of the BlackBerry device users. For example, you can create an IT policy, configure the IT policy rules for executive-level feature and security requirements, add executives to a group, and assign the IT policy to the group.

For more information about creating an IT policy, configuring IT policy rules, and assigning an IT policy to a user account or group, see the *BlackBerry Enterprise Server Express Administration Guide*.

Default IT policy

The BlackBerry® Enterprise Server Express includes a default IT policy. When you install the BlackBerry Enterprise Server Express, the IT policy rules in the default IT policy do not contain any values. You can configure and apply the default IT policy to user accounts or you can create new IT policies and assign the new IT policies to user accounts to control the BlackBerry devices in your organization's environment.

Descriptions of IT policy rules

2

Common policy group

IT policy rules in the Common policy group apply to BlackBerry® device owner information and to MMS.

Disable MMS IT policy rule

Description

This rule specifies whether a BlackBerry® device user can send and receive MMS messages.

Default value

The default value is No.

Usage

Change this rule to Yes to prevent security risks that are associated with sending and receiving MMS messages. For more information, see the *BlackBerry Enterprise Solution Security Technical Overview*.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 4.0.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Device Only Items

Allow SMS IT policy rule

Description

This rule specifies whether a BlackBerry® device user can send SMS text messages.

Default value

The default value is Yes.

Usage

Change this rule to No to prevent a user from sending SMS text messages.

Changing this rule to No does not prevent a user from receiving SMS text messages.

Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Connect™ 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Maximum Password Age IT policy rule

Description

This rule specifies the number of days before a BlackBerry® device password expires and a user must set a new password. The permitted range is 0 through 65,535 days.

Default values

The default value in the Default IT policy is a null value.

Usage

If you configure this rule to 0, the BlackBerry device password does not expire.

Dependencies

A BlackBerry device uses this rule only if the Password Required rule is configured to Yes.

Minimum requirements

- C++-based BlackBerry device that is running BlackBerry® Device Software 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software 3.6
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Maximum Security Timeout IT policy rule

Description

This rule specifies the maximum time (in minutes) that a BlackBerry® device user can specify as the security timeout value. The security timeout value is the number of minutes of inactivity before the BlackBerry device locks. The permitted range is 10 through 480 minutes.

Default values

The default value in the Default IT policy is a null value.

Dependencies

A BlackBerry device uses this rule only if the Password Required rule is configured to Yes.

A BlackBerry device user can specify any timeout value that is lower than the maximum value, unless you configure the User Can Change Timeout rule to No.

To configure a timeout value, in the Password policy group, configure the Set Password Timeout rule.

Minimum requirements

- C++ based BlackBerry device that is running BlackBerry® Device Software 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software 3.6
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Minimum Password Length IT policy rule

Description

This rule specifies the minimum number of characters that are required for a BlackBerry® device password. The permitted range is 4 through 14 characters. The maximum password length, which this rule does not control, is 32 characters.

Default value

The default value is a null value.

Dependencies

A BlackBerry device uses this rule only if the Password Required rule is configured to Yes.

Minimum requirements

- C++ based BlackBerry device that is running BlackBerry® Device Software 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software 3.6
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1 or 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Password Pattern Checks IT policy rule

Description

This rule specifies whether to verify that a BlackBerry® device password matches specific character pattern requirements.

Default values

The default value in the Default security IT policy is No restriction.

Usage

Change this rule to At least 1 alpha and 1 numeric character to require that a BlackBerry device user type at least 1 alphabetic character and 1 numeric character.

Change this rule to At least 1 alpha, 1 numeric, and 1 special character to require that a BlackBerry device user type at least 1 alphabetic character, 1 numeric character, and 1 special character.

Change this rule to At least 1 upper-case alpha, one lower-case alpha, 1 numeric, and 1 special character to require that a BlackBerry device user type at least 1 upper-case alphabetic, one lower-case alphabetic, 1 numeric, and 1 special character.

If you select option 2 or 3, password pattern checking is not available for C++ based BlackBerry devices.

By default, a BlackBerry device prevents setting passwords that use a natural sequence of characters or numbers. If a user inserts a symbol into a natural sequence, a BlackBerry device can use the password.

Dependencies

A BlackBerry device uses this rule only if the Password Required rule is configured to Yes.

Minimum requirements

- C++ based BlackBerry device that is running BlackBerry® Device Software 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software 3.6
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Password Required IT policy rule

Description

This rule specifies whether a BlackBerry® device user must configure a password on a BlackBerry device.

Default values

The default value in the Default IT policy is No.

Minimum requirements

- C++ based BlackBerry device that is running BlackBerry® Device Software 2.5
- Java® based BlackBerry device that is running BlackBerry Device Software 3.6
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1 or 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

User Can Change Timeout IT policy rule

Description

This rule specifies whether a BlackBerry® device user can override the security timeout value.

Default value

The default value is Yes.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

User Can Disable Password IT policy rule

Description

This rule specifies whether a BlackBerry® device user can turn off the requirement for a BlackBerry device security password.

Default values

The default value in the Default IT policy is Yes.

Dependencies

A BlackBerry device uses this rule only if the Password Required rule is configured to Yes.

This rule is obsolete for Java® based BlackBerry devices that are running BlackBerry® Device Software version 4.0 or later and C++ based BlackBerry devices that are running BlackBerry Device Software version 2.7.

Minimum requirements

- C++ based BlackBerry device that is running BlackBerry Device Software 2.5
- Java based BlackBerry device that is running BlackBerry Device Software 3.6
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Bluetooth policy group

For more information about Bluetooth® security on BlackBerry® devices, see the *BlackBerry Enterprise Solution Security Technical Overview* and *Security for BlackBerry Devices with Bluetooth Wireless Technology*.

Disable Bluetooth IT policy rule

Description

This rule specifies whether support for Bluetooth® technology on a BlackBerry® device is turned off.

Default value

The default value is No.

Usage

If Bluetooth technology is turned on when a BlackBerry device receives this rule, the user must reset the BlackBerry device for the change to take effect.

Minimum requirement

- Java® based BlackBerry device
- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 3.8
- BlackBerry® Enterprise Server Express 5.0 SP1

Camera policy group

Disable Photo Camera IT policy rule

Description

This rule specifies whether the camera is available on a BlackBerry® device.

Default value

The default value is No. The camera is available on the BlackBerry device.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Disable Video Camera IT policy rule

Description

This rule specifies whether the video camera feature on a BlackBerry® device is turned on.

Default value

The default value is No. The video camera is available on the BlackBerry device.

Usage

Change this rule to Yes to turn off the video camera feature.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.3

- BlackBerry® Enterprise Server Express 5.0 SP1

Email Messaging policy group

The rules in the Email Messaging policy group apply to wireless message reconciliation and attachment viewing.

Confirm External Image Download IT policy rule

Description

This rule specifies whether a BlackBerry® device displays a confirmation dialog box when a BlackBerry device user clicks the Get Images link in an HTML-formatted email message.

Default value

The default value is No.

Usage

The message that the confirmation dialog box displays informs users that they might expose their email addresses if they download an image from the Internet. If you change this rule to Yes, BlackBerry device users must verify whether they want to download an image each time they click the Get Images link in an HTML-formatted email message.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 5.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Disable Manual Download of External Images IT policy rule

Description

This rule specifies whether a BlackBerry® device user can request to view URL-referenced content (such as pictures) that is embedded in email messages manually.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.5
- BlackBerry® Enterprise Server Express 5.0 SP1

Disable Rich Content Email IT policy rule

Description

This rule specifies whether a BlackBerry® device can receive email messages in rich text or HTML format.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.5
- BlackBerry® Enterprise Server Express 5.0 SP1

Maximum Native Attachment MTH attachment size IT policy rule

Description

This rule specifies the maximum size (in KB) of a single standard attachment that a BlackBerry® device user can download to a BlackBerry device. The permitted range is 0 through 1,048,576 KB.

Default value

The default value is 10,240 KB.

Usage

Change this rule to 0 to turn off the ability to download standard attachments on a BlackBerry device.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.5
- BlackBerry® Enterprise Server Express 5.0 SP1

Maximum Native Attachment MFH attachment size IT policy rule

Description

This rule specifies the maximum size (in bytes) of a standard attachment that a BlackBerry® device user can upload from a BlackBerry device. The permitted range is 0 through 3 MB.

Default value

The default value is 3 MB.

Minimum requirements

- Java® based BlackBerry device

- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Maximum Native Attachment MFH total attachment size IT policy rule

Description

This rule specifies the total size (in bytes) of all standard attachments that a BlackBerry® device user can upload from a BlackBerry device. The permitted range is 0 through 5 MB.

Default value

The default value is 5 MB.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Password policy group

A BlackBerry® device uses the IT policy rules in the Password policy group only if, in the Device Only items, you configure the Password Required IT policy rule to Yes. For more information about using passwords on BlackBerry devices, see the *BlackBerry Enterprise Solution Security Technical Overview*.

Forbidden Passwords IT policy rule

Description

This rule specifies the passwords that a BlackBerry® device user cannot use. You must separate multiple passwords with a comma (.).

Default value

The default value is a null value.

Usage

By default, a BlackBerry device prevents a user from configuring passwords that use a natural sequence of characters or numbers. The BlackBerry device also prevents common letter substitutions automatically. For example, if you include "password" in the forbidden passwords list, users cannot use "p@ssw0rd", "pa\$zword", or "password123" on the BlackBerry device.

Dependencies

A BlackBerry device uses this rule only if the Password Required rule is configured to Yes.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.1
- BlackBerry® Enterprise Server Express 5.0 SP1

Maximum Password History IT policy rule

Description

This rule specifies the maximum number of previous passwords that a BlackBerry® device checks new passwords against to prevent a BlackBerry® device user from reusing previous passwords.

Default values

The default value is 0. The BlackBerry device does not check for reused passwords.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Set Maximum Password Attempts IT policy rule

Description

This rule specifies the number of password tries that a user can make before a BlackBerry® device deletes all of the application data permanently. The permitted range is 3 to 10 tries.

Default value

The default setting is 10 password tries.

Usage

The maximum number of password tries is 10. Use this rule to lower the number of possible password tries.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Set Password Timeout IT policy rule

Description

This rule specifies the number of minutes of inactivity before the security timeout occurs and a BlackBerry® device user must type the password to unlock the BlackBerry device.

Default value

For BlackBerry® Device Software versions earlier than version 4.7, the default value is 2 minutes.

For BlackBerry Device Software version 4.7 and later, the default value is 30 minutes.

Usage

Use this rule to change the default security timeout interval.

Dependencies

A BlackBerry device uses this rule only if you change the Password Required IT policy rule to Yes.

If you do not change the User Can Change Timeout IT policy rule to No, the user can change the security timeout to any value.

By default, the maximum security timeout interval is 60 minutes.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Suppress Password Echo IT policy rule

Description

This rule specifies whether, after a given number of incorrect password attempts, the characters that a BlackBerry® device user types in the Password dialog box appear on the screen.

Default value

The default value is Yes.

Dependencies

The BlackBerry® device uses this rule only if a user configures a password on the BlackBerry device. To require a password, configure the Password Required rule to Yes.

To specify the number of incorrect password tries that the BlackBerry device permits before the characters that the user types appear on the screen, configure the Set Maximum Password Attempts rule.

Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 1.2, 2.0, 2.1, or 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Security policy group

Content Protection Strength IT policy rule

Description

This rule specifies the cryptography strength that a BlackBerry® device uses to encrypt content that it receives while it is locked. When you specify a value, the content protection feature is turned on.

Default values

The default value is a null value.

Usage

Configure this rule to Strong to use a 160-bit ECC public key. This key provides good security and good performance and is adequate for most situations.

Configure this rule to Stronger to use a 283-bit ECC public key. This key provides better security but slower performance than the Strong setting.

Configure this rule to Strongest to use a 571-bit ECC public key. This key provides the highest level of security but the slowest performance of the three settings.

For BlackBerry devices that are running BlackBerry® Device Software 5.0 and later, if on-board device memory exists on the BlackBerry device when you configure this rule, the rule also encrypts the on-board device memory (embedded MC) to the BlackBerry device user password and a device-generated key.

For BlackBerry devices that are running BlackBerry Device Software versions that are earlier than 5.0, you can configure the External File System Encryption Level IT policy rule. The External File System Encryption Level IT policy rule also encrypts the media card.

Dependencies

A BlackBerry device uses this rule only if you configure the Password Required IT policy rule to Yes.

If you configure this rule to Strong or Stronger, configure the Minimum Password Length IT policy rule to 12 characters. If you configure the content protection strength to Strongest, instruct the user to create a password of at least 21 characters. These password lengths maximize the encryption strength that the longer ECC keys are designed to provide.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Disable External Memory IT policy rule

Description

This rule specifies whether to prevent a BlackBerry® device user from accessing the media card on a supported BlackBerry device.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Disable IP Modem IT policy rule

Description

This rule specifies whether the IP modem on an applicable BlackBerry® device is available.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Disallow Third Party Application Downloads IT policy rule

Description

This rule specifies whether a BlackBerry® device user can install an application that the Research In Motion® signing authority system did not digitally sign on a BlackBerry device.

Default values

The default value is No.

Usage

This rule prevents a user from installing an unsigned third-party application that is sent over a wireless network or installed using the BlackBerry® Desktop Manager or application loader tool. This rule applies to any unsigned applications that the BlackBerry® Enterprise Server Express or another party sends to a BlackBerry device.

If you change the value to Yes, this rule does not remove any existing third-party applications from a BlackBerry device.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 2.1, 4.0
- BlackBerry® Device Software 3.6
- BlackBerry Enterprise Server Express 5.0 SP1

Encryption on On-Board Device Memory Media Files IT policy rule

Description

If a BlackBerry® device user inserts a media card in the BlackBerry device, this rule specifies whether the media files that are located on the media card are encrypted to the user password and the device-generated key.

Default value

The default value is Allowed. If a BlackBerry device user inserts a media card in the BlackBerry device, encryption of the media files that are on the media card is allowed.

Usage

Change this rule to Required or Disallowed to prevent a user from changing this setting on the BlackBerry device.

Dependencies

A BlackBerry device can use this IT policy rule only if you also configure the Content Protection Strength IT policy rule.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 5.0

- BlackBerry® Enterprise Server Express 5.0 SP1

External File System Encryption Level IT policy rule

Description

This rule specifies the level of encryption that a BlackBerry® device uses to encrypt files that it stores on a media card.

Default values

The default value in the Default IT policy is Not required.

Usage

You can use this rule to require that a BlackBerry device encrypt a media card, either including or excluding media card files. You cannot use this rule to encrypt files that a BlackBerry device user transfers to the media card manually (for example, from a USB mass storage device).

The master keys for the media card are stored on the media card. A BlackBerry device is designed to use the master keys to decrypt and encrypt the files on the media card. A BlackBerry device is designed to use the BlackBerry device key, a password that a BlackBerry device user provides, or both to encrypt the master keys.

Change this rule to Encrypt to User Password (excluding multimedia directories) if the media card requires encryption with a password that the user provides.

Change this rule to Encrypt to User Password (including multimedia directories) if the media card requires encryption with a password that the user provides.

Change this rule to Encrypt to Device Key (excluding multimedia directories) if the media card requires encryption with a BlackBerry device key.

Change this rule to Encrypt to Device Key (including multimedia directories) if the media card requires encryption with a BlackBerry device key.

Change this rule to Encrypt to User Password and Device Key (excluding multimedia directories) if the media card requires encryption with a password that the user provides and a BlackBerry device key.

Change this rule to Encrypt to User Password and Device Key (including multimedia directories) if the media card requires encryption with a password that the user provides and the BlackBerry device key.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Force Lock When Holstered IT policy rule

Description

This rule specifies whether a BlackBerry® device locks when a BlackBerry device user inserts it in the holster.

Default values

The default value in the Default IT policy is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Required Password Pattern IT policy rule

Description

This rule specifies the permitted structure of a BlackBerry® device password.

Passwords can contain Latin-1 characters only.

Default value

The default value is a null value.

Usage

Use the following characters in the password pattern to specify the character type that is permitted and its position in the password:

- a: Permits any letter.
- A: Permits an uppercase letter only.
- c: Permits any consonant.
- C: Permits an uppercase consonant only.
- v: Permits any vowel.
- V: Permits an uppercase vowel only.
- N, n, or #: Permits a number only.
- S, s, or @: Permits a symbol only.
- ?: Permits any letter, number, or symbol.

If you configure this rule, the user can create a password that is greater than or equal to the length of the pattern on a BlackBerry device. Password characters that exceed the pattern length can be any letters, numbers, or symbols.

Attention: Preventing a specific password character reduces the entropy level and security level of the password.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.2

- BlackBerry® Enterprise Server Express 5.0 SP1

S/MIME Application policy group

The IT policy rules in the S/MIME Application policy group apply to BlackBerry® devices running the S/MIME Support Package for BlackBerry smartphones. For more information about using the S/MIME Support Package for BlackBerry smartphones, see the *S/MIME Support Package for BlackBerry Devices Security Technical Overview*.

S/MIME Allowed Content Ciphers IT policy rule

Description

This rule specifies the encryption algorithms that a BlackBerry® device can use to encrypt S/MIME-protected messages.

Default value

The default value is to use all supported algorithms.

Usage

To maintain compatibility with most S/MIME clients, use Triple DES encryption and one of the RC2 algorithms. By default, a BlackBerry device is designed to encrypt email messages using Triple DES encryption if it does not know the decryption methods available to the recipient.

Minimum requirements

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones 1.5
- BlackBerry® Application Suite 1.0
- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

S/MIME Force Encrypted Messages IT policy rule

Description

This rule specifies whether a BlackBerry® device encrypts all messages that it sends using S/MIME encryption.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- S/MIME Support Package for BlackBerry® smartphones 1.5
- BlackBerry® Application Suite 1.0

- BlackBerry® Connect™ 4.0
- BlackBerry® Device Software 3.6
- BlackBerry® Enterprise Server Express 5.0 SP1

Wi-Fi policy group

The previous name of this policy group was WLAN policy group.

Disable Wi-Fi IT policy rule

Description

This rule specifies whether a BlackBerry® device user can access a Wi-Fi® network from a Wi-Fi enabled BlackBerry device.

Default value

The default value is No.

Usage

Change this rule to Yes to prevent a user from accessing a Wi-Fi network from the BlackBerry device.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.2.1
- BlackBerry® Enterprise Server Express 5.0 SP1

Wireless Software Upgrades policy group

Disallow Patch Download Over WAN IT policy rule

Description

This rule specifies whether to prevent a BlackBerry® device from downloading updates for the BlackBerry® Device Software over a WAN connection.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry Device Software 4.5
- BlackBerry® Enterprise Server Express 5.0 SP1

Wired Software Updates policy group

IT policy rules in the Wired Software Updates policy group apply to the BlackBerry® Device Software update process when a user connects a BlackBerry device to a computer.

Allow Web-Based Software Loading IT policy rule

Description

This rule specifies whether a user can update the BlackBerry® Device Software using the web-based software loading feature.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry Device Software 5.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Cryptographic Services Backup IT policy rule

Description

This rule specifies whether the BlackBerry® device can back up cryptographic services data when a user updates the BlackBerry® Device Software.

A cryptographic service is any service that uses a cryptographic key to protect the communication between the BlackBerry device and the BlackBerry® Enterprise Server Express or the BlackBerry® Internet Service (for example, the encryption keys that are generated during activation that are used to protect the data that the BlackBerry device and the BlackBerry Enterprise Server Express send between each other).

Default value

The default value is Yes.

Usage

If you allow a BlackBerry device to back up cryptographic services data, the BlackBerry device can continue to use a cryptographic service after the software loading process completes without requiring the user to reactivate the BlackBerry device manually.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry Device Software 5.0
- BlackBerry Enterprise Server Express 5.0 SP1

Descriptions of application control policy rules

3

For information about configuring application control policy rules, see the *BlackBerry Enterprise Server Express Administration Guide*.

Are Internal Network Connections Allowed application control policy rule

Description

This rule specifies whether an application can make internal network connections. You can configure this rule to prevent the application from sending or receiving any data on a BlackBerry® device using an internal protocol (for example, the BlackBerry MDS Connection Service). You can also configure this rule so that an application prompts a BlackBerry device user before it makes internal connections through the BlackBerry device firewall.

Default value

The default value is Prompt User.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Are External Network Connections Allowed application control policy rule

Description

This rule specifies whether an application can make external network connections. You can configure this rule to prevent the application from sending or receiving any data on a BlackBerry® device using an external protocol (such as WAP or TCP). You can also configure this rule so that an application prompts a BlackBerry device user before it makes external connections through the BlackBerry device firewall.

Default value

The default value is Prompt User.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Are Local Connections Allowed application control policy rule

Description

This rule specifies whether an application can make local network connections (for example, connections to a BlackBerry® device using a USB or serial port).

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Can Device Settings be Modified application control policy rule

Description

This rule specifies whether an application can change configuration settings and user settings on a BlackBerry® device.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.2.1
- BlackBerry® Enterprise Server Express 5.0 SP1

Can the Security Timer be Reset application control policy rule

Description

This rule specifies whether an application can reset the time that must pass before a BlackBerry® device locks automatically.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.2.1

- BlackBerry® Enterprise Server Express 5.0 SP1

Disposition application control policy rule

Description

This rule specifies whether an application is optional, required, or not permitted on the BlackBerry® device. You can use this rule to make a specific application required on the BlackBerry device or to prevent BlackBerry device users from installing unspecified or untrusted applications on the BlackBerry device.

Default value

The default value is Optional.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Browser Filters API Allowed application control policy rule

Description

This rule specifies whether an application can access browser filter APIs to register a browser filter on a BlackBerry® device. You can use this rule to permit third-party applications to apply custom browser filters to web page content on a BlackBerry device.

Default value

The default value is Not Permitted.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Email API Allowed application control policy rule

Description

This rule specifies whether an application can send and receive email messages using a BlackBerry® device.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Event Injection API Allowed application control policy rule

Description

This rule specifies whether an application can simulate input events on a BlackBerry® device, such as pressing keys or performing trackball actions.

Default value

The default value is Not Permitted.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the File API Allowed application control policy rule

Description

This rule specifies whether an application can access, change, delete, and move files on a BlackBerry® device.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.2
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the GPS API Allowed application control policy rule

Description

This rule specifies whether an application can access the GPS APIs on a BlackBerry® device. You can configure this rule to prevent the application from accessing the GPS APIs on a BlackBerry device or to prompt the BlackBerry device user before an application can access the GPS APIs.

Default value

The default value is Prompt User.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Handheld Key Store Allowed application control policy rule

Description

This rule specifies whether an application can access the key store APIs on a BlackBerry® device.

Default value

The default value is Allowed.

Dependencies

If you configure the Minimal Signing Key Store Security Level IT policy rule and the Minimal Encryption Key Store Security Level IT policy rule to use the high security level, this rule does not apply. A BlackBerry device prompts the BlackBerry device user for the key store password each time that an application tries to access the private key.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Interprocess Communication API Allowed application control policy rule

Description

This rule specifies whether an application can perform cross application communication operations. You can use this rule to permit two or more applications to share data or for one application to use the connection permissions of another application.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Phone API Allowed application control policy rule

Description

This rule specifies whether an application can make calls and access call logs on a BlackBerry® device. You can configure this rule to prevent the application from making calls on a BlackBerry device or to prompt a BlackBerry device user before the user makes calls.

Default value

The default value is Prompt User.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Media API Allowed application control policy rule

Description

This rule specifies whether an application can run or create multimedia files on a BlackBerry® device.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.3
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Module Management API Allowed application control policy rule

Description

This rule specifies whether an application can add, change, or delete Java® .cod files on the BlackBerry® device.

Default value

The default value is Allowed.

Minimum requirements

- Java based BlackBerry device
- BlackBerry® Device Software 4.3
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the PIM API Allowed application control policy rule

Description

This rule specifies whether an application can access the BlackBerry® device PIM APIs, which control access to a BlackBerry device user's personal information, such as contacts.

Note: Permitting an application to access PIM data APIs and use internal and external network connection protocols might permit an application to send all of a user's personal information from a BlackBerry device.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Screen, Microphone, and Video Capturing APIs Allowed application control policy rule

Description

This rule specifies whether an application can record media, such as audio and video, using the BlackBerry® Browser or other applications on a BlackBerry device.

Default value

The default value is No.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.2.1
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the Serial Port Profile for Bluetooth API Allowed application control policy rule

Description

This rule specifies whether an application can access the Bluetooth® SPP API.

Default value

The default value is Allowed.

Dependencies

If you configure the Disable Serial Port Profile IT policy rule to Yes, this rule does not apply. A BlackBerry® device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Access to the User Authenticator API Allowed application control policy rule

Description

This rule specifies whether an application can access the user authenticator framework API. The user authenticator framework permits the registration of drivers that provide two-factor authentication to unlock a BlackBerry® device.

This rule applies to the BlackBerry® Device Software and third-party Java® applications.

Default value

The default value is Allowed.

Usage

For BlackBerry devices that are running BlackBerry Device Software version 5.0 and later, this rule applies to drivers for smart card readers and to custom two-factor authentication methods that are created by developers in your organization.

For BlackBerry devices that are running BlackBerry Device Software versions that are earlier than version 5.0, this rule applies to drivers for smart cards only.

Minimum requirements

- Java based BlackBerry device
- BlackBerry Device Software version 4.0
- BlackBerry® Enterprise Server version 4.1 SP2

Is Access to the Wi-Fi API Allowed application control policy rule

Description

This rule specifies whether a BlackBerry® device can send and receive data over a Wi-Fi® connection and access information about the Wi-Fi network.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software version 4.2.1
- BlackBerry® Enterprise Server version 5.0

Is Key Store Medium Security Allowed application control policy rule

Description

This rule specifies whether an application can access key store items that are stored at the medium security level. The application must prompt a BlackBerry® device user for the key store password when it tries to access the private key for the first time or when the private key password timeout expires.

Default value

The default value is Allowed.

Dependencies

If you configure the Minimal Signing Key Store Security Level IT policy rule and the Minimal Encryption Key Store Security Level IT policy rule to use the high security level, this rule does not apply. A BlackBerry device prompts the user for the key store password each time that an application tries to access the private key.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Is Theme Data Allowed application control policy rule

Description

This rule specifies whether a BlackBerry® device user can use custom theme applications that are developed using the BlackBerry® Theme Studio as themes on a BlackBerry device.

Default value

The default value is Allowed.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

List of Browser Filter Domains application control policy rule

Description

This rule specifies the list of domains for which an application can apply browser filters to web page content on a BlackBerry® device. For example, you can specify www.google.com and www.yahoo.com as domains for which an application can use a browser filter for search engines.

Default value

The default value is a null value.

Minimum requirements

- Java® based BlackBerry device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

List of External Domains application control policy rule

Description

This rule specifies the external domain names that an application can establish a connection to.

Default value

The default value is a null value.

Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

List of Internal Domains application control policy rule

Description

This rule specifies the internal domain names that an application can establish a connection to.

Default value

The default value is a null value.

Minimum requirements

- Java® based BlackBerry® device
- BlackBerry® Application Suite 1.0
- BlackBerry® Device Software 4.0
- BlackBerry® Enterprise Server Express 5.0 SP1

Glossary

4

DES

Data Encryption Standard

ECC

Elliptic Curve Cryptography

GPS

Global Positioning System

HTML

Hypertext Markup Language

IP

Internet Protocol

MFH

message from handheld

MTH

message to handheld

PIM

personal information management

S/MIME

Secure Multipurpose Internet Mail Extensions

SMS

Short Message Service

USB

Universal Serial Bus

WAN

wide area network

WLAN

wireless local area network

Provide feedback

5

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

Legal notice

6

©2010 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, SureType®, SurePress™ and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. IBM, Domino, Lotus, Lotus Notes are trademarks of International Business Machines Corporation. Microsoft is a trademark of Microsoft Corporation.. Java is a trademark of Sun Microsystems, Inc.. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

The BlackBerry smartphone and other devices 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 the U.S. and in various countries around the world. Visit www.rim.com/patents for a list of RIM (as hereinafter defined) patents.

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

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

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

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

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

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

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

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

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

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

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

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

Published in Canada